Robert MACIEJEWSKI
University of Applied Sciences in Wałcz
https://orcid.org/0000-0002-1153-8688

DOI : 10.14746/ps.2020.1.23

RIGHT TO PRIVACY AND STATE POLICY ON CYBER SECURITY. NECESSITY OR THREAT FROM THE STATE

The state, as a politically organised community, has a duty to ensure that its citizens, on the one hand, have the right to privacy (right to be alone), which is one of the fundamental rights of every human being, and, on the other hand, it has a duty to guarantee the safety of its citizens, including safety in cyberspace. It therefore seems essential that the state strikes a balance between citizens' rights to privacy and their duty to act for their security, including cyber security. However, the emerging omnipotence of the state in cyber security is becoming an increasing threat to citizens and their right to privacy. Under the guise of ensuring the security of its citizens, the state interferes in almost every aspect of life, and repeatedly does so in a way that can hardly be considered compatible with the standards of a democratic rule of law. Particular attention should be paid to the activities of state bodies in cyberspace. The use by state services of programs for so-called mass surveillance, without the control of judicial authorities, causes that from a democratic state it starts to transform into a total state from where it is not far from a totalitarian one.

The main research objective of this article is to attempt to answer the question whether and what kind of threat to the fundamental rights of citizens, in particular the right to privacy and consequently to the democratic rule of law, posed by the State's actions to ensure security in cyberspace. The research has mainly used such research methods and techniques as content analysis, analysis of legal acts and analysis of records of available data sources (*desk research*).

RIGHT TO PRIVACY – THE CONCEPT

The notion of "privacy" has two fundamental meanings: the first one results from putting it in opposition to the notion of "audience," which refers to the sphere that usually remains in the hands of the public authority; the second – narrower – refers to a specific person and is linguistically similar to such terms as "personal," "individual," and thus defining human personality (Sakowska-Baryła, 2015: 23).

Of particular importance in this context is the article published in 1890 in the Harvard Law Review by two Boston lawyers, Samuel D. Warren and Louis D. Brandeis, under the telling title "The Right to Privacy" (Warren, Brandeis, 1890: 193–220). This article is considered to be a breakthrough in the literature not only because it signifi-

cantly emphasizes the notion of the right to privacy, as this term was previously known in American doctrine. The point is that it presents a new perspective on civil rights, while at the same time extending their scope to include an autonomous right aimed at protecting the sphere of private life (Braciak, 2002: 288). The authors pointed out that technological progress is conducive to the danger of violating individual privacy. They therefore saw a need to identify legal means that could be used to protect a good called "privacy" (Sieńczyło-Chlabicz, 2006: 26).

The issue of the right to privacy began to change at the turn of the 1960s and 1970s. of the 20th century. The factor which led to the separation of personal data protection as a separate area of law was technological development in the field of information processing (Jagielski, 2010: 10).

The sphere of private life also found its place in civil case law as a separate personal good (Kordasiewicz, 2000: 20). A breakthrough in this respect was the ruling of the Supreme Court on January 18, 1984, in which it was stated that "an open catalogue of personal rights makes it possible to include in their scope goods which [...] are connected with the sphere of private and family life, with the sphere of intimacy. Protection in this area may relate to the disclosure of facts from personal and family life, the misuse of information obtained, the collection of information and assessments from the sphere of intimacy through private interviews in order to publish them or otherwise publicise them" (OSN, 1984). This ruling, combined with the construction of the presumption of unlawfulness of an act violating personal interests adopted by the legislator (Article 24 of the Civil Code), gave the aggrieved party the possibility to pursue claims for the infringement of privacy (Radwański, Olejniczak, 2015: 150–151).

The first normative regulation concerning the civil law protection of private life in Poland was made in 1984. At that time, on the basis of art. 14 sec. 6 of the Press Law Act, a ban was introduced on publishing information and data concerning the private sphere of life without the consent of the person concerned. The exception was the defence of a socially justified interest or public activity of the person concerned. Art. 49 of the Act provided for the sanction of a fine for violation of its provisions, while under Art. 40 it became possible to grant monetary compensation for harm suffered in case of intentional violation of personal rights by publishing press materials (Kordasiewicz, 2000: 22).

Privacy is about an individual's anonymity, but at the same time, many of the information that appears on the market exists objectively, independently of the person concerned, allowing him or her to be identified. It seems right to assume that each of us strives to control the circulation of information about ourselves and wants to hide from the curiosity of others (Piotrowski, 2016: 18). As a result, privacy also identifies with the control of information about oneself. Privacy is equated here with selective disclosure, i.e. deciding when, what data and how much of it we reveal about ourselves. This understanding of privacy is also closest to the concept of the right to the protection of personal data.

In the literature on the subject, there are four basic ways of understanding privacy and, consequently, the right to privacy:

– The perception of privacy as an expression of an individual's personality and his or her ability to define himself or herself as a human being;
– Treating privacy as a synonym for autonomy, i.e. the freedom of the individual to think, decide and act;

– To see privacy as an individual's ability to control the circulation of information about him or her, and thus to control his or her relationship with other people;
– Defining privacy by listing its essential components, such as: secrecy, anonymity and seclusion, identity and intimacy, mental peace, physical seclusion, physical exclusivity and autonomy (Mednis, 2016: 14).

In the age of a global society, the issue of information autonomy, which is a kind of subcategory of privacy, has gained particular importance. Closely linked to it are the safeguards offered by the right to the protection of personal data. The danger to be averted by the use of increasingly specialised legal tools is external interference in the private life of individuals. This is due to the acquisition of information belonging to its privacy sphere or centralisation or the monopolisation of the data collected in the files (Preisner, 2002: 909). The right to personal data protection focuses on the protection of information autonomy, which is also referred to as information privacy. Its essence boils down to stating that an individual should have the right to control the content and circulation of information that concerns him/her. It should also be rendered anonymous, as this is required by respect for its privacy and the right to correct and update its data. The inability to exercise such control deprives the individual of his or her sense of freedom to decide his or her own fate. In this case, privacy goes beyond the traditional right to remain at peace. Currently, the right to control personal data, which means the possibility to decide when and to what extent this data can be shared with other entities, is considered the most important aspect of privacy (Piotrowski, 2016: 20).

It should be emphasized that the right to privacy, as expressed in Article 47 of the Constitution and the right to the protection of personal data, which is covered by Article 51 of the Constitution, may constitute assessment criteria used in the process of adjudicating on compliance with the Constitution. However, these rights – due to the provisions of the preamble to the Constitution and its Article 30 concerning human dignity – are at the same time the normative basis of the system, expressing its identity, determined by the dignity and freedom of the individual (Constitution of the Republic of Poland).

The Constitutional Tribunal aptly points out that "the protection of privacy and information autonomy is a consequence of the protection of the inherent and inalienable dignity of man (Article 30 of the Constitution)" (CT judgment, 2014). It is precisely the preservation of human dignity that requires respect for his purely personal sphere, in which he is not exposed to the need to "be with others" or to "share" his experiences or experiences with others (ECJ, 2009).

According to Article 51.1 of the Constitution, no one may be obliged, other than under the Act, to disclose information concerning his person. According to Article 51.2 of the Basic Law, public authorities may acquire, collect and make available only such information about citizens as is necessary in a democratic state of law (Constitution of the Republic of Poland). The Constitution – as indicated by the CJEU jurisprudence – thus implements the most essential elements of the right to the protection of private life: respect for the individual's informational autonomy, i.e., the very obligation to provide access to data limited to strictly defined statutory situations and limiting the arbitrariness of the legislator – therefore, the act cannot shape the scope of the obligation freely (CT judgment, 2002).

In the light of doctrine and jurisprudence, the right to privacy and protection of personal data, as constitutional values associated with the protection of privacy – determines not only the relationship between public authority and the individual, but also the relationship between individuals. The protection of privacy therefore applies to all forms of communication "in any form of communication, regardless of the physical medium used (e.g. personal and telephone calls, written communications, fax, text and multimedia messages, e-mail)" (CT judgment, 2014). According to the CT, this protection covers 'not only the content of the message, but also all the circumstances of the communication process, which include personal data of the participants in the process, information about the telephone numbers dialled, the websites viewed, data showing the time and frequency of calls or enabling the geographical location of the participants in the call, and finally data about the IP or IMEI number (CT judgment, 2014). In the light of the CT's jurisprudence, the "constitutionally guaranteed freedom of man and his information autonomy also includes protection against covert monitoring of the individual and his conversations, even in public and generally accessible places. It does not matter whether the exchange of information concerns strictly private life or professional activity, including business activity. For there is no such sphere of a person's personal life that constitutional protection would be excluded or self-limiting. In each of these spheres, therefore, the individual has the constitutionally guaranteed freedom to transmit and obtain information, including making available information about himself" (CT judgment, 2014).

The right to privacy is linked to the protection of personal data. Recent changes in the area of personal data protection were introduced by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) – the so-called RODO (General Data Protection Act of 10 May 2018).

SECURITY IN CYBERSPACE

The term "cyberspace" was created for the science fiction literature and popularised by William Gibson, who described cyberspace as an unimaginable complexity that is like a "consensual hallucination experienced every day by billions of authorised users in all countries [...]" (Wasilewski, 2013: 226).

However, there is no commonly accepted definition of cyberspace. Attempts to define this concept are more or less general. In a broad, and at the same time abstract, cyberspace is a global information infrastructure, the interconnectivity between people by means of computers and telecommunications, a communication space created by a system of Internet connections that facilitates the network user's contacts in real time and includes all electronic communication systems that transmit information coming from numerical sources (Lakomy, 2015: 76) or "a world-wide information domain where the data carrier is electromagnetic spectrum" (Banasiński, 2018: 24), as well as "a space for open communication through interconnected computers and computer memories working around the world" (Levy, 2002: 380). Such an approach draws attention to the basic

elements of the cyberspace environment, which are: "the vastness (global reach), the fusion of all resources into a single, huge database, complexity and spatiality understood as the inability of cyberspace to relate to the physical (including geographic) dimensions of the real world" (Wasilewski, 2013: 226). In other words, cyberspace is "plastic, liquid, calculable with great accuracy and processable in real time, hypertextual, interactive and finally virtual" (Levy, 2002: 380). The term "virtual" most often refers to an artificial image of reality created by computer devices using graphic programs. But not only – the virtuality of cyberspace also allows for the creation of communities (groups of people) playing specific roles, similarly as in the real world, the so-called cybertrols creating a kind of cyberbrain; such virtual communities are athermal, unrelated neither temporally nor physically (Kawecka, Wójcik, 2015: 155–157).

The basic factor creating cyberspace is the material ICT system, which is a set of cooperating IT devices and software, providing processing and storage, as well as sending and receiving data through telecommunication networks by means of a specific type of telecommunication end device. The literature stresses that cyberspace cannot be identified with the Internet (Banasiński, 2018: 25), treated as "a global system of data exchange based on interconnected local networks, located in many physical locations, allowing simultaneous multi-flat interaction of users from all over the world" (Kulesza, 2010: 57). Cyberspace equally covers the Internet, telecommunication networks or computer systems, and thus all IT systems included in a global network.

The normative definition contained in Polish legislation treats cyberspace as a space for the processing and exchange of information, created by ICT systems, i.e. teams of cooperating IT devices and software that ensure the processing, storage, as well as sending and receiving of data by telecommunications networks by means of a terminal device appropriate for a given type of telecommunications network, designed to be connected directly or indirectly to network terminations, together with the links between them and the relations with users. This definition is also developed in the Cyber Security Strategy of the Republic of Poland for 2017–2022, where, in addition, the Polish cyberspace, understood as "cyberspace within the territory of the Polish state and in places where Polish representations operate (diplomatic posts, military contingents, vessels and aircraft) outside the territory of the Republic of Poland, subject to Polish jurisdiction", has been identified by adopting the territorial criterion (Cyber Security Strategy, 2017).

Focusing primarily on the tool context, such definitions overlook or marginalise the social component of cyberspace, which refers to cyber users and which treats cyberspace as 'a complex environment resulting from non-material interaction between people, software and services on the Internet realised through technical devices and networks connected to it; an equally important, integral and interconnected element with technical infrastructure is its relationship with people and the interaction between people related to its use (Rzucidło, Węgrzyn, 2015: 142). It is therefore assumed in the literature that "cyberspace is a virtual environment for more or less open communication through interconnected computer systems and information and communication links" (Marcinkowski, 2015: 114).

Just as serious definition problems as cyberspace are caused by the concept of cyber security, or security in cyberspace. This is an effect of the blanketness of the

concept of security itself, which takes on different content depending on its qualifier and its subjects. As a normative concept, security is a typical general clause justifying certain actions of the State in the public interest. The notion of security is a dynamic, variable category that needs constant redefinition and has an open scope (Korzeniowski 2016: 140–141).

The definition of cybersecurity proposed by the National Initiative for Cybersecurity Careers and Studies (NICCS)[1] defines security as a situation which ensures that "[...] information or communication systems and the information contained therein are protected or protected against damage, unauthorised use, modification or exploitation" (Chmielewski, 2016: 108). The same institution also proposed a broad definition of cyber security, as "a strategy, policy and standards for both cyber security and its activities, covering, on the one hand, the full range of activities aimed at reducing threats, reducing vulnerability and deterrence, international engagement, responding to events, and, on the other hand, a flexible prevention policy, including appropriate computer network operations, information provision, law enforcement, diplomacy, military, intelligence services, relating to the security and stability of global information and communication infrastructure" (Chmielewski, 2016: 108).

In turn, the International Telecommunications Union in its Recommendation ITU-T X.1205 defines cyber security as "a set of tools, policies, security concepts, safeguards, guidelines, risk management methods, actions, training, best practices, assurances and technologies that can be used to protect the cyber environment and user organisation and resources. User organisation and resources include connected computer facilities, personnel, infrastructure, applications, services, telecommunication systems and all information transmitted and/or stored in the cyber environment. Cyber security seeks to ensure that the security characteristics of the user organisation and resources are achieved and maintained in relation to relevant security threats in the cyberbased environment" (*Rekomendacja*). General security objectives include availability, integrity (which may include authentication and non-repudiation) and confidentiality.

The Cyber Security Strategy of the Republic of Poland for 2017–2022 identifies the concept of cyber security with the security of IT networks and systems and ICT security, treating them as synonyms meaning "the resilience of IT systems, at a given level of trust, to any activity that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or related services offered or accessible via these networks and IT systems" (Cyber Security Strategy, 2017). This definition reflects the provisions of the international standard ISO/IEC 27032, which defines security in cyberspace as preservation of confidentiality, availability and integrity, although it is indicated that other information security features, such as "authenticity, accountability, non-repudiation and reliability in cyberspace." The ISO/IEC 27032 standard, which contains a set of recommendations for Internet service providers, does not necessarily refer to cyber protection (cybersafety), i.e. preventing the effects of negative events that may occur as a result of using information techniques (Chmielewski, 2016: 108–109).

[1] An organization managed by the Cyber Security Education and Awareness Department (located at the Department of Homeland Security of the U.S. Government's Office of Cyber Security and Communications).

The Act of 5.07.2018 on the National Cyber Security System, which, using the ISO/IEC 27032 standard, defines the notion of cyber security as "the resistance of information systems to any activities that violate the confidentiality, integrity, availability and authenticity of processed data or related services offered by these systems," takes a much broader approach to this issue (Act).

The Cyber Security Strategy of the Republic of Poland for 2017–2022 identifies the concept of cyber security with the security of IT networks and systems and ICT security, treating them as synonyms meaning "resistance of IT systems, at a given level of trust, to any activity that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or related services offered or accessible via these networks and systems" (Cyber Security Strategy, 2017). This definition reflects the provisions of the international standard ISO/IEC 27032, which defines security in cyberspace as preservation of confidentiality, availability and integrity, although it is indicated that other information security features, such as "authenticity, accountability, non-repudiation and reliability in cyberspace." The ISO/IEC 27032 standard, which contains a set of recommendations for Internet service providers, does not necessarily refer to cyber protection (cybersafety), i.e. preventing the effects of negative events that may occur as a result of using information techniques (Chmielewski, 2016: 108–109).

The Act of 5.07.2018 on the National Cyber Security System, which, using the ISO/IEC 27032 standard, defines the notion of cyber security as "the resistance of information systems to any activities that violate the confidentiality, integrity, availability and authenticity of processed data or related services offered by these systems," takes a much broader approach to this issue (Act).

The Polish Cyber Security Doctrine of 2015 takes a different approach to this issue, which distinguishes the Polish Cyber Security (security of the Republic of Poland in cyberspace), treating it as "a process of ensuring safe functioning in cyberspace of the state as a whole, its structures, natural persons and legal entities, including entrepreneurs and other entities without legal personality, as well as information systems and information resources at their disposal in global cyberspace and the security of the Polish Cyberspace, understood as a part of the state's cyber security, comprising a set of organisational, legal, technical, physical and educational undertakings aimed at ensuring the undisturbed functioning of the cyberspace of the Republic of Poland together with the public and private critical information and communication infrastructure and the security of information resources processed therein" (*Doktryna*, 2015).

IMPACT OF GOVERNMENT POLICIES ON CYBER SECURITY AND THE RIGHT TO PRIVACY

Ensuring security in cyberspace raises the question of whether state authorities will not use this as an argument to restrict the freedoms and freedoms of citizens and, in particular, to violate their privacy.

The relevant services, with practically infinite possibilities to aggregate data from different sources, including those available only to authorised authorities, have the

possibility to build a space where freedom and thus privacy is only a temporary illusion, maintained for as long as and to the extent that the authorities need it. The information disclosed by E. Snowden on the conduct of extensive intelligence programmes by the U.S. National Security Agency (NSA) and the UK Government Communications Headquarters (GCHQ) has become a cause for discussion on the limits of citizen surveillance, as well as a subject for consideration of the effectiveness and usefulness of existing legal standards for the protection of the legitimate interests of individuals (Grzelak, 2015: 196–199).

The case of E. Snowden, however, forces us to consider the consequences of arbitrary entry into the sphere of privacy in the context of the functioning of the standards that form the foundation of a democratic society – freedom, equality, freedom of expression or the right to information. Testifying before a special committee of the European Parliament and referring to the broad powers of access to information and the threats resulting from this fact to the protection of democratic standards, E. Snowden stated: "without getting up from my seat, I could read the private messages of any member of that committee, as well as any other citizen" (Rojszczak, 2019: 243–244). In addressing the problem of the scope of the justified use of surveillance mechanisms, it should be taken into account whether the transfer of such extensive powers and knowledge about the private affairs of all citizens to special services is, in fact, an activity that fosters the development and maintenance of the standards of a democratic state.

Those who support the use of mass surveillance programmes argue that this is due to the ever-increasing terrorist threat and the associated emergence of various forms of extremism. Such an understanding of surveillance is treated as a necessary measure to ensure public security and, consequently, as a justified case of applying a limitation of legal privacy protection mechanisms (Rojszczak, 2017: 172–174).

Mass surveillance programmes are conducted on a different legal basis from individual surveillance. These are usually regulations related to the functioning of the telecommunications market or the rights of special services. Therefore, the provisions of criminal procedure cannot be applied in this case. Therefore, it requires separate consideration of the legitimacy of applying restrictive standards of conduct for the implementation of individual surveillance in a situation where the application of the same measures – however, in relation to a large group of people (or the society as a whole) can be carried out without the procedural safeguards resulting from the criminal procedure (Rzucidło, Węgrzyn, 2015: 145).

In an attempt to explain what mass surveillance programmes are, it can be concluded that there are activities of public authorities or private entities acting on their behalf, whose aim is to collect information on an unspecified group of people (often the entire population) in an unbiased and wholesale manner. Such programmes do not have generally known and transparent rules on the use of the data, so it is not clear what is the purpose of the processing, to whom the data can be made available – in particular whether and what are the rules on their transfer to third countries (Rojszczak, 2017: 181). As can be seen from this, mass surveillance programmes have as their object the introduction of unlimited control in electronic communications.

Several major surveillance programmes can be identified (Rojszczak, 2017: 182–184):

- PRISM – this program enables NSA to have permanent access to data collected by major Internet service providers such as Microsoft, Yahoo, Google, Facebook, PalTalk, Youtube, Skype, AOL or Apple;
- RAMPART-A – thanks to this program, the NSA is able to obtain any information transmitted on the Internet all over the world. The program has been used by intelligence agencies from Germany and Denmark, allowing the installation of eavesdropping devices on fiber optic links and transferring the obtained data for further processing in the USA;
- OAKSTAR is part of UPSTREAM. Within its framework, NSA cooperated with a Polish partner,[2] within the BUFALLOGREEN operation. It allowed NSA to intercept metadata (since March 3, 2009) and communication content (since March 25). The conducted activities were aimed at collecting information related to international communications passing through the territory of Poland. It is not entirely clear whether these activities have been completed and what were the legal grounds for cooperation of Polish services with the NSA in the field of wholesale collection and transmission of information covered by the telecommunication secrecy to foreigners. This is particularly important if one takes into account the fact that the right to respect for privacy guaranteed in the Constitution covers all persons subject to Polish jurisdiction and not only citizens;
- MUSCULAR – this is a programme aimed at intercepting data from Google and Yahoo processing centres located in the UK.

In addition to the above mentioned surveillance programs, another extremely dangerous program has appeared, called PEGASUS. This program exploits vulnerabilities in phone systems and allows you to take control of the entire device. What's more, the program includes encrypted communicators such as WhatsApp and Signal because of access to the microphone and keypad (encryption of the message by the communicator takes place only at the moment of sending it) and PEGASUS intercepts the message as it is written.

When discussing the issue of state surveillance of a citizen, one cannot overlook the so-called legal path of obtaining and collecting data on citizens by state authorities, i.e. a path based on legal regulations, in particular:

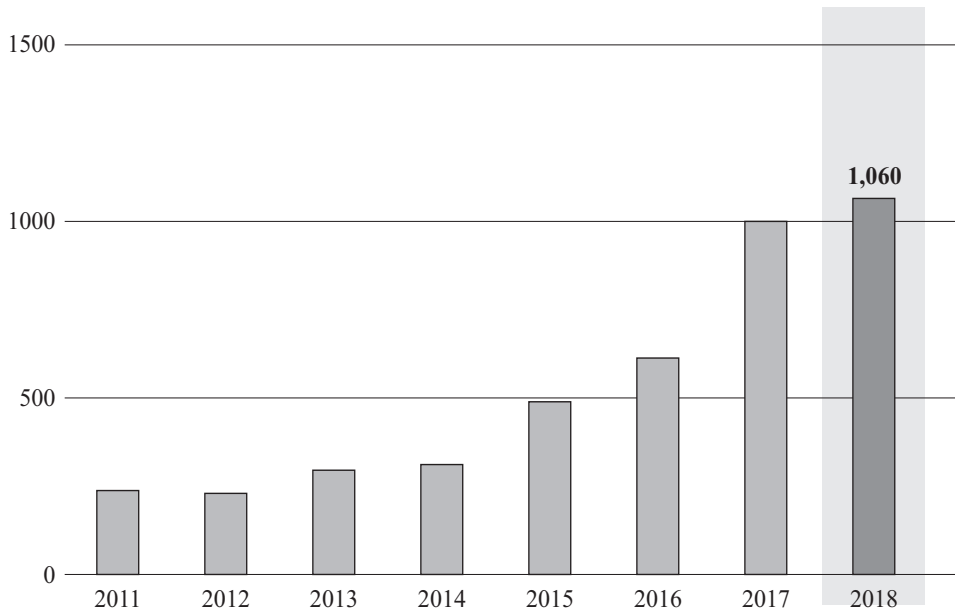
- the Act of 6 June 1997 – Code of Criminal Procedure (Journal of Laws of 1997, No. 89, item 555 as amended);
- the Act of 6 April 1990 on the Police (Journal of Laws of 2015, item 355 as amended);
- the Act of 12 October 1990 on the Border Guard (Journal of Laws of 2014, item 1402 as amended);
- the Act of 28 September 1991 on Fiscal Control (Dz. U. of 2015, item 553 as amended);
- the Act of 21 August 1997 – Law on the organization of military courts (Journal of Laws of 2015, item 1198 and 1890);
- the Act of 27 July 2001 – Law on the system of common courts (Journal of Laws of 2015, item 133, as amended);

[2] The disclosed documents do not specify whether it was ABW, AW or SKW.

– the Act of 24 August 2001 on Military Police and Military Order Organs (Journal of Laws of 2016, item 96);
– the Act of 24 May 2002 on the Internal Security Agency and the Intelligence Agency (Journal of Laws of 2015, items 1929 and 2023);
– the Act of 18 July 2002 on the provision of electronic services (Journal of Laws of 2013, item 1422 and of 2015, item 1844);
– the Act of 16 July 2004 – Telecommunications Law (Journal of Laws of 2014, item 243, as amended);
– the Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service (Journal of Laws of 2014, item 253, as amended);
– the Act of 9 June 2006 on the Central Anti-Corruption Bureau (Journal of Laws of 2014, item 1411, as amended);
– the Act of 27 August 2009 on the Customs Service (Journal of Laws of 2015, item 990, as amended);
– the Act of 29 August 1997 – Banking Law (Journal of Laws of 1997, No. 140, item 939, as amended).

Data obtained in a legal manner – on the basis of legal regulations – are mainly obtained from Internet service providers. In the statistics for 2018 it is as follows:

Figure 1. Facebook

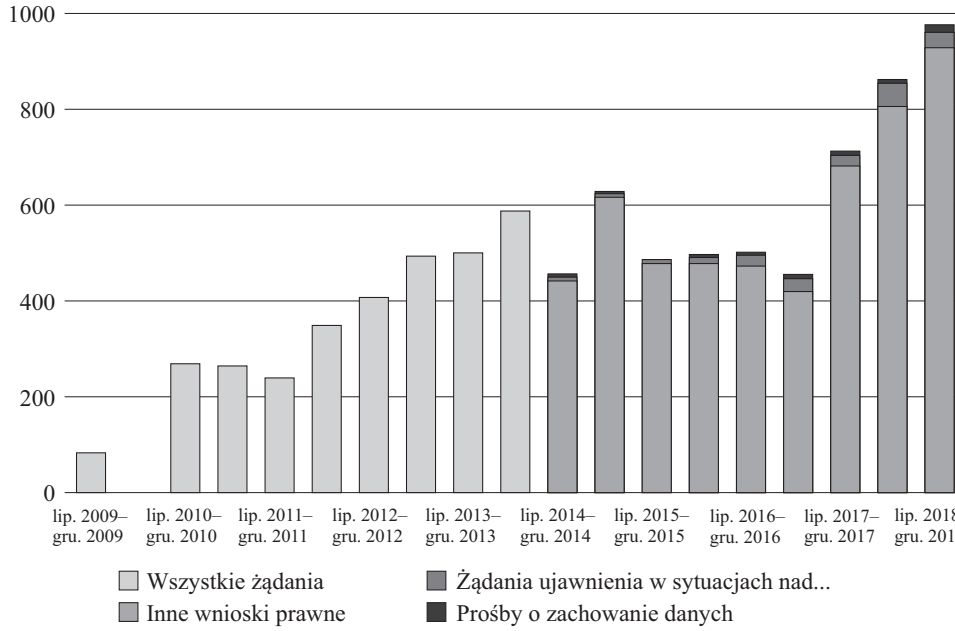


Source: https://www.spidersweb.pl/2019/09/jak-inwigiluja-polskie-sluzby.html (18.12.2019).

The situation is similar for Microsoft and Apple. In the second half of 2018, Polish services asked Microsoft for information about the data 101 times, and this concerned 1,444 accounts. Of these, 34% of the requests were rejected, 34% of the data were not found, and in the remaining 30% the data were provided. At the same time, 61 requests

for data were sent from Poland to Apple and concerned 1,702 devices, 29 financial identifiers and 15 accounts. Apple 60% of the requests were positively received.

Figure 2. Google



Source: https://www.spidersweb.pl/2019/09/jak-inwigiluja-polskie-sluzby.html (18.12.2019)

The size of such activities may be proved by the report of the Minister of Justice of the Public Prosecutor General for 2018, which also includes information concerning acquisition of telecommunications and Internet data. According to the report, the Police, the National Revenue Administration, the Border Guard, the Internal Security Agency, the CBA, the Treasury Intelligence Service, the Military Police Headquarters, the Military Police Branches and the Military Counterintelligence Service processed a total of 1,356,775 data, including the following: 1,325,241 telecommunications and 22,933 Internet.[3] The scale of this phenomenon is constantly growing anyway:

– in 2012 – The police registered 5,995 applications and orders for operational control;
– in 2013 – 6,814;
– in 2014 – 7,975;
– in 2015 – 8,945;
– in 2016 – 9,506;
– in 2017 – 9,876.

[3] The data presented are based on official information provided by Polish services, https://wiadomosci.dziennik.pl/wydarzenia/artykuly/603182,inwigilacja-sluzby-podsluchy-polska-prawo.html.

Out of the total number of applications, only 151 were not permitted to order an operational control, including 142 applications did not obtain consent of the prosecutor and 9 of the regional court having territorial jurisdiction.[4]

* * *

Certain circumstances may make democratic values an obstacle to cybersecurity. Cyber-security management is an extreme in authoritarian states that control access to the Internet, with the aim of, among other things, restricting users access to websites selected and accepted by the authorities. The methods used to make the elements of cyber security management work together, especially between the government and individuals, increasingly determine the model of power in the state. The pluralist nature of cyberspace provides an opportunity for free, individual and unfettered expression. However, if democratic values are limited in this area, then the balance between democracy and security will be compromised in favour of security. Evidence of unethical and illegal activities is provided by documents leaked thanks to a former NSA employee – Edward Snowden. They revealed, among other things, the enormous scale of cyber surveillance used by intelligence services and their activities penetrating private areas in communication networks.

The domination of the value of cyber security in state policy may cause a number of negative consequences, which may include, among others, the desire to introduce legal regulations that may restrict civil rights and freedoms, and in the next stage may lead to violence. In addition to the high physical damage and direct financial losses, the very likelihood of future cyber threats may cause social distrust and aversion to working with new technologies.

It seems obvious that programmes of mass and unlimited surveillance do not meet the criterion of necessity in a democratic society. As a result, their implementation causes unauthorised interference of public authorities in the sphere of citizens privacy. It should also be emphasized that the global nature of the Internet means that mechanisms based on territoriality in a rather limited way ensure effective protection of individuals' rights against violations by public authorities in cyberspace.

The above considerations lead to the conclusion that legal privacy safeguards are an effective mechanism that can lead to a limitation of the scope of data collected by the State, including for mass surveillance programmes. While the use of other measures, including technical ones, may increase the sense of privacy in individual cases, they do not systematically address the lack of respect by intelligence services for rights under international and national legislation.

There is no doubt that ICT surveillance methods play an extremely important role in the activities of state security services, allowing, inter alia, interception of communications and metadata through searches of databases. These activities – both legal and illegal – undoubtedly constitute interference with fundamental rights, especially the right to data protection and privacy. Therefore, it is extremely important to consider the necessity of subjecting such state actions to the control of independent bodies,

[4] The data presented were based on official information provided in the report of the Minister of Justice of the Attorney General https://www.prawo.pl/prawnicy-sady/tajemnica-zawodowa-sluzby-naruszaja-mimo-zakazu,332166html.

which will make it possible to maintain a kind of balance between citizens' right to privacy and arbitrary decisions of state bodies violating this sphere. The practice of exchanging information obtained through covert surveillance between States is becoming more and more common "The increasing practice of governments to transfer and share intelligence obtained through covert surveillance – a practice whose usefulness in the fight against international terrorism, as already stated, is beyond doubt and which concerns both exchanges between Council of Europe Member States and with other jurisdictions – is another factor requiring special attention as regards external surveillance and remedies" (Judgment of the ECHR of 12 January 2016).

A citizen's clash with the machinery of the state puts the former in a position to lose out if he is not equipped with real means and possibilities of effective defense against the services' aspirations to omniscient knowledge of citizens. Without depreciating the power of the competent authorities to legitimately interfere in the sphere of privacy, it must be stated that such interference must take place solely on the basis of the rules of law, "[The] interference can only be justified under Article 8(2) if it is lawful, pursues one or more of the legitimate aims set out in Article 8(2) and is necessary in a democratic society in order to achieve those aims [...]" (*ECtHR judgment of 4 December 2015*) and should always be reviewed by independent judicial authorities if we are not to be threatened by the vision of an Orwellian totalitarian state.

REFERENCES

Banasiński C. (2018), *Podstawowe pojęcia i postawy prawne bezpieczeństwa w cyberprzestrzeni*, in: *Cyberbezpieczeństwo. Zarys wykładu*, (ed.) C. Banasiński, Wolters Kluwer, Warszawa.

Braciak J. (2002), *Prawo do prywatności*, in: *Prawa i wolności obywatelskie w Konstytucji RP*, (eds.) B. Banaszak, A. Preisner, Wydawnictwo C.H. Beck, Warszawa.

Chmielewski Z. (2016), *Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich*, „Studia z Polityki Publicznej", No. 2.

Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej (2015), Warszawa.

Grodecka M., *Jak inwigilują polskie służby*, Spider's web, https://www.spidersweb.pl/2019/09/jak-inwigiluja-polskie-sluzby.html.

Grzelak M. (2015), *Skutki sprawy Edwarda Snowdena dla prywatności danych w cyberprzestrzeni*, „Bezpieczeństwo Narodowe", No. I.

Jagielski M. (2010), *Prawo do ochrony danych osobowych. Standardy europejskie*, Wolters Kluwer, Warszawa.

Kawecka K., Wójcik D. (2015), *Patologie w cyberprzestrzeni – analiza przypadku grupy pomocowej utworzonej w jednym z portali społecznościowym*, in: *Patologie w cyberprzestrzeni. Profilaktyka zagrożeń medialnych*, (ed.) D. Morańska, Wydawnictwo WSB, Dąbrowa Górnicza.

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz. U. 1997, Nr 78, poz. 483 z pózn. zm.

Kordasiewicz B. (2000), *Cywilnoprawna ochrona prawa do prywatności*, „Kwartalnik Prawa Prywatnego", z. 1.

Korzeniowski L. F. (2016), *Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych*, European Association for Security, Kraków.

Kulesza J. (2010), *Międzynarodowe prawo Internetu*, Wydawnictwo Ars Boni et aequi, Poznań.

Lakomy M. (2015), *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wydawnictwo Uniwersytetu Śląskiego, Katowice.

Leśniak G., *Tajemnica zawodowa nie przeszkadza służbom w podsłuchiwaniu*, Prawo.pl, https://www.prawo.pl/prawnicy-sady/tajemnica-zawodowa-sluzby-naruszaja-mimo-zakazu,332166.html.

Levy P. (2002), *Drugi potop*, in: *Nowe media w komunikacji społecznej w XX wieku. Antologia*, (ed.) M. Hopfinger, Oficyna Naukowa, Warszawa.

Marcinkowski C. (2015), *Cyberprzestrzeń a istota wybranych zagrożeń społecznych dla bezpieczeństwa współczesnego człowieka*, in: *Patologie w cyberprzestrzeni. Profilaktyka zagrożeń medialnych*, (ed.) D. Morańska, Wydawnictwo WSB, Dąbrowa Górnicza.

Mednis A. (2016), *Prywatność od epoki analogowej do cyfrowej – czy potrzebna jest redefinicja?*, in: *Prywatność a jawność – bilans 25-lecia i perspektywy na przyszłość*, (ed.) A. Mednis, Wydawnictwo C.H. Beck, Warszawa.

Nowosielska P., *Polska to inwigilacyjne El Dorado. Cała prawda o podsłuchach*, Wiadomości Dziennik, https://wiadomosci.dziennik.pl/wydarzenia/artykuly/603182,inwigilacja-sluzby-podsluchy-polska-prawo.html.

General Data Protection Act of 10 May 2018 (Journal of Laws 2018, item 1000) and in agreement with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

OSN I CR 400/83 – OSN 11/1984, nr 195.

Piotrowski R. (2016), *Prawo do prywatności i ochrony danych osobowych jako wartości konstytucyjne*, in: *Prywatność a jawność – bilans 25-lecia i perspektywy na przyszłość*, (ed.) A. Mednis, Wydawnictwo C.H. Beck, Warszawa.

Preisner A. (2002), *Zamiast zakończenia. Rozwój technologiczny a przyszłość praw jednostki*, in: *Prawa i wolności obywatelskie w Konstytucji RP*, (eds.) B. Banaszak, A. Preisner, Wydawnictwo C.H. Beck, Warszawa.

Radwański Z., Olejniczak A. (2015), *Prawo cywilne – część ogólna*, Wolters Kluwer, Warszawa.

Rekomendacja ITU-T X.1205, https://www.itu.int/rec/T-REC-X.1205-200804-I.

Rojszczak M. (2019), *Prywatność w epoce Wielkiego Brata: podstawy prowadzenia programów masowej inwigilacji w systemie prawnym Stanów Zjednoczonych*, Ius Novum, No. 1.

Rojszczak M. (2017), *Prawne podstawy prowadzenia masowej inwigilacji obywateli opartej na hurtowym i nieukierunkowanym przechwytywaniu danych w UE z uwzględnieniem dorobku orzeczniczego TSUE i ETPC*, „Studia Prawa Publicznego", No. 2.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz. Urz. UE L Nr 119, s. 1, ze sprostowaniem.

Rzucidło J., Węgrzyn J. (2015), *Stany nadzwyczajne w sytuacji szczególnego zagrożenia państwa w cyberprzestrzeni*, „Przegląd Prawa Konstytucyjnego", No. 27.

Sakowska-Baryła A. (2015), *Prawo do ochrony danych osobowych*, Wydawnictwo Presscom, Wrocław.

Sieńczyło-Chlabicz J. (2006), *Naruszenie prywatności osób publicznych przez prasę. Analiza cywilno-prawna*, Wydawnictwo Zakamycze, Kraków.

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

Warren S. D., Brandeis L. D. (1890), *The Right to Privacy*, "Harvard Law Review", Vol. 4: 193–220, http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm.

Wasilewski J. (2013), *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego", No. 9.

Cyber Security Strategy of the Republic of Poland for 2017–2022 (2017), Ministry of Digitalisation, Warsaw.

Act of 18 April 2002 on the state of natural disaster, Journal of Laws of 2017, item 1897 as amended.

Act of 21.06.2002 on the state of emergency, Journal of Laws of 2017, item 1928 with amendments.

Act of 29.08.2002 on martial law and the powers of the Commander-in-Chief of the Armed Forces and the principles of his subordination to the constitutional bodies of the Republic of Poland, Journal of Laws of 2017, item 1932 as amended.

Act of 5 July 2018 on the National Cyber Security System, Journal of Laws. 2018 item 1560.

Judgment of the ECHR of 12 January 2016 in the case of Szabo and Vissy v. Hungary, complaint No. 37138/14, § 77.

ECtHR judgment of 4 December 2015 in case of Roman Zakharov v Russia [VI], complaint No. 47143/06, § 227.

Judgment of the Constitutional Tribunal of 12.11.2002, SK 40/01, OTK-A 2002, No. 6, item 81.

Judgment of the Constitutional Tribunal of 23.6.2009, K 54/07, OJ of 2009. No. 105, item 880.

Judgment of the Constitutional Tribunal of 30.7.2014, K 23/11, Journal of Laws of 2014, item 1055.

ABSTRACT

In the era of extremely rapid technological development, the state is directing particular interest towards security in cyberspace and cyber security is becoming a dominant value in its policy. Such a policy may cause a number of negative consequences, such as the willingness to introduce legal regulations that may limit civil rights and freedoms, and in the next stage may lead to violence. As a result, their implementation causes excessive, and often unauthorized, interference of public authorities in the sphere of citizens' privacy. It should also be stressed that the global nature of the Internet means that mechanisms based on territoriality in a rather limited way ensure effective protection of individual rights against violations by public authorities in cyberspace. In addition to significant physical damage and direct financial losses, the mere likelihood of future cyber threats may cause social distrust and unwillingness to work with new technologies.

Keywords: right to privacy, cyberspace, cyber security, mass surveillance

PRAWO DO PRYWATNOŚCI A POLITYKA PAŃSTWA W ZAKRESIE CYBERBEZPIECZEŃSTWA. KONIECZNOŚĆ CZY ZAGROŻENIE ZE STRONY PAŃSTWA

STRESZCZENIE

W dobie niezwykle szybkiego rozwoju technologicznego szczególne zainteresowanie państwo kieruje ku bezpieczeństwu w cyberprzestrzeni, a dominującą wartością w jego polityce staje się cyberbezpieczeństwo. Tego rodzaju polityka może wywołać szereg negatywnych

konsekwencji, do których można zaliczyć m.in. chęć wprowadzenia regulacji prawnych, które ograniczać mogą prawa i swobody obywatelskie, a w następnym etapie mogą prowadzić do stosowania przemocy. Skutkiem tego, ich realizacja powoduje nadmierną, a niejednokrotnie nieuprawnioną ingerencję organów publicznych w sferę prywatności obywateli. Należy też podkreślić, że globalny charakter Internetu sprawia, iż mechanizmy oparte na terytorialności w dość ograniczony sposób zapewniają skuteczną ochronę praw jednostek przed naruszeniami ze strony władzy publicznej w cyberprzestrzeni. Obok dużych szkód fizycznych i bezpośrednich strat finansowych, samo prawdopodobieństwo wystąpienia przyszłych cyberzagrożeń wywoływać może społeczną nieufność i niechęć do pracy z nowymi technologiami.

Słowa kluczowe: prawo do prywatności, cyberprzestrzeń, cyberbezpieczeństwo, masowa inwigilacja

Article submitted: 11.02.2020; article accepted: 12.05.2020.