LEX LOCALIS

Security v. Privacy - Legal Aspects

Authors:
Katarzyna Chałubińska-Jentkiewicz
Monika Nowikowska


§
LEX
LOCALIS

Title: Security v. Privacy – Legal Aspects

Authors: univ. prof. dr. Katarzyna Chałubińska-Jentkiewicz (War Studies University, Poland), assist. prof. dr. Monika Nowikowska (War Studies University, Poland)

Review: prof. dr. Joanna Sieńczyło-Chlabicz (University of Bialystok, Faculty of Law, Poland), assoc. prof. dr. Jarosław Kostrubiec (Maria Curie-Skłodowska University, Faculty of Law and Administration, Poland)

Kataložni zapis o publikaciji (CIP) pripravili v Narodni in univerzitetni knjižnici v Ljubljani
COBISS.SI-ID=52948739
ISBN 978-961-7124-01-9 (pdf)

First published in 2021 by
Institute for Local Self-Government Maribor
Smetanova ulica 30, 2000 Maribor, Slovenia
www.lex-localis.press, info@lex-localis.press

For Publisher:
assoc. prof. dr. Boštjan Brezovnik, director

Price: free copy

The book has been prepared in the result of cooperation at the realization of the research project, entitled "The Polish cybersecurity system - a model of legal solutions" The Agreement MON Nr GB/4/2018/208/2018/DA] granted by Ministry of National Defence.

https://doi.org/10.4335/978-961-7124-01-9 ISBN 978-961-7124-01-9

Available online at http://www.lex-localis.press.

Security v. Privacy - Legal Aspects

Authors:
Katarzyna Chałubińska-Jentkiewicz
Monika Nowikowska

Maribor, 2021

LEX LOCALIS

Security v. Privacy – Legal Aspects

KATARZYNA CHAŁUBIŃSKA-JENTKIEWICZ & MONIKA NOWIKOWSKA

Abstract The monograph is an attempt to indicate areas where there are threats to the privacy of an individual in the conditions of development of new technologies and to determine necessary regulatory directions. There is no doubt that one of the task of the state is to protect the safety of its citizens. Necessary is therefore to establish the status of an individual in the conditions of legal regulations ensuring protecting personal and public safety, and indication of new rules for the operation of public administration and to specify the limits of interference by public authorities. Implemented by state authorities some tasks may constitute a significant limitation of the legal protection of life private entity, guaranteed in art. 47 of the Polish Constitution. In that sense there is a natural antinomy between state security and privacy of the individual, the freedom of the individual from state interference. Society undoubtedly, it is willing to give up part of its freedom in exchange for security. These concessions are called part of the social contract. Challenge but it is the fixing of mutual limits of concessions between freedom and safety. How much can an individual be expected to relinquish freedom for the sake of common security and vice versa, to what extent can be waived from the implementation of security policy to ensure the necessary scope of freedom.

Keywords: • privacy • security • new technologies • regulation • public safety

CORRESPONDENCE ADDRESS: Katarzyna Chałubińska-Jentkiewicz, Ph.D., University Professor, War Studies University, Law Institute, Aleja Generała Antoniego Chruściela „Montera" 103, 00-910 Warsaw, Poland, email: k.jentkiewicz@akademia.mil.pl. Monika Nowikowska, Ph.D., Assistant Professor, War Studies University, Law Institute, Aleja Generała Antoniego Chruściela „Montera" 103, 00-910 Warsaw, Poland, email: m.novwikowska@akademia.mil.pl.

https://doi.org/10.4335/978-961-7124-01-9 ISBN 978-961-7124-01-9

Available online at http://www.lex-localis.press.

Content

Introduction

The subject of our considerations is to indicate areas where there are threats to the privacy of an individual in the conditions of development of new technologies and to determine necessary regulatory directions. In this scope of research, it is necessary to determine the status of an individual in the conditions of regulations ensuring protection of personal security, but also public safety in the current legal status, as well as to indicate new rules of operation of public administration and to specify the limits of interference by public authorities. This problem relates to several basic areas of regulation. These are: protection of constitutional rights and freedom of an individual, restrictions of these rights and freedom in the conditions of necessary operation of public administration, and determination of instruments for implementing this protection.

In the context of such research assumptions, the basis for consideration it is just the issue of new regulatory solutions. The main and priority question seems to be the issue of defining the objectives of protecting public security in the context of the rights of an individual, since security constitutionally justifies all restrictions, but is also the basis for the operation of public administration and the use of specific instruments by public authorities. This will refer to research questions about the level of defining the objectives of the national security (state security, internal security, individual - personal security), the scope of defining and competence in achieving these objectives (institutional solutions, legal norms and procedures). This issue will concern the role of the state, the content of public tasks, determined by the objectives of the public interest, the responsibility and entitlements of public administration authorities, as well as the obligations of an individual - a citizen. The limits must be set by fundamental rights expressed in international agreements and in the Polish Constitution.

In this area, it is important to specify the regulatory goals expressed in the strategies and assumptions underlying the regulatory policy based on development trends related to the ideology of an individual freedom in the full area of its activity.

Consequently, the area of our considerations should be divided into four areas:

1. Individual and fundamental rights, taking into account axiological aspects, the basis of which should be perceived in the philosophical and sociological concepts of human dignity.
2. Identity as a phenomenon and permanent element related to personal and national security and the challenges of a digital world.
3. System solutions for privacy and identity presented on the selected examples, with particular emphasis on the current system of the constitutional and administrative law in the digital conditions.

4. Security as a premise for restrictions of privacy and identity.

The basic research problem is to determine a contemporary status of an individual - as part of the nation - a citizen in the regulatory area, in the context of protection of the national security. The legal situation of an individual - a citizen - consists of a set of rights and obligations set by legal norms and decisions of administrative bodies. In this area of research, the sphere of human constitutional rights and obligations should be separated from the rights and obligations of a citizen in the executive sphere of the state, i.e. public administration. This is a particularly important issue for analyzing the issue in the context of social changes related to the development of the so-called digital democracy and the need to ensure cyber security.

In this aspect, we can talk about public authority, which faces a new task - re-legitimization within the division of power, where the boundaries of this division are blurred as a result of the widespread administrative and legal convergence as a consequence of technological convergence. The situation of an individual - a citizen requires a new regulatory approach. After the era of *ex post* activities, the concept of an *ex ante regulation is more often required*. Digital conditions and technological progress carry the risk of losing control, the monitoring by the public authorities of security conditions - starting from the public security to individual interests in the general sense of personal security. There is also an international factor that requires inter-state cooperation in the conditions of blurred national borders and the continuing deprivation of identity differences. It seems that in these conditions it is necessary to set priorities and specify the areas of primacy of public institutions over the world of economic concerns using new technologies in achieving profit at the expense of, among others, a consumer privacy (Lorenzi & Berrebi, 2019:236-237).

The situation of an individual's privacy guaranteed by the international law and constitutional norms is the basis for determining the conditions of the rule of law. Reference should also be made to the protection of fundamental rights guaranteed by the European law. On the global scale, regulations regarding the right to privacy need updating. This is due to the fact that large international corporations supervise and monitor consumer behavior of the network users - most often with their more or less informed consent. Glocalization is a standard in a *big data* driven economy. Optimization of marketing campaigns means data positioning, profiling and creating sales systems based on the knowledge about the individual. As J-H. Lorenzi, M. Berrebi (2019:226) "(...) the terrifying border has been crossed in the field of controlling our own will. Knowledge of a person is and will be so great that it will ultimately affect his behavior. In this case, we can speak without hesitation about the mechanism of self-fulfilling prophecy, that is, the almost permanent loss of our freedom of choice as individuals". Fundamental rights are treated as one of the principles of the European legal order, and their protection is thus analyzed in the jurisprudence of the European Court of Justice. However, there is the problem of the interface between two concepts of the right to privacy. A continental concept, in which dignity is an important element of protection,

which results in the protection of feelings and the need to preserve intimacy from the tradition derived from the American sense of freedom, expressed as a value associated with ensuring the protection of the place, the integrity of the home mir. This difference in understanding the right to privacy automatically translates into the concept of regulating the sphere of the right to privacy (Stalla et al., 2014:7).

At the same time, it should be emphasized that the relationship between rights and obligations in the sphere of administrative law and administrative activities at the national level may be even more diverse. That is why, first of all, the legal situation of an# individual - a citizen, in the conditions of operation of the public administration at the national level should be analysed (Dybowski, 2007)[1]. In fact, this issue touches the priority of the functions of the state over the rules of the economic freedom. The very definition of the public administration can be formulated based on its goals, i.e. protection of the national security. Ultimately, the needs of individuals fill the content of the needs of the state. One of these needs is the sense of security. This is due to the fact that the administrative body is not the recipient of the citizen's behavior, but only the entity verifying this behavior. Often, this verification is associated with the restrictions of the fundamental freedoms and rights, dictated by the protection of the public interest, and one of its main objectives is to ensure security. This phenomenon is particularly evident in the sphere of opposition to the protection of personal data against the obligations of the so-called data retention. That is why in this relation one should also analyze the issue of civic duties, which are an obvious consequence of the organization and functioning of the state as a sovereign.

Another important concept for our considerations will be the issue of public subjective rights. Public subjective law is a concept closely related to the rights and competences acquired by an entity within the scope of a specific legal relationship related to the entity's situation in the area of the public law. In the case of research related to the status of an individual - citizen in the space of protection of the right to privacy, as part of the organizational and management function of the state. The purpose of this research is to formulate a diagnosis regarding the condition of the Polish State in the area of ensuring the national security and personal security in the conditions of cyberspace development.

The analysis of the above issue will allow a division of the situation of an individual - a citizen, into activities related to constitutional guarantees, which will always form the basis for assessment of the status of an individual - a citizen, as part of the functioning of the state, in particular, in the sphere of performing its organizational function. System solutions regarding civil rights and freedoms related to the right to privacy in the area of the state's organizational activities are of significant importance. There are two problems to be discussed here. One concerns the issue of supervision and its various instruments that serve public authorities to execute the tasks related to the restriction of freedom of an individual - a citizen. This sphere of issues includes these related to the legal situation in the light of convention arrangements related e.g. to bodily inviolability and moral

integrity. The key element of this analysis will be prohibition of using invasive information systems against an individual.

The second problem concerns a takeover of control by developed technology companies that use knowledge about an individual on a global scale, and avoiding contact with them will be considered social exclusion. Facebook, Google or Amazon business models rely on the identification of a user, collection of information about the user, as well as its sale. In the technological environment, the freedom of choice according to one's own will becomes problematic. This area also concerns the use of market mechanisms based on the processing of knowledge about the users and manipulation of this knowledge in a political struggle. The information struggle entering the private area may in consequence also lead to the national identity crisis. It seems that this situation causes a natural protest and strengthens the need for consolidation primarily at the national and state level, taking into account those elements close to a given community which identify it. However, taking advantage of this type of weakness is another level of threats that affect the sovereignty of the nation and state.

The conflict noted by the authors between the need to ensure cybersecurity and the right to privacy of an individual - a citizen, also requires consideration from the point of view of the phenomenon of cyberterrorism. It seems that the choice between freedom and security is a very difficult one. The threat of cyber terrorism has a dual nature. On the one hand, there can be assassinations, material losses, fear in the society. On the other hand, however, an excessive state reaction can also be considered a threat. It is important for democratic societies to overcome terrorism by maintaining their principles of freedom on which they are founded. Closing a citizen by the state in a well-guarded fortress, increasingly newer systems of monitoring, surveillance and control do not constitute a solution to the problem. This would mean the loss of value, including the right to privacy, which must be defended in the fight against cyberterrorism. To ensure cybersecurity, one should adopt an acceptable risk approach and think about it in an innovative way, perceiving it as a process with many links, including legal and organizational solutions. It is important to know that the fight against cyberterrorism implies not only technology and organization, but also moral challenges. When considering moral issues, basic values, such as the privacy of individuals - citizens, should be taken into account. One cannot break the rules one defends. If, by fighting cyberterrorism and defending democratic values, we start to break them out of the fear of threat, terrorists may believe that they have won (Aleksandrowicz, 2015: 157-158).

This important research area should have been divided into several detailed issues, thematically arranged, constituting at the same time the scope of recommendations in the area of future regulations, also restrictions in the area of the right to privacy, as an inevitable stage in the protection of humanity and its future.

Notes:

[1] The issue of the protection of rights and freedoms at the European level was discussed in the work of Dybowski, Fundamental rights in the jurisprudence of the ECJ, in which the author discusses the functions of fundamental rights in the Community legal order through references to the jurisprudence of the European Court of Justice.

Chapter I

Privacy and the Right to Privacy in the Cyber Security System - Definition Issues, the Scope of Regulation

1 The concept of privacy: definitions, the scope of regulation

The concept of the right to privacy as a protected personal good is a product of the American doctrine *of the right of privacy*. The issue of the right to privacy under the Polish legal order has for years been the subject of research and has a rich jurisprudence. In Poland, A. Kopff was the first to formulate the thesis that the sphere of private life of a person belongs to his/her personal rights and is protected under the provisions of the Civil Code. According to the author, the sphere of private life is a personal good including everything "which, due to a justified separation of an individual from the general public, serves the development of its physical and psychological personality and maintenance of the achieved social position" (Kopff, 1972:32-33).

In the Constitution of the Republic of Poland of April 2, 1997, in Article 47 the right to privacy was expressed *expressis verbis*. This provision guarantees everyone the right to a legal protection of a private and family life, honor and good name, and to decide about their personal lives. On the basis of the Constitution of the Republic of Poland, privacy is understood in two meanings: a broader one - as the freedom from interference in the sphere inaccessible to other people and the freedom to decide about one's own life, views, beliefs, and a narrower one, identified with the right to decide on the scope of information about oneself disclosed to others (Sieńczyło-Chlabicz el al., 2019:239).

The analysis of the provisions of the Polish Constitution indicates that the right to privacy, in addition to Article 47, is guaranteed by a number of other provisions that complement each other (Młynarska-Sobaczewska, 2009:396). These provisions include Article 51 clause 1, which stipulates that no one may be obliged otherwise than under the Act to disclose information about his/her person, the so-called right to the information autonomy. This provision guarantees the protection of data and information about a citizen - an individual, and the freedom to keep secret any information which, in the person's opinion, belongs to his/her sphere of private or intimate life. An exception to the principle of the information autonomy of an individual may be provided for only when it is necessary in a democratic state ruled by law and is subject to strict formal and material requirements provided for by the principle of proportionality (Safjan, 2002:234).

Similarly, Article 53 clause 7 of the Constitution of the Republic of Poland stipulates that no one may be obliged by organs of the public authority to disclose his/her worldview,

religious beliefs or religion. The literature on the subject also indicates that the broadly understood right to privacy also includes the right of parents to raise children in accordance with their beliefs (Article 48 of the Constitution of the Republic of Poland) and to provide children with moral and religious education and teaching in accordance with their beliefs (Article 53 clause 3 of the Constitution of the Republic of Poland). It should be noted that the manifestation of the right to privacy is, specified in Article 50 of the Constitution of the Republic of Poland, inviolability of the home and admissibility of conducting a search only in cases and in the manner specified in the Act, and provided for in Article 49 - secrecy of correspondence[1].

The Polish legislator has not defined the concept of personal rights but only made a closer determination of the scope of personal rights by their exemplary listing in Article 23 of the Civil Code (1964). The structure of this provision, and especially the phrase "in particular" used in it, shows that the personal rights indicated in it are listed only *exempli modo* (Sieńczyło-Chlabicz el al., 2019:229).
In Article 23 of the Civil Code the legislator mentions: health, freedom, honor, freedom of conscience, surname or pseudonym, image, secrecy of correspondence, inviolability of the home, scientific, artistic, inventive and rationalization work. Privacy has not been expressed in it *expressis verbis*. It should be noted that the catalog of personal rights is constantly expanded by the doctrine (Radwański, 1997:149) and the case law[2], and its open nature allows it to cover various values that the legislator is unable to foresee. As the Court of Appeal in Bialystok aptly emphasized in its judgment of January 12, 2017, the definition of personal rights is based on an open catalog, and the personal rights listed therein are exemplary. The nature of these goods is varied, because they are related to a human being and the sphere of private life of an individual.

The analysis of the Polish case law allows for the statement that in none of the judgments has the court made an attempt to exhaustively enumerate the circumstances covered by the right to privacy. Each time, courts individually, depending on a specific factual situation, assign a given situation to the scope of privacy or refuse protection in this respect. Based on the case law of the Supreme Court and common courts, an example catalog of circumstances that have been included in the sphere of private life can be indicated.

In the Polish jurisprudence, the right to privacy is defined as the information autonomy, understood as, guaranteed to each person, the right to independently decide on the extent to which he/she wants to remain anonymous and within which they agree to disclose information to third parties. It is an individual himself/herself that defines the scope, sphere of events in his/her life that can be disclosed to third parties.

2 The concept of security - Security and cyber security - Strategy

The modern conditions of an individual's functioning in cyberspace determine the need to take new activities in the scope of establishing the norms, principles and values that are the standard in the real world. The need for protection and guarantee of security in the virtual reality is indicated by the European Commission in a Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, entitled "The European Union Cybersecurity Strategy: Open, Secure and Protected Cyberspace"[3]. In this Communication, the Commission emphasized that fundamental rights, democracy and the rule of law should be protected in cyberspace. Freedom in the internet environment requires security and protection. Cyberspace should be protected from incidents, harmful activities and abuse, with government administrations playing a significant role in ensuring free and secure cyberspace. Their mission should be to respect and protect fundamental rights on the internet and maintain internet reliability and interoperability. However, large parts of cyberspace are owned by the private sector and therefore, all initiatives in this area must take its leading role into account.

As the result of the process of digitization and expanding the scope of electronic communication services, a new regulatory policy has become necessary. We are currently witnessing radical changes in the way society and the global economy operate. The report *Suggested directions for the development of the information society in Poland until 2020* indicates that the key area of changes in this respect, apart from the political and economic aspects of competitiveness of economy, will be the role of public authorities. The state will be forced to limit the scope of its management function in favor of shaping strategies and mechanisms of development, standardization and mediation. The revolutionary changes result mainly from the fact that "the current methods of exercising power and managing the state will simply be ineffective in a society in which information will become the main product." Digitization has become the cause of administrative *convergence*, i.e. the process of creating new, common administrative solutions in place of traditional administrative differences. Such areas are defined at the level of the European Union and their division is marked by new threats to the national security.

One of the key regulatory goals is to ensure cyber security, which requires actions related to maintaining the availability and integrity of the network and infrastructure, as well as the confidentiality of information contained therein, taking into account the right to privacy and respect for identity. It should be noted here that cybersecurity is of particular importance in ensuring an individual's fundamental rights in terms of his/her privacy.

Ensuring cybersecurity is becoming one of the basic goals of the state and the determinant of these principles is the protection of basic values that should have the same degree of protection in cyberspace as in the real world. It should be noted that the effectiveness of security protection in cyberspace depends primarily on the degree of protection of

fundamental rights, freedom of expression, personal data protection and the right to privacy. At the same time, what is underlined, is the importance of introducing the requirements of transparency and accountability.

Open and free cyberspace removes social and international barriers, allows the exchange of cultures and experiences between countries, communities and individuals, enabling interaction and exchange of information and, consequently, knowledge, experience and technology.

The general definition of the concept of security as the state of peace, harmony, and undisturbed functioning always refers to various manifestations of human activity. In turn, the basic security attributes associated with the communication processes include confidentiality, which means that only authorized persons have access to specific data and information; then the integrity of digital content, which means that the data and information contained therein are correct, intact and have not been subjected to any manipulation. Another feature is accessibility - i.e. a rule related to the functioning of an IT system, containing the availability of data, processes and applications in accordance with the requirements of a user. The definition of the latter characteristic, i.e. "accessibility", was referred to by the now repealed Regulation (EC) No. 460/2004 of the European Parliament and of the Council of March 10, 2004, establishing the European Agency for Network and Information Security , Regulation (EU) No. 526/2013 of the European Parliament and of the Council of May 21, 2013 on the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No. 460/2004. In the latter document, apart from the concepts which included a definition of the information security, "accessibility" has also been defined[4], which means that data is available and services are fully operational. In the case of access to data, the specific element that relates to security issues is the concept of "authentication", which, according to the repealed ENISA Regulation, is a confirmation of identity of entities or users. In turn, "data integrity" meant confirmation that the data sent, received or stored is complete and unchanged, while "data confidentiality" meant protecting communications or stored data against their interception and reading by unauthorized persons. It should be noted that legal provisions strictly define the basic security conditions that should be met by the ICT system. First of all, it should ensure the confidentiality of data and information (data under certain conditions become information), but not limit their availability and integrity with other subsystems or documents. Entities providing electronic services, also in the area of communication, introduce security management technologies and procedures. However, in addition to individual solutions, systematic cross-sectoral cooperation (public sector - private sector) is becoming important. Such a need arises from the fact that cybersecurity problems are global, which is determined by the characteristics of the ICT network itself, as well as the ease of transferring information, especially after a digital conversion process.

3 Public access and security

An important condition for the operation of the unit in the network is the right of access to ICT services, and thus access to information and the possibility of its exchange. Due to the scale of impact of a digital world on social life, limited or no access to the internet, and the inability to use digital technologies put citizens at a disadvantage in life, the society - in a disadvantageous economic and economic situation, and the state - in a disadvantaged situation in dealing with external and internal threats. This rule includes the thesis that everyone should be able to access the internet and access an undisturbed flow of information. The basic element of the principle of access for all is a guarantee of integrity and internet security. Such position requires a definition of the legal conditions for the provision of telecommunications services, in particular, a universal service, access to ICT services and provision of electronic services.

In connection with the global approach of deregulation in the area of ICT networks, it is accepted that cyberspace should not be controlled by one entity. There are a number of commercial stakeholders and NGOs which are involved in the ongoing management of the internet resources, protocols and standards, as well as the future development of the internet. The EU assumes a stand that participation of all the interested parties in the current internet governance model is the best way to ensure network security and multilateral management model most relevant to the regulatory needs in cyberspace. Considering the range of the ICT network, it is believed that such a model allows for greater control, reliable supervision and joint responsibility. However, huge dependence on the information and communication technologies in all areas of life has led to the emergence of weak points that need to be properly identified, thoroughly analyzed, removed or neutralized, which seems only possible at the level of the state and its national system, which does not exclude the situation of joint operation of the public and private sectors, as well as the activity of individual citizens (self-regulation), which will allow to provide protection, and when it becomes necessary, to introduce coordination. In this case, there is a question of the organizational and legal model of cooperation between the public and private sectors.
Due to the fact that networks and ICT systems mainly constitute a private property, it is necessary to combine public and private sector activities to increase cybersecurity. The strategy assumes that the private sector will develop its own cyber resilience capabilities at the technical level and ensure the exchange of best practices between individual industries. Self-regulation and practical codes containing instructions on how to respond to incidents, identify causes and conduct forensic analyzes appear to be an important element of these activities. According to the European Commission, the public sector should benefit from these experiences. In the conditions of technology development, it seems necessary to work on new solutions that would minimize or eliminate the state of threats. It is also necessary to have a procedure to exchange information on the state of threats and their effects, as well as to be more aware of the costs associated with innovation that would allow to counteract threats.

Therefore, carrying out legislative activities in which entities operating in many key areas (energy, transport, banking, stock exchanges, technologies enabling the provision of key Internet services, as well as public administration bodies) assess the threats to cyber security to which they are exposed, ensure the reliability and resilience of networks and information systems using appropriate threat prevention strategies, and exchange information with relevant network and information security authorities. Privacy protection is becoming one of the key issues in the area of regulation. Public-private partnership, apart from the form of entrustment, is primarily a form of supporting the implementation of public tasks, especially in the provision of services with participation of a public and private entity. This type of partnership is a modern instrument of public authorities serving to fulfill its obligations towards society. The concept of joint implementation of tasks by the public and private sectors, especially in rapidly developing fields, is an attractive way to achieve the set goals. Even if the planned activity is not profitable, thanks to remuneration, a public-private partnership may be attractive to a private entity and at the same time, be an effective solution for achieving public interest objectives. Current budget funds allocated for the implementation of the tasks of public authorities constitute the financial basis for a public-private partnership. At the same time, the use of the private sector infrastructure, professional knowledge and human resources at the disposal of public sector entities to implement public tasks may contribute to reducing the public costs and achieving the intended goal by means of modern means (also innovative management methods, and image-related activities).

4 Strategic priorities and actions towards cyber security

The main strategic goals include: protection of the internet environment by ensuring freedom and security. If it is assumed that solving problems related to security in cyberspace is primarily the task of the Member States, there is a need to specify priorities, which include a number of instruments: achieving resilience to cyber threats, radical reduction of cybercrime, developing a defense policy and developing capabilities in the field of cybersecurity in conjunction with the common security and defense policy, expanding industrial and technological resources for cyber security, and establishing a coherent international cyberspace policy for the European Union and promoting fundamental EU values[5], including respect for the right to privacy and identity of an individual.

One of the basic elements of the strategy is to increase resistance to cyberthreats in the area of cybersecurity. The positive results achieved in the scope of the past experience form the basis for further planning of regulatory initiatives at the EU level that can counteract cross-border cyber threats and help respond in a coordinated manner in emergency situations. In line with the strategy, these activities will strongly support the smooth functioning of the internal market and increase internal security in the EU. The European Commission has expressed the need to increase resources and streamline the

procedures used by public and private entities to prevent, detect and manage incidents in the area of cybersecurity. To coordinate these activities a policy on the *Network and Information Security* (NIS) has been developed and in 2004 a European Agency for the Network and Information Security (ENISA)[6] was established. Elements of these activities are Directive (EU) 2016/1148 of the European Parliament and of the Council of July 6, 2016 on measures for a high common level of security of the network and information systems within the Union (NIS) and of July 5, 2018 on the national cybersecurity system[7].

The network and information security is increasingly more important for the economy and the whole society. Ensuring the network and information security has become an important condition for creating a reliable environment for the provision of digital services. Incidents are becoming more and more serious and global. However, the future of legislative solutions touches on very sensitive issues related to the freedom and privacy of an individual. Therefore, the issue to be resolved will be the importance of the public as well as of the individual interest. Undoubtedly, creating mechanisms of regulation related to cyberspace while maintaining an open, free and secure virtual environment is a challenge on a global scale, which also conditions differences in the traditions of understanding the right to privacy. The issues indicated here mean that questions about the place of regulation and its scope, and even about the level of setting its goals remain valid. This dilemma also touches on the issue of the responsibility of the state for tasks related to maintaining balance between the need to ensure the security of an individual and the community, privacy and identity of an individual and protection of the national security, based on the community-specific axiology and universal values related to fundamental rights and freedoms.

Notes:

[1] In the judgment of 20 June 2005, the Constitutional Tribunal emphasized that the manifestation of the right to privacy is also the freedom of communication, including not only the secrecy of correspondence, but also all kinds of interpersonal contacts, file no. K 4/04, OTK-A 2005, No. 6, item 64.

[2] See the judgment of the Supreme Court of 19 January 1981, III CRN 204/80, LexPolonica No. 318288; the judgment of the Supreme Court of 25 May 1982, IV CR 129/82, LexPolonica No. 321197; the judgment of the Supreme Court of April 15, 2004, IV CK 284/03, Lex No. 176084; the judgment of the Supreme Court of 24 June 2019, III CSK 267/17, Lex No. 2684205; judgment of the Court of Appeal in Katowice of March 7, 2019, I ACa 752/18, Lex No. 2693895; judgment of the Court of Appeal in Warsaw of February 1, 2019, V ACa 44/18, Lex No. 2635004.

[3] Communication from the EU Commission of 7.2.2013 (JOIN (2013) 1 final).

[4] Access - within the meaning of Directive 19/2002 EC of the European Parliament and of the Council of 7 March 2002 on access to electronic communications networks and associated facilities and interconnection (DD) - did not mean access provided to end users / subscribers, only provision of devices and / or services to another enterprise, under strict conditions, to provide electronic communications services, including access to virtual network services.

[5] In 2001, the Commission adopted a communication entitled "Network and Information Security: Proposals for a European Approach" (COM (2001) 298); in 2006, a secure information society (COM (2006) 251). In the period from 2009, the Commission also adopted an Action Plan and Communication on Critical Information Infrastructure Protection (CIIP) (COM (2009) 149, approved by Council Resolution 2009 / C 321/01, and COM (2011) 163, endorsed by Council Conclusions 10299/11).

[6] The Council and Parliament are currently negotiating a new regulation to strengthen and modernize its mandate.

[7] The act on the national cybersecurity system - Journal of Laws of 2018, item 1560.

Chapter II

Regulations Related to the Protection of Privacy in the Cyber Security System

1 An individual - a citizen as a subject of the right to privacy and identity and administrative and legal obligations

Changes in telecommunication and computer science are a basic factor influencing transformations in the private sphere of a human. Introduction and application of new information and communication technologies is of great importance for the functioning of the state, its organs and the entire society. Currently, knowledge and information are considered the most important factors for the development of society. Data processing, collection and storage (Big Data) is the main purpose and task not only of entrepreneurs, but also of the state. Data that is a subject of processing or marketing is often the main element in achieving important public goals. Currently, the public sector is expected to settle matters through innovative and modern activities under the so-called e-services. In the mid '90s, of the twentieth century, the Internet ceased to be a technological novelty and became an important place of providing services to public entities, entrepreneurs and private individuals. Due to the nature of the use of data and information, distressing phenomena for the private sphere of an individual can be noted. Changes related to new technologies require a redefinition of basic concepts, as well as the identification of entities responsible for ensuring the security of an individual, his/her privacy and identity. These two categories of phenomena affecting the functioning of individuals and nations - technological development and security constitute two main areas of regulation. A characteristic feature of these two zones of influence is that they condition each other, because without security, one cannot speak of development, which in turn determines both situations of new threats and ultimately enables a better sense of security (Koziej: 2011:18).

1.1 Axiological and legal bases for identity protection - Security and human rights

Security is interdisciplinary. We can assume that security is the primary need of a human and social groups, and also their most important goal (Stańczyk, 1996:18). It is a value whose the achievement is the basic duty of public authorities. It is an important instrument for ensuring material and spiritual values. It stands above various socio-economic, historical and cultural aspects of activity of an individual and of the state. According to Kuźniar (1996), it is the primary, existential need of individuals, social groups and finally, states. It is not only about survival, integrity or independence, but also about the security

of development, which ensures protection and enrichment of identity of an individual or a nation. Most often, security is defined both as a state (a sense of security achieved by a given subject) and as a process (ensuring a sense of security of a subject). For considerations contained in this part of the work, however, the second approach seems more useful, since it reflects the natural, dynamic nature of the phenomenon of security. The subject of security may be all individuals having their own interests and expressing ambitions to pursue these interests. They can be individuals, various social groups, nations, international communities and finally, all humanity. Accordingly, we can distinguish various categories of security: individual (personal), group (ancestral, tribal), national, public, international (regional, global) (Koziej, 2011:18). As W. Kitler (2013:18) rightly notes, the most perfect form of securing the needs of man (an individual) and social group in the area of security so far is the state. In the context of security, it is the state that is to watch over external security, as well as internal order. State security refers to the security of its institutions and organizations, the established territory, as well as the population subject to power. State security is about maintaining order in the state community and ensuring its internal and external security. This is the task of a public authority.

The relationship between an individual and a public authority has been and is a subject of many philosophical, sociological, political and legal considerations, just like the idea of freedom and human rights, which, as it has already been pointed out, was conceived along with the development of civilization in modern Europe. This development was influenced, among others, by Judeo-Christian ethics referring to inherent dignity, Greek philosophical current and the Roman law. It should be added here that although the Greek law did not contain wording on civil liberties (Jellinek, 1921:174), an individual had independence of action. W. Kawka (1939:5), a classicist of the Polish administrative law, emphasized that antiquity did not recognize human personality directly, but by citizenship. "The attitude of an individual to the state has always been shaped for the sake of the state, and because the sphere of freedom of an individual was not strictly legally defined, so on this basis one can speak of its omnipotence. Such an attitude of an individual towards the state was justified by the Greeks' view of the state and society at that time (Kawka, 1939:5)".

Nowadays, the relationship between security and human rights has a special dimension shaped by modern technologies. "Security and human rights are situations in which we face great responsibility. I know how painful this tension between them is, how they get in the way of one another and how they exclude each other. For example , *I can almost see the checkpoints* and the wall separating the Occupied Territories from my home in Jerusalem. I understand what the checkpoints are for *and* I accept the arguments of the supporters of the wall, but I know that for Palestinians it is humiliation, a violation of their rights." This is how an Israeli writer Zeruya Shalev speaks in an interview with Paweł Smoleński (2013:26) on the topic discussed in the book "The remains of love". This particular conflict of values related to civil rights and freedoms and the need to

ensure security is significant not only in situations related to an armed conflict. This relationship is important in every situation when the task and public goal of the state is to ensure the security of an individual, a nation, society - citizens. In all circumstances related to the state's obligations towards an individual, his/her fundamental rights are to be considered. The regulation related to the obligations of the state affects the legal situation of an individual, in this space which, by definition, requires constant analysis in terms of protection of the system of human and citizen rights and freedoms, including the right to privacy and identity. The legal situation of an individual – citizen[1] consists of a set of rights and obligations set by legal norms and decisions of administrative bodies. In this area of research, the sphere of human constitutional rights and obligations should be separated from the rights and obligations of a citizen in the executive sphere of the state. It is at the interface of these two different relationships that the value of individual rights and freedoms is established. Human rights and security are a very current dilemma in the world of developing new technologies and digitization of the human life.

Rights are the state's obligations to act on behalf of an individual. These rights are referred to as positive rights. Freedom, on the other hand, is a sphere of human activity in which public authority must not interfere. Hence, negative rights are often used in reference to freedom. It was G. Jellinek as the author of the "status theory" that initiated a discussion on public subjective rights. In his opinion, these rights arise from the relationship of an individual with the state and are determined by constitutional law, however, an individual can act completely freely within the limits set by the state.

Under these conditions, a necessary element of observing and exercising the rights of an individual is the separation of powers, independence of courts and existence of constitutional judiciary.

In conclusion, it can be stated that human rights are a specific category of rights that everyone has as obligated to exercise them, since they are non-transferable, with the state being primarily obliged to do so. Public subjective rights also serve the purpose of exercising the rights, including the protection of privacy and its specific identity element. This is particularly important in the conditions of digitization and computerization of the state, in which the selection of instruments for identity protection has not been finally made. Two important interests are in dispute in this area: general interest, related to the need for access to e-services, public information and the possibilities of *re-using* public sector information and unitary, individual interest, which concerns the private life of an individual, his/her personal rights, dignity and the consequent protection of identity.

The catalog of human and citizen rights and freedoms is included in chapter II of the Polish Constitution. This chapter contains a general part that defines the basic principles characterizing the canon of fundamental values recognized in the Republic of Poland as the basis for the protection of a human and citizen. The set of rights is first opened by the right to dignity.

1.2 Humanity as a source of human dignity - dignity as a source of identity protection

According to the Universal Encyclopedia of Philosophy (Herbut, 1997:260), dignity is a property that stems from the existential and personhood structure due to the fact that it exists as an end in itself and for itself, and never as a means of human action (Krapiec, 2003:17). In *the Lexicon of Classical Philosophy*: "Dignity (Latin *dignitas*) is a special value of a human as a person living and being in communion with other people; also a positively valuing relation to oneself and a group with which an individual identifies himself/herself" (Chlewiński et al., 1997:260) which means that one of the elements of dignity is an individual identification, identity of an individual.

In accordance with Article 30 of the Constitution of the Republic of Poland, the inherent and inalienable dignity of the person constitutes a source of freedoms and rights of persons and citizens. It is inviolable, and its respect and protection are the responsibility of public authorities. Thus, human dignity is the basis for the functioning of the state, the actions of public authorities but also a directive for each regulation, according to which all other rights and freedoms, including the right to the identity of the individual, are determined. Therefore, according to P. Winczorek (2003:83) it should be assumed that "the philosophical basis of the constitutional norms concerning freedoms and rights of a human and citizen is the thesis according to which they are not established by the legislator's imperious ruling, but are merely declared by him", which is confirmed by Art. 30 of the Constitution of the Republic of Poland, and this approach results from the naturalistic direction of thinking about legal sciences. This position is shared by W. Zakrzewski (1998:167), according to whom "human rights are a qualified form of the rights and freedoms of the individual, to protect his/her interests, assigned to every human person, regardless of nationality and any differentiating features". According to this author, the source of human rights is not the state and the legal system but the law of nature, according to which the basis of individual rights is inherent dignity. This position of the right to dignity among other rights and freedoms gives all human rights supranational, inalienable and inviolable character. This applies to both to the issues related to a regulation at the legislative level, as well as to all areas, stages and forms of functioning of a public authority in the executive aspect. Therefore, the inherent character and inalienability of human dignity should be seen in the context of natural rights.

Identity is derived from human dignity. It should be noted, however, that dignity is a key element in ensuring national security in the aspect of protection of human and civil rights and freedoms, while identity as a derivative of dignity is the element which in certain situations will be subject to restrictions dictated by the reasons of ensuring this security. Unlike the national identity, which carries the imperative of a higher good, as does the public interest in relation to other rights and freedoms, e.g. freedom of speech. Rights derived from the right to dignity are natural rights, thus protection of identity of the individual is a public subjective right. This last principle is particularly important for the

assessment of protection of identity in a relationship of an individual and a public authority.

The principle of inviolability of dignity, in turn, implies a ban on taking any actions aimed at violating or even limiting dignity. As B. Banaszak (2012:172) notes, "public authorities are not only obliged to respect it - i.e. not to violate it with their actions, but also to protect it - i.e. to create a system of procedures, legal orders and prohibitions preventing all violations of and threats to dignity". Analyzing the principle of the inviolability of the human dignity, the Constitutional Tribunal, in the judgment of the Constitutional Tribunal of April 4, 2001 stated: "[...] the obligation to respect and protect dignity has been imposed on the public authorities of the state. Consequently, all actions of the public authorities should, on the one hand, take into account the existence of a certain sphere of autonomy, within which a person can find full social fulfillment, and on the other, these actions cannot result in a creation of legal or factual situations which deprive the individual of a sense of dignity" (Borski, 2014:15).

1.3 Identity - what does it mean?

The concept of identity, also in the conditions of development of new technologies, raises interpretation doubts. We speak of identity in various meanings of this term. According to the Polish Language Dictionary (Słownik Języka Polskiego), identity means "being the same; sameness" (Doroszewski, 1968:832). According to M. Domańska (2019), we can talk about the identity of the individual that every human has and on the basis of which he/she builds the foundations of his/her individual dignity. M. Flis defines the concept of identity as "(...) a set of ideas, judgments and beliefs that the subject constructs towards himself/herself, i.e. the system of self-definition of a social actor." This term is associated with a set of features that allow one to identify, recognize a person or a group of people. Determining someone's identity is to recognize the specific characteristics of a person (but also of a group - in the context of the national identity), which distinguish this person (a group - in the context of the national identity) from others. The function of identity is therefore to identify a person or a group based on having a certain number of attributes. R. Coomaraswamy (2002:483) assumes that identity is not essentially invariable, because it is a composite consisting of many independent, often competing, contradictory and transformable criteria. That is why identity often changes, also in response to the reaction or variability of ideologies and under the influence of life experiences. It is also emphasized that identity of the individual is relative to identity of other individuals. According to M. Domańska (2019), it cannot be ruled out that "the ambivalent sense of belonging to a particular group is an overinterpretation of a certain process of shaping identity of the individual. Such inconsistency of a hybrid identity may already appear on the simple combination of sex and religion when the individual identifies with members of a religious group, but at the same time his view of the role of a woman in the life of this group remains inconsistent with the vision of himself. Therefore, an illusion of a certain whole, as a value fulfilling a definition of an individual's identity, will not always

be an identification value for this individual, because it should be created simultaneously based on life experiences and shape identity on the basis of self-determination" (Domańska, 2019).

In the judgment of the Supreme Court of June 6, 2003, the court defined the concept of identity assuming that in the wording of Art. 13, clause 2 of the press law [...] personal data referred to in this provision should be understood as any information enabling identification of a protected person. These include not only information about name and surname, date and place of birth or place of residence, but also other information regarding, for example, family relationships, occupation or place of work, which enables identification of a person in a given environment".

The issue of the right to identity can be considered primarily in the context of violation of personal rights. The catalog of personal rights defined in Art. 23 of the Civil Code is open, and the scope of application of this provision covers all personal rights understood as certain intangible assets related to the existence and functioning of civil law entities which in social life are considered important and deserve protection. Personal rights are certain intangible assets widely recognized in society and closely related to man, determining his/her individuality and distinctiveness. Revealing identity of a person involves violation of his/her personal rights. Pursuant to the judgment of the Appeals Court in Warsaw of July 8, 2009 the publication also contained true information, name and place of work of the plaintiff, although the plaintiff did not express consent to their publication. [...] there was a violation of the plaintiff's personal interest in the form of his name and surname, as well as in the form of making public the information about the plaintiff's private life (the manner of spending his free time). Although the information was true, the defendant's action had to be considered unlawful. [...] providing full personal details of this person enabled his identification by people who knew him - his family, friends and neighbors".

According to A. Wilk (2014), the concept of identity in the legal sense should also include the psychological basis of its comprehension. In psychological terms, it is defined as knowledge about oneself, the individual's conviction about himself/herself. Another definition is the biographical self-awareness of man. J. Kozielecki (1981:313) claims that identity and self-knowledge create a complex relationship - a self-image, i.e. the so-called self-knowledge. M. Jarymowicz and T. Szustrowa (1980:442) define identity as "awareness of one's own coherence in time and space - in various periods of life, social situations and roles, as well as awareness of one's distinctiveness, individuality and uniqueness". Psychology separates issues of identity in general from the issues of a sense of identity, which is understood as a sense of an individual existence. Similarly, there is a separation between security and a sense of security. The sense of identity in psychology is characterized in four aspects:

1) the sense of distinctiveness from the environment;
2) the sense of continuity of "own self;

3) the sense of internal consistency;
4) the sense of having internal content (Mandrosz-Wróblewska, 1988: 28-28).

Identity differentiates, if only through biographical data" (Gałdowa, 2000:29). The psychological approach to the right to know one's own identity, including biological identity, therefore, seems to differ from the approach to this issue from the point of view of protecting the rights of the individual who wishes to exercise such a right. It can be assumed that name and surname describe both the individuality of a person and his/her relations with the community, mainly with the family. The name is in a sense a symbolic act of giving identity, while a change of name may be associated with an attempt to change identity (Wilk, 2014). At the same time, it should be noted that, as Hannah Arendt writes, it is with their action and speech that people show who they are, revealing their unique identity, while appearing in the human world. In a word, it is our actions, the way of thinking and articulating our thoughts define our identity as a protected good.

2 The individual - a citizen as a subject of the right to privacy and identity and administrative and legal obligations

The individual's situation in the context of his/her personal rights and obligations includes both obligations, which may include the above-mentioned personal rights and freedoms, listed in the catalog of the Basic Law, as well as a number of other rights and freedoms that have not been explicitly and directly specified. The basic right is the right to life and personal freedom. These include the right to physical integrity, the right to integrity of the place of residence, the right to secrecy of communication and sharing information about oneself (the information autonomy already mentioned before, expressed in Art. 51 of the Polish Constitution), the right to a family life. These are just a few rights and freedoms from the broad catalog of rights and freedoms that relate to the private sphere of man. The administrative law refers to these rights and freedoms by granting competences to specific administrative bodies including obligations and rights towards the individual - a citizen. The limits of the rights and freedoms of the individual - a citizen are evidenced by the scope of public administration rights determined, as already indicated above, in competence norms, as well as the scope of obligations of the individual - a citizen, which relate to personal rights and freedoms.

Summing up the legal status of the individual - a citizen in the context of his/her privacy and identity protection, it should be stated that in Art. 47 of the Constitution, two separate situations have been regulated: firstly, the individual's right to legal protection of the spheres of his/her life indicated in the first part of the provision, and secondly, the freedom to decide on matters set out in the final part thereof. The first right of the individual must be accompanied by a statutory regulation that defends privacy, family life, honor and good name. On the other hand, the second right means prohibition of interference into the freedom of the individual shaping his/her personal life. This freedom is also one of the manifestations of the general freedom of man expressed in Art. 31, clause 1 of the Polish

Constitution and personal freedom in the strict sense, guaranteed by Art. 41, clause 1 of the Polish Constitution. Both constitutional norms contained in Art. 47 of the Polish Constitution are commonly referred to as the "right to privacy".

The right to personal integrity includes the physical and spiritual integrity of the individual (Complak, 1998:45). When we talk about personal rights and freedoms, we also mean the right to privacy. The right to privacy is a personal right protected in the national legal order, a constitutionally protected right (Art. 47 of the Polish Constitution) and in the international order (Art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, drawn up in Rome on November 4, 1950). The right to personal freedom and the right to privacy contained in Art. 47 of the Polish Constitution, however, are not absolute values, if it is supported by another norm, principle or constitutional value, and the degree of this limitation remains in proportion to the rank of the interest that the restriction is intended to serve (Sokolewicz, 1985:252).

The freedom expressed in Art. 41, clause 1 of the Polish Constitution, guarantees everyone personal integrity and personal freedom, with the provision that deprivation or restriction of freedom may only occur on the terms and in the manner specified in the Act. It is characterized as the ability for an individual to make decisions in accordance with his/her own will, to make free choice of conduct in the public and private life, unrestricted by other people. Freedom of the individual - in the light of the constitutional standards in force - is perceived as the fundamental value of a democratic society, due to the individual by nature, indisputable and inalienable, which is the source of development of their personality, personal well-being and social progress (Sarnecki, 2003). In a democratic state ruled by law, freedom is protected in a special way, including the freedom of private life and the autonomy of choices made, as one of the fundamental principles of the modern human rights doctrine, entrusted to special protection of the State.

According to the jurisprudence of the Constitutional Tribunal, the importance of the right to privacy in the system of constitutional protection of rights and freedoms is highlighted, among others by the fact that this right is - in accordance with Art. 233, clause 1 of the Polish Constitution - inviolable even in the event of a state of emergency or martial law. This means that even such exceptional and extreme conditions do not allow the legislator to soften the premises under which one can enter the sphere of private life. Undoubtedly, the norms limiting these rights and freedoms should be regulated at the statutory level. Respect for privacy is closely linked to the constitutional order to protect human dignity (Art. 30 of the Constitution). Man's dignity requires respect for his/her purely personal sphere, so that he/she is not exposed to the necessity of "being with others" or "sharing" his/her experiences or intimate experiences with others. The private sphere is built of various circles that are more or less open (legally) to external influence and constitutional approval for imperious entry by the authorities is not the same. One of the manifestations of the freedom of the individual is "the right to decide about one's personal life", referred

to in Art. 47 of the Constitution, indicated as the second basic constitutional model. This provision also guarantees everyone the right to a legal protection of private life. Privacy, understood as the right to "live one's own life, arranged according to on e's own will, limited to the necessary minimum of all external interference", refers, among others, to one's personal life (and thus also the identity of the individual) and is sometimes called "the right to be left alone". Speaking of the right to protection of a private and family life, honor and good name, and to decide on one's personal life, the Polish Constitution prohibits the state from interfering with the private life of the individual, but also imposes positive obligations on the state. It also means that as part of its obligations, also related to ensuring security, the State may impose various obligations on the individual - a citizen.

2.1 Civil status

The basic obligations of the individual - a citizen include the obligation to register the characteristics determining the civil status and thus the legal situation of the individual, affecting the identification to his/her identity (birth, marriage and death), regulated in the Act of November 28, 2014 – the Law on the Civil Registry Records. Supervision over the registration of a civil status is exercised by the minister competent for internal affairs based on the principles set out in separate regulations. Voivodes supervise the activities of civil registries in the scope of fulfilling their obligations set out in the Act. Incompatibility of the files with the facts can be proved only in court, in non-contentious proceedings for their annulment, correction or determination of content. Public administration bodies shall provide the civil registries with copies of administrative decisions affecting the content or validity of a civil status certificate within 7 days from the date on which the decision became final, with the exception of administrative decisions on a change of name or surname, which are transferred pursuant to the Act of October 17, 2008 on a Change of Name and Surname. The register of civil status is kept in the ICT system, and the maintenance and development of the register of civil status, in order to implement the tasks specified in the Act, is provided by the minister competent for computerization, including: 1) providing protection against unauthorized access to the register of civil status; 2) ensuring data integrity in the register of civil status; 3) ensuring availability of the ICT system in which the register of civil status is kept for entities processing data in that register; 4) preventing damage to the ICT system in which the register of civil status is kept; 5) setting out the rules for the security of the processed data, including personal data; 6) setting out the rules for reporting a breach of personal data; 7) ensuring accountability of activities carried out on the data in the register of civil status; 8) ensuring the correctness of the data processed in the register of civil status.

2.2 Obligation to register identity

Another obligation of the individual citizen is the population register and related registration of elements of individual citizen identity. This issue has been regulated by

the Act of April 16, 2004 amending the Act on the Population Register and Identity Cards and then the Act of September 24, 2010 on the Population Register. Pursuant to Art. 2 of the Act, the population register consists of registering the basic data identifying the identity and administrative and legal status of natural persons specified in the Act, while the population register is kept in the Universal Electronic System of the Population Register, which is the PESEL register, and in the registers of residents kept in the ICT system. According to W. Maciejko (2016), the phrase "identity identification" was placed by mistake, since only a natural person can be identified, and this can be done through the process of getting to know his/her identity. The essence of the status of the administrative law is that it does not involve designation of a natural person in the legal circulation required by the regulations of the private law (in particular the civil law). Therefore, it is not admissible to state that the identity of a person recorded in the population register translates into his/her civil law status (e.g. the resolution of the Supreme Court of November 17, 2009, III CZP 89/09, OSNC 2010, No. 5, item 71, states that the PESEL number may facilitate identification of a person in civil law transactions). According to this author, the population register is used to determine the identity and spatial location of a natural person. It is, apart from civil status acts, a basic legal instrument defining a citizen as a party to the legal relationship of citizenship. The exceptions include the use of the PESEL number to implement the obligation under the regulation of the private law. Such an exception is the labor law obliging the employee to disclose the PESEL number to his/her employer (see the judgment of the Supreme Court of August 5, 2008, I PK 37/08, OSNP 2010, No. 1, item 4). Similarly, P. Mierzejewski (2013) assumed that the use of the term "identifying identity" in the above provision is an obvious misunderstanding, since it identifies a specific natural person and not his/her identity (e.g. by means of a document issued by the authorities with materially recorded data identifying a given person).

2.3 The right to possess a passport

One of the rights regarding identity of the individual is the right to receive a passport. In accordance with Article2 point 1 of the Act of July 13, 2006 on Passport Documents, the biometric data is the image of the face and fingerprints placed in passport documents in an electronic form. Preparation of a passport document means the transfer of personal and biometric data of the applicant for a passport document to the passport book in a graphic and electronic form. The passport document entitles one to cross the border and stay abroad and certifies Polish citizenship, as well as the identity of the person indicated in it in terms of the data it contains.

The person collecting the passport document checks by means of an electronic reader whether the personal and biometric data contained in this document are consistent with the facts. It should be emphasized here that in the area of the rights and freedoms of the individual - a citizen it is guaranteed, among others that everyone has the right to leave

any country. Therefore, any ban on leaving the state is tantamount to the interference with this right by public authorities. This also applies to the situation of a passport retention.

2.4 Public trust services and threats to the identity of the individual

Digital transactions, just like traditional ones, need the creation of instruments which guarantee the correct identification of the transactions participants. At the same time, these transactions can affect the protection of the participants identity. In the traditional solution, such an instrument is an identity document, which has a material form. In turn, in the digital transactions, a replacement of an identity document is an electronic identification means, i.e. an intangible or material entity that contains person's identification data and is used for authentication for an online service. A very important area regulated by the Regulation (EU) No. 910/2014 of the European Parliament and of the Council of July 23, 2014 on electronic identification and trust services in relation to electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS) are trust services. eIDAS lists several types of trust services, including the creation of electronic time stamps, electronic signatures, electronic seals, and website authentication services. A trust service is an electronic service usually provided for remuneration, which includes:

- verification, creation and validation of electronic seals, electronic signatures or electronic time stamps, registered electronic delivery services and certificates related to these services;
- verification, creation and validation of website authentication certificates;
- maintenance of seals, electronic signatures or certificates related to these services.

Trust services play a very important role in the electronization of legal transactions. They allow documents to be delivered and produced initially in an electronic version. The first trust service discussed is an electronic signature. According to the dictionary definition, "signature" means name and surname, less often an emblem, initials, handwritten by someone; an inscription placed under a drawing, photo, graph, etc. explaining its content; confirmation of a letter by placing one's own name on it. An electronic signature is a string of characters identifying the customer (sender), encrypted with a digital key.

The operation of public administration today requires the use of new methods and techniques of communication. Using conventional instruments loses with "new technologies" and does not always ensure efficiency in terms of speed and universal access. In contacts and relations with the administration, a (secure) electronic signature becomes very important, which undoubtedly facilitates the flow of correspondence but also speeds up the circulation of documents. This takes place thanks to an appropriate level of computerization of the office that serves a specific administrative entity (Chałubińska-Jentkiewicz & Karpiuk, 2016:265). Today, most important matters are handled electronically. New opportunities save time, make life easier and contribute to greater openness and transparency of activities. The Internet, which is a tool for building

an information society, is the cause of revolution in many areas of life. However, each revolution has negative consequences, i.e. threats related to the use of electronic services. They mainly concern the issues of personal data protection as well as information related to private life. Issues related to access to data contained in public registers are only a fraction of the negative phenomenon, which is constant deprivation of privacy of individuals by both the network users and public administration. Computerization processes, lack of proper safeguards and procedures do not favor this protection. We live in conditions of mass tracking, under which both private and public institutions collect data on individuals at an unprecedented pace (Angwin, 2014:20). The public sector, even if it does not contribute to this process directly, is actively involved in it through the use of infrastructure, which most often belongs to private institutions. Cloud computing that is supposed to store public sector data, but also archival data and public sector information, does not guarantee security. The costs of producing digital objects are very high, which is emphasized by all institutions digitizing their resources all over the world. Currently, the costs of long-term and secure storage of digital data are rarely included in the digitization processes. Therefore, it seems necessary to maintain access to older resources by implementing effective archiving strategies, including perpetual archiving and proven storage formats. In order to provide Polish digital resources with protection and security, one of the most urgent needs is to build a network of secure data warehouses and digital repositories that will store two basic categories of objects - collections after digitization and digital documents - born ##digital. The critical element in building systems is the right formulation of security requirements. Three basic groups can be considered as security pillars in the ICT systems:

- Administrative and procedural security - development and constant supervision over the adopted security policy, strict definition of the scope of responsibility, and support for all technologies used and solutions with appropriate procedures describing the principles of their correct and safe functioning.
- File and transmission security - ensuring reliable mechanisms of data confidentiality both stored on carriers as wall as transmission security, e.g. by creating a separate secure telecommunications infrastructure or ensuring confidentiality mechanisms in the application layer.
- Secure mechanisms of access to resources - mechanisms of access control, isolation, segmentation, protection of interconnection contacts, ensuring strong mechanisms of user identification and authentication.

3 The importance of digital processes in legal protection of identity

The information revolution, which began in the seventies[2] of the last century, changed not only thinking about the economy, but above all individual behavior and needs. Information has become an important value, which is the subject of legal protection, is often an important asset of an enterprise, is important for national security reasons, and is also an important instrument in the operation of public authority. Contemporary society is often called the information society (the information economy is one model and there

is no division into its national or regional variations) or cyberspace (it should be noted that cyberspace is a place that can be considered in various aspects: technological, social, economic and legal, but it is also a space that is used in public administration activities). Technical changes that have taken place in recent years and their consequences have influenced the quality of life of the individual, whose expectations of public authority have been radically focused on the development of new technologies in every sphere of life. Cashless transactions were introduced on a large scale, the banks' operations, including accounting systems, were computerized. Proportional to the development of new technologies, there are completely unknown threats to the sense of individual and community security. In a Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, entitled "The European Union Cyber Security Strategy: an open, secure and protected cyberspace" (of 7 February 2013 (JOIN(2013)0001), the European Commission emphasized that "in cyberspace, protection of fundamental rights, democracy and the rule of law should be ensured. Our freedom and our prosperity are increasingly dependent on an efficient and innovative Internet, which will continue to play a key role if the private sector and civil society continue to stimulate its development. However, freedom in the online environment requires security and protection. It should be protected from incidents, harmful activities and abuse, with the governmental administrations playing a significant role in ensuring free and secure cyberspace. They have a number of tasks: ensuring access and openness, respecting and protecting fundamental rights on the Internet, and maintaining the reliability and interoperability of the Internet". Different terms are used to describe the new digital civilization. It can be assumed that the information society is one that possesses technical, legal and economic instruments, but above all it has information knowledge that allows to use these instruments. The overall changes taking place in the world related to globalization and the digital process create new situations in which the individual must operate to effectively achieve their goals, new needs related to the changes of living conditions. Thus, the scope of functions that the state should fulfill in relation to society is increasing. The need for these transformations does not only have a technical aspect, it is also a process of changes in social mentality, which seems to be the most important and the most difficult to implement, it is the need to change the standards of the relationship between the individual and public authority; the citizen and the state, and finally the need for education, including the implementation of such important public tasks as: developing e-skills, obtaining economic and strategic benefits related to digitization, preventing social exclusion. This last task in contemporary development conditions is identified with the concept of social inclusion, and applies to those individuals or social groups that are not sufficiently prepared to function in the information society. As a consequence, the digitization of the private sphere affects the security of the individual in the context of protecting their privacy and identity.

Adequately to the digitization of the private sphere, this process is also subject to the public sphere. The computerization process is also a significant change in the relations of administrative bodies, and consequently in the relations between clerk and clerk. One can

speak here about the computerization of public tasks and, consequently, public services. The basis for the computerization of public services is the appropriate legal environment, new regulations keeping pace with the principle of proportionality, social and technological changes that create the first. Each current and future strategy that defines the assumptions of computerization policy should be subject to periodic updating, which seems necessary due to the pace of development of applied technological, organizational and social solutions in every area of life, and consequently also in public administration. Therefore, it should be assumed that computerization is a space for public administration in which the use of technological progress and digitization processes is the basic way of implementing public tasks and services.

3.1 Homo interneticus

Privacy in cyberspace is the ability to maintain data as well as personal habits and behaviors not disclosed publicly. Currently, as a result of new trends, media activity and in conditions of conflict of values, one should consider whether the term identity has lost its original meaning, and above all, whether we can still talk about the existence of identity protection. Technological development is largely connected with social media, and these have become an important element of our lives. In addition to entertainment and acquiring information on the web, we also create our image - by publishing photos and content. Digital reality, in which we are never anonymous, has changed thinking about privacy and its limits. The German researcher Spiros Simitis in 1985, when the possibility of automatic data processing still seemed to be a problem, emphasized that privacy is not an end in itself. It is a means to achieve the ideal of a democratic political system in which citizens are treated as more than information providers for all sighted and all optimizing technocrats. S. Simitis warned that when privacy disappears, both the chance for an independent assessment of political processes and the opportunity to develop and maintain one's lifestyle disappear. Perhaps maintaining personal and also national identities. Today, based on the analysis of only telecommunications data (for example, information about who connects with whom and when and in what location it is located) one can predict individual behavior. On the basis of what content has been "liked" on the internet, it is possible to determine racial origin, intelligence level, sexual orientation, addictions or political views of network users. Disclosed information on PRISM software in 2014 by the Washington Post and Guardian US raised questions about the security of private material published online. The materials reached public use thanks to reports of Edward Snowden - a former employee of the US Intelligence Agency. In June 2013, the American newspaper The Washington Post and the British newspaper The Guardian described the secret intelligence program PRISM, which has been in operation since 2007, based their findings on documents provided by Edward Snowden, a former employee of the Central Intelligence Agency (CIA) and the National Security Agency (NSA). The purpose of the disclosed program was to allow US special forces to access all data on servers of Internet service providers (including Microsoft, Yahoo, Google, Facebook, Skype, YouTube and Apple), including collecting information about users.

Thanks to PRISM, access to everything we publish on the web has been obtained; audio video recordings, photos, conversations, e-mail and other data of users using services belonging to these corporations. In the case of PRISM, the fact that most of the data went through servers belonging to American companies was used. The United States has not denied the program. Reports caused a real storm and wave of accusations against the US, but US authorities defended the whole process. US Intelligence Director James Clapper has stated that the program complies with applicable law and cannot be used to deliberately monitor US citizens or other people living in the United States. PRISM's focus is on third-country nationals, and the data collected is used to protect the United States against major threats, such as terrorism.

The processing of user data is the everyday life of institutions such as Facebook or Google, which admits that it records and analyzes conversations of users of smart speakers. Recordings collected from these devices are sent directly to language specialists who work, among others over speech recognition. The issue of these wiretaps was publicized by VRT News television, which was contacted by one of Google's collaborators. VRT News was able to obtain from these conversations data related to the identity of selected users, such as name and address of residence. In a statement on the subject, Google Poland stated that *When building our products we are guided by the fact that they can serve every user - as part of this we invest in technologies in the field of speech so that they work in many different languages, accents and dialects. This allows products like the Google Assistant to understand the query, regardless of whether it is spoken in English or in Hindi. As part of the work related to the development of this technology in different languages, we work with language experts around the world to better understand the nuances and accents of a given language. These experts review and transcribe a small number of queries - so that we can better understand these languages. This is an extremely important part of the process of building technologies related to human speech and is necessary to create products such as the Google Assistant. We have received information that one of the reviewers has violated our data security principles by providing confidential audio material in Dutch. Our Security and Privacy teams are investigating this matter to take appropriate action. We also re-evaluate our security mechanisms in this area to prevent this type of violation in the future. We use a wide range of safeguards to protect user privacy throughout the entire process of viewing this data. Language experts review only about 0.2% of all audio slices. As part of this process, these materials are not associated with the user account and viewers are instructed not to transcribe conversations in the background or other sounds, but only to transcribe clippings with queries to Google. The Assistant sends data to Google only if the device detects interaction with the Assistant - e.g. after saying the command "Hey, Google / Ok, Google" or after manually calling the Google Assistant. Each time the device communicates with Google to perform a query or instruction, a clear signal appears (e.g. on the screen of an Android device or in the form of flashing dots on the Google Home housing). In rare situations, devices with Google Assistant may experience what we call "false call". This means that our software has interpreted some words or sounds as*

reminiscent of an Assistant calling command (like "Ok, Google"). However, we use many safeguards to prevent such false calls. Building products that can serve everyone is part of Google's DNA. We set high standards of privacy and security in the development of our products - and we demand the same standards from our partners. In addition, we provide users of our services with tools for account storage. Anyone can completely disable the storage of audio data on a Google Account or decide to automatically delete them after 3 or 18 months. We've always worked to explain how our privacy settings and policies work even better, and we'll look at how we can further explain how this data is used to improve speech technologies. To change or view these settings, just visit the Google Accounts page - you can also view (and delete) all of your account activity.

Due to problems with the moral assessment of this type of activities, it should be noted that innovation is not, however, an unequivocal symbol of only a positive perception of changes, because despite the increase in awareness of Internet users in the field of expansive activities of online media entering deeply into privacy and using the identity of their recipients and initial indignation and the actual change of attitudes of some users, most of them go to the agenda. Still, organizing and introducing clear rules for using the internet is a must. Just like the publication of clear and transparent information on interference with privacy, with particular emphasis on identity. Such a need, dictated by considerations of ethics and morality, is the future of regulation in the field of interactive media, especially the so-called social media.

3.2 Biological identity

New techniques and technologies not only affect the issues of identification (personal, consumer preferences, moral preferences, political views, religious beliefs or sexuality) of network users. This issue also touches on the issue of human improvement, i.e. interference with the biological identity of a human being. Therefore, this problem will always refer to the issue of dignity and morality. As it has already been emphasized, granting by the constitution-maker dignity the attribute of inalienability means that a man cannot be deprived of it, nor can he renounce it himself. This means that public authorities cannot specify the conditions for loss of dignity or how an individual should behave so that their behavior can be considered "worthy" of man and thus subject to protection (Kondratowicz-Bryzik & Sękowska-Kozłowska, 2013). It seems that in the face of numerous threats related to creativity, based to a large extent on the development of new technologies, legal regulation should be required to protect the rights and freedoms of the individual, including his dignity and morality - pursuing the same goals and personal safety and public interest objectives. It should be noted that there is a limit beyond which it is impossible to confer a scientific character on a given undertaking, and practicing science cannot be a cover for actions violating the rights and freedoms of other persons. According to this view, it becomes possible to separate the sphere of undisputed facts, which requires special protection, and the sphere of assessments of these facts, which do

not intend to question them, which seems to be crucial for assessing the situation of human privacy and his identity in the modern world.

According to recital 34 of the GDPR, genetic data should be defined as personal data regarding the inherited or acquired genetic characteristics of a natural person, obtained from the analysis of a biological sample of a natural person, in particular from the analysis of chromosomes, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) or analysis of other elements enabling to obtain equivalent information.

The Directive of the European Parliament and of the Council 98/44/EC of July 6, 1998 on the Legal Protection of Biotechnological Inventions is important for determining the content of the principle of the protection of biological identity (OJ L 213, 30.7.1998, pp. 13–21). Recital 16 of the Directive states: "Patent law must be applied taking into account the basic principles protecting a person's dignity and integrity; it is important to confirm the principle that the human body at all stages of its formation or development, including germ cells, and simply to discover one of its elements or one of its products, including the selection or partial selection of the human genome, cannot be patented". In turn, recital 40 states that: "there is agreement in the Community that interventions in the human germ line and human cloning violate public order and decency; it is therefore important that the possibility of granting a patent on methods of modifying human germline identity and methods of human cloning should be expressly excluded". The importance to this issue in European Union law is provided by these Directives: the Directive 2004/23/EC of the European Parliament and of the Council of 31 March 2004 on setting quality standards and the safe donation, procurement, testing, processing, preservation, storage and distribution of human tissues and cells (OJ L 102, 7.4.2004, pp. 48–58) and European Commission Implementing Directives: 2006/17/EC of 8 February 2006 as regards certain technical requirements for the donation, procurement and testing of human tissues and cells (L 038, 09/02/2006 pp. 40 – 52) and 2006/86/EC of 24 October 2006 as regards traceability requirements, notification of serious adverse reactions and events and certain technical requirements for the coding, processing, preservation, storage and distribution of human tissues and cells (OJ L 294, 25.10.2006, pp. 32–50) as well as Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community Code relating to medicinal products for human use (OJ L 311, 28.11.2001, pp. 67–128), in which we find confirmation of the principle of minimum and partial harmonization of European Union law, which may affect the scope of protection of human dignity in the Member States.

3.3 Anonymization and pseudonymization and identity protection

One of the fundamental problems related to identity protection is the question of whether it is possible to extend the regulation of personal data to identity protection, including that of fictitious or hidden in the process of anonymization. Anonymity on the web is as durable as sandcastles seized by the tide - they can stay in place, but they won't be what

they were before the ocean swallowed them. Many people think that sitting behind the keyboard of your computer in the comfort of your own home, with a cat on your lap, logging in with casual Nick is anonymous. It is important that you can be anyone on the Internet, but you can't not be yourself. In fact, every step taken in front of the monitor leaves a trail, after which you can track down the person who left it. Being anonymous on the Internet is technically impossible. Each action causes a reaction, even if it is not visible at first glance.

Looking at the matter from a technical point of view, anonymity and its concept do not exist on the Internet. Anonymity is commonly defined as:

- not revealing their name or unknown by name,
- one whose author or perpetrator is unknown,
- involving people unknown or indistinguishable,

This definition of anonymity is completely impossible in the field of the Internet. This is due to the numerous technical complexities that a user must meet to use the network. Everyone who has ever used the social services offered by the Internet, whether it is a Facebook account or a more advanced discussion forum, had to provide some part of their personal data. That is, they disclosed his name - to a greater or lesser extent. They recognized themself and left a mark. Technically, every computer that gains access to the network has its own unique identifier - the IP address. Of course, it is possible to camouflage the IP address by using the appropriate encryption software or a network using the so-called *onion routing.* This term defines multidimensional data encryption and sending through proxy servers called network nodes. Such activities are aimed at securing data about the sender of the information, its recipient and its content. This process gives an almost anonymous possibility of using the network by blurring the actual IP address. Hiding the IP address, however, is not a perfect method, a well-trained specialist or hacker will be able to find the original sender.

Anonymity on the web is also not legally guaranteed in Polish legislation. Of course, the user may assert their rights if these are violated, they have the right to do so under constitutional provisions, but the Polish legislator imposed a legal obligation on telecommunications service providers when it comes to collecting data on network users. These provisions are contained in Articles 180 (a) and 180 (d) of the Telecommunications Law of 16 July 2004. The provisions contained in these two Articles state that the operator of the public telecommunications network and the provider of publicly available telecommunications services are obliged to:

- stopping and storing data on the terminal device initiating the connection and the device to which it is directed, data on the location of these devices as well as on the date and time of the connection and its duration,
- disclosing data to authorized entities as well as to the Customs, court and prosecutor in accordance with separately established rules,

- protect data that they are required to obtain against accidental or unlawful breach, processing or disclosure.

When analysing this issue, it should be emphasized that anonymisation itself and thus limited identification of a person can be a way to protect privacy. There is a reasonable approach that anonymous data is less protected and therefore subject to limited regulation, although it should be noted that anonymous data may affect the scope of protection of a person's privacy, especially in the context of establishing their identity. Thus, it can be assumed that anonymisation will affect the scope of identity protection. The aforementioned identification is associated with establishing the identity, including the biological one, in which the study using genetic data is an identification process. However, this does not mean that an identified person cannot remain anonymous. Thus, the process of anonymisation relates to the process of identifying difficulties but does not exhaust the issue of identity protection. Therefore, the data may be identifiable because it enables identification, but also anonymous in the context of determining personal data, because it is necessary to distinguish identifiable data and anonymous data. Anonymisation alone does not exclude liability for the protection of personal data, nor does it limit the obligations related to the protection of anonymized data. While personal data is associated with a specific person, a change in personal data does not have to change the identity of that person. Similarly, anonymous data can shape someone's identity. A person with a specific identity but using anonymous or anonymised data is subject to legal protection in the area of privacy. Identification relates to associations with individual persons as individuals, but more and more often groups of users are identified in the network, an example of which is profiling specific consumers in a given respect. Ultimately, the determinant of protection is whether personal or anonymous data is for a particular person. Is it possible to determine their identity. Not necessarily the name and surname, as the data may not be the only identifier. Absolute anonymity is impossible to guarantee. Although individual data cannot be uniquely identified, secure connections with a specific person, the combination of a relatively large amount of data about a person facilitates identification. The data shared on the web represent a unique portfolio that allows you to construct an increasingly clear profile that fits a smaller number of people. This can be information such as name, address or national PESEL identification number - described as generally identifiable. This is because the correct interpretation enables a connection between these data elements and specific people. Certain data may be information encoded in an identifiable manner. We are then dealing with the so-called pseudonymisation, which means on the basis of the GDPR that personal data shall be processed in such a way that it can no longer be attributed to the specific data subject without the use of additional information. A parallel condition is that such additional information be stored separately and subject to technical and organizational measures that prevent it from being assigned to an identified or identifiable natural person. Thus, pseudonymisation may involve the conversion of possessed data (e.g. name and surname) into a series of letters or numbers that can be deciphered only on the basis of separately stored information (key). Unlike anonymisation, pseudonymisation is a completely

reversible process and therefore data that has been secured in this way still needs to be protected in accordance with the requirements of the GDPR.

Anonymized data either lose the nature of data protected by the Act (personal data), or remain data of a specific type, but already anonymized, which allows their processing without the need to meet certain conditions (e.g. without the consent of the data subject) or processing them for purposes other than before anonymization. As a rule, after anonymization processing restrictions are at least significantly reduced, in some areas protection is completely turned off. The electronic environment specific to the telecommunications sector is particularly conducive to anonymisation, as opposed to service or official environments in which data is processed in paper form.

The provisions of the GDPR do not contain a definition of "anonymisation". However, recital 26 states that data protection principles should apply to all information about identified or identifiable natural persons. Pseudonymous personal data that can be attributed to a natural person by means of additional information should be considered as information about an identifiable natural person. To determine whether a person is identifiable, one should take into account any reasonably probable ways (including the separation of entries for the person), for which there is a reasonable probability that it will be used by an administrator or other person for direct or intermediate identification of the individual.

3.4 Identity and profiling - the future of regulation?

The dynamic development of new technologies, the related digitization and the increase in innovation in this area have an ongoing impact on the shape of personal security. The space of ICT networks is also a place of emergence of new threats that require analysis, definition of goals and appropriate regulation. One of the key areas of intensive involvement of network participants is the advertising area. Regulatory policy regarding advertising activities sees particular dangers in the sphere of the right to privacy. Laws, jurisprudence and related to advertising in new technologies allow to state that standards of protection against unfair activities are still too inflexible in relation to the changing reality, despite the fact that the aims and functions of advertising remain unchanged and do not differ from traditional forms. Advertising in new technologies allows the use of previously unknown methods. The Internet has contributed to the creation of, among others spamming, viral marketing or website positioning, which was not possible in the age of traditional media.

Respecting the provisions regarding the protection of personal data, personal rights and counteracting unfair competition in marketing activities takes on a new meaning in the context of cyber advertising. Completely unknown forms of internet communications are entering the space of personal security. Advertising should focus the attention of the potential recipient, this is its purpose, but without violating their privacy sphere.

Contemporary advertising activities are closely connected with the right to privacy, which is constitutionally guaranteed, including by protecting the private sphere and the security of correspondence and personal data. There is a conflict with another good, which is personal security, which ultimately touches on issues of public security and, consequently, national security. We can highlight informational ads, i.e. ones that are intended to build awareness of the brand and its new products. Another category may be inducement ads aimed at building shopping preferences or directly encouraging purchase. There are also ads that resemble the position of an established brand. They focus on strengthening customer loyalty. This is called remarketing, i.e. reaching people who visited a given site, made a purchase, engaged in content, and left an email. We can also identify enhancing ads, i.e. ones that convince customers to make a purchase. They also offer e.g. extension of the service or its additional variants. Advertising is also a way to influence emotions. Thanks to it, consumers are informed about new services, interesting solutions and possibilities. Advertising is also a convenience of wide selection and raising awareness.

According to the Supreme Court in its judgment of 26 January 2006 (file no V CSK 83/05), advertising is any statement directed to potential consumers regarding goods, services, as well as entrepreneurs offering goods or services, aimed at encouraging and encouraging recipients to buy goods or using services. The incentive can be expressed directly, e.g. by using terms corresponding to specific activities that will result in the sale of goods or services, or indirectly – by creating a suggestive image of goods and services, as well as the entrepreneur themself, to the extent that the recipients are compelled to purchase goods and services. Ads can be misleading in various ways. In turn, hidden advertising, surreptitious advertising – in accordance with the provisions of Article 16 (1) (4) of the Unfair Competition Act is a statement which, by encouraging the purchase of goods and services, gives the impression of neutral information and, having regard to the content of Article 7 point 11 of the Unfair Business Practices Act consists in using journalistic content in mass media to promote the product in a situation where the entrepreneur has paid for this promotion, and this is not clear from the content.

Due to the globalization of markets and the improvement of communication, the internet is currently the most popular medium. It also has the largest number of active users. There is significant market share and soaring online advertising. The Internet allows universal access to the advertising market and the publication of own content. Online advertising takes a wide variety of forms, some of which are ethical and some do not comply with these requirements. The advertisement uses e.g. flashing banners or deceptive "windows" that distract the user. Sites often do not control that on a page there are links that lead to sites with malware or to adult material. The problem of ethicality of e-advertising is therefore increasingly addressed. Universal and unrestricted access to the internet and the digitization of society requires advertisers to comply with basic principles such as respect for the right to privacy and protection of personal data. In Poland, the Code of Conduct in the Field of Advertising (IAA) was also adopted, which was developed in 1997 by the

Polish branch of the International Advertising Association. Programs blocking and limiting the display of e-ads have been created, which are gaining popularity, e.g. Adblock. Therefore, advertising can be considered one of the most aggressive means of interpersonal communication.

The issue of profiling is closely related to advertising. The world of marketing and new media has revolutionized the issue of online privacy and activities generally called profiling have clearly indicated the direction of development by increasing the scope of impact on users at the expense of their private sphere. Recital (30) of the GDPR states that natural persons may be assigned internet identifiers – such as IP addresses, cookie identifiers – generated by their devices, applications, tools and protocols, or other identifiers, generated for example by RFID tags. This can result in leaving traces, which in particular in combination with unique identifiers and other information obtained by the servers can be used to create profiles and to identify these people.

Profiling can be considered as an automated process leading to inference about specific characteristics, behaviors, habits possessed by a man, etc. Analysis and categorization of consumers according to specific criteria. It is also adapting marketing activities to the consumer profile. From 5 May 2018, profiling is defined in the GDPR Regulation as any form of automated processing of personal data, which involves the use of personal data to evaluate certain personal factors of a natural person, in particular to analyze or forecast aspects of the natural person's work effects, their economic situation, health, personal preferences, interests, credibility, behavior, location or movement. To simplify, profiling is a division of users according to their interests, shopping intentions, age or social status. Thanks to profiling, specific ads are displayed to users who will be interested in a given offer. By tracking users, social networking sites can offer them better tailored content. Profiling aims, as already mentioned above, to select the target group for a given product or service so that advertising is effective.

Profiling is done by analyzing the passwords that users enter in the browser. The basis of profiling are cookies. These are files in which the browser saves various information, e.g. what sites have been visited. The changes that the European Union introduced in telecom regulations mean that website owners must inform users that the site uses cookies. This means that it stores information or has access to information contained therein. In accordance with Article 22 of GDPR: the data subject has the right not to be subject to a decision that is based solely on automated processing, including profiling, and has legal effects on him. Therefore, the GDPR defines the purpose resulting from the legitimate interests of the administrator - you can object to such use of data. Online advertising is growing very quickly. It causes legal problems as well as moral dilemmas.

Advertising, which constitutes a significant interference in the sphere of privacy, is characterized by a number of unfair practices used by the advertiser and related entities, i.e.: tantalizing inconvenient for clients (over layer advertising), sending unsolicited

commercial information (spam) and abuse of technical means of information (information noise, things in internet).

The 21st century is characterized by a clear use of new technologies, tools and innovative solutions not only in the commercial industry, but also in politics (political marketing), e.g. during election campaigns. With the advancement of technology, the art of effective political communication and persuasion, as well as the ability to manage internal political structures naturally began to move to the network. As a result, political marketing began to introduce a set of online tools into politics, thanks to which political communication gradually became easier, and in addition the efficiency of actions aimed at gaining increased voter support. Similarly to the e-commerce industry, the profiling technique discussed above and the phenomenon of the information bubble function as political advertising on the same principles. New ads go beyond the territorial and time limits that have been in force so far. Depending on the different forms of communication, as well as the position and status of the content provider, different legal requirements regarding liability for advertising content will apply. This situation applies to virtually every sphere of human activity, which is increasingly dependent on the processes taking place in virtual reality.

European policy focuses on fundamental issues, but the European forum is also a place to discuss the right relationship: the individual and their security and new technologies. Questions arise about the nature of advertising and the purpose of collecting data on the web. How far does our "right to anonymity" reach? What does online anonymity mean? So far, there is no doubt that we are dealing with a systemic question, i.e. to what extent individual rights are balanced with legitimate interests of information. A significant part of the population seems to be aware of the existence of regulation in the area of networks. Nevertheless, there are population groups in which the level of media literacy and awareness of the existence of relevant regulations is clearly lower. Competences related to advertising help people recognize products or services offered for sale, but recognizing more subtle techniques is complex and basically beyond the reach of our perception. Freedom of expression and freedom of information, and now also freedom of the network, are in a clear tension in relation to the personal security expressed in the privacy of the individual.

4 Public axiology system and national identity in legal regulations and security threats

The sense of national identity is a value recognized by the Polish legal system and also by the law of the European Union. Man shapes their personality under the influence of society and its culture, and the nation is a natural community for a man. National heritage, legacy, identification with the achievements and values represented by ancestors is a personal good, subject to protection under Article 23 and 24 of the Civil Code. Continuing or cultivating a good tradition of ancestors is also considered a significant value, taking

into account objective criteria (see judgment of the Supreme Court of 28 February 2003, file no V CK 308/02).

The obligation to respect the national identities of the Member States under Article 4 (2) of the Treaty on European Union is based on the recognition by the CJEU of their institutional autonomy. In accordance with Article 4 of TEU, it should be for the Member States to fill in the concept of "national identity". Since these competences refer to general categories, as well as individually identified situations, specific to each state according to its political and constitutional structures, it would be necessary to determine what national identity is. In making attempts to define national identity, states must take into account paragraph 3 of Article 4 of TEU, in which the Union's obligation to respect national identity is balanced with the principle of sincere cooperation and the obligation on Member States to ensure compliance with obligations arising from treaties or acts of EU institutions. Respect for dignity and freedom and human rights is part of the identity of all European countries, and for the Member States of the Council of Europe, which are parties to the European Convention on Human Rights, the body setting standards for individual protection is the European Court of Human Rights. Guaranteeing states the right to create and apply norms that could violate these freedoms and rights was accepted as a condition for preserving the identity of states in the process of European integration. The body that sets the standard of individual protection is the European Court of Human Rights and its case law is often the benchmark for national courts and tribunals.

National identity is a personal good - recognized the Court of Appeal in Krakow. Ref. Act I ACa 1080/16, ordering Onet.pl to apologize for the photograph illustrating the article about the collaboration and romance of Polish women with Germany during World War II. In March 2016, an article on Onet.pl appeared. "Relationships of Polish women with German soldiers during World War II. For many people, it's still unthinkable". It was an interview with Mirosław Karet, the author of the book "I fell in love with the enemy", which tells about, among others, romances of Polish women with German soldiers and "domestic prostitution". The article is illustrated with a photo of women going to be shot in the Palmiry forest, led by German soldiers dressed in military uniforms. They were marked with the signature: "romance with a German soldier was strictly forbidden, but in Poland live children who are the fruit of such relationships". One of the women in the photo was the mother of Krystian Brodacki, Maria Brodacka, who was murdered for hiding a soldier of Jewish origin. Her son brought a lawsuit to protect personal rights. In a judgment, the court ordered the Ringier Axel Springer Polska publishing house to apologize to the plaintiff and awarded PLN 100,000 in damages. According to the position of the Court, one of the personal rights violated was national identity.

Cultural security is a concept that refers directly to issues related to the protection of national identity and national heritage. According to UNESCO, culture is the spirit of the nation and there is no culture other than what is defined by cultural identity. The words

of the continuator of ancient thought of St. Thomas Aquinas: "Genus humanum arte ratione viviti". As John Paul II[2] expressed, they have a universal sense in which different traditions meet, constituting the spiritual heritage of humanity and various epochs of its culture. The important significance of culture lies in the fact that it is the right shape for human life as such. Man lives a truly human life through culture. (...) man cannot do without culture. Culture is the future of man, therefore ensuring cultural security is of such importance to every individual and every nation. As emphasized by J. Czaja (2005:23) in his work "Cultural Security of the Republic of Poland", it is difficult to create any objective indicators of a threat to cultural security, especially in non-conflicting states.

The digital age that came with the development of computerization brings completely new threats on an unimaginable scale. The reasons for this phenomenon should be seen in the changes that occur in communication. According to Z. Bauman (2011:91), "globalization, by gnawing the sovereignty of states – nations, is breaking the protective wall of territorial independence, for which national identity has been protecting itself for over two centuries and in which it saw the guarantee of its security". Changes related, in particular, to the "digitization of human life" are the main reason for the emergence of threats to the cultural security of the nation. Cyberspace is currently the main area of human activity, and virtual digital reality penetrates into real life. This applies to business exchanges, exchange of various types of content, including information, as well as thoughts, ideas and views. Technological convergence, which is accompanied by legal and administrative convergence, make the digitization process an inherent attribute of human activities in every field. The development of multimedia platforms, mobile telephony and digital television, and broadband networks are conducive to the exchange of concepts. There is a problem of information overload and seeking reliable sources. There is an identity conflict. In 2010, D. Engelbart said that "In 20 or 30 years, all the IT knowledge that can currently be accumulated in a single city, or even currently exists around the world, will fit into a computer that can be held in barely one hand" (Lunenfeld, 2010:48). We are close to this situation, because the world has shrunk and as a consequence there is a lack of space for cultural diversity. The process of digitization is not indifferent to national identity. National identity is associated with the concept of a nation state which is undergoing crisis in the current conditions of civilization development. This applies above all to the effectiveness of its actions. J. Dunn (2007:15) draws attention to these issues, who combines situations of this crisis with two types of changes: strengthening everyone, except for the most extreme situations (also related to armed conflict) in the normative idea of the nation-state, and increasing awareness of new challenges regarding economic issues, ecological, military, political and cultural, which transcend national borders. The latter challenges are the subject of consideration presented in this part of the discussion on efficiency and legality in public administration activities in the protection of public security. As a result of this crisis, challenges related to cultural security create a situation of necessity to take specific protective measures. These are completely new tasks for public authorities. It should not be forgotten that these

activities must take place taking into account the requirements of the "democratic constitutional state". The concept of "democratic constitutional state" introduced by J. Habermas (1994:125, 113) refers to the theory of laws, which requires a policy of recognition that protects the integrity of the individual in the life contexts in which their identity is shaped. This author emphasizes that the consequence of implementing the system of rights is necessary here, which must be accompanied by social movements and political struggle to succeed.

Notes:

[1] Later in the work We use the concept of an individual - citizen, because We discuss the issue of individual rights and freedoms in the context of the state - individual - citizen relationship. The assessment of this relationship requires taking into account the obligations that a citizen has to fulfill towards the state.
[2] In 1963 the term "information society" appeared.
[3] One of the most famous projects of this type is Tor (The Onion Router). Tor is most often used to bypass content filtering mechanisms, censorship and other communication restrictions used, for example, in totalitarian countries, and can also be used to hide the user's IP number. The foundations of this network, which prevents the analysis of network traffic and, consequently, provides users with almost anonymous access to Internet resources (there have been reported cases of tracing users using the Tor network) were developed in 2003 by Roger Dingledine, Nick Mathewson and Paul Syverson. Currently, the development of the Tor system is handled by the Tor Project (www.torproject.org) - a non-profit organization registered in the USA. The Tor network is a virtual computer network that uses the so-called onion routing. It works by encrypting your data multiple times and then sending it through a series of proxy servers called network nodes or onion routers. Each of the nodes decodes only one layer of the transmitted message in order to obtain information about the further path of the packet. Thus, the transmission intermediary only knows the node that sent the packet directly to it and the onion router to which it sent the message directly. The data about the package origin, its recipient and the content of the information sent are not disclosed to him. Additionally, before each of the packet jumps, a pair of one-time cryptographic keys are first exchanged between the servers, used to decode the next data layer. From the target computer's point of view, incoming traffic comes from the outbound Tor node.
The term garlic routing has many interpretations. Currently, Monero defines it as the method by which Kovri and I2P create an anonymous message-based web peer overlay network. Garlic encryption of garlic routing is similar to layer encryption in onion routing and it effectively hides sender's IP addresses and secures information sent to the destination node (and vice-versa). In writing, the concept of garlic routing appeared in Roger Dingledine's Thesis Free Haven in June 2000 (Section 8.1.1) as a derivative of the concept of "onion routing".

Chapter III

Regulations Related to the Protection of Privacy in the Cyber Security System

1 The right to be let alone

The right to remain in peace, also known as the right to be alone, or to be left alone, constructed by Warren and Brandeis, was a response to the publication of authorship works by the press. They stated that the protection of the individual's thoughts and emotions expressed in creative activity, consisting in preventing its public disclosure, should be implemented as part of the general right of the personality to be left alone. The authors concluded that the law that protects the literary works of the individual, not against theft or misappropriation, but against their unauthorized publication, is not the principle of protecting private property, but the inviolability of the personality of the individual. They tried to describe a legal institution that would allow individuals to protect themselves against interference by third parties in their home sphere. They considered that the right to be left alone should be considered a "law against the world" and violation of this right should constitute grounds for redress. Interfering with the privacy of the individual causes pain and suffering that is more severe than bodily harm. It is pointed out that Warren and Brandeis tried to build a bridge between the European, western privacy culture, which was based on the right to protect the good name of the individual, and the American tradition of freedom, which had its sources in the law of so-called domestic peace. At the core of *the law to be let alone* formulated by American scholars was a fundamental distinction between the public and private spheres. These authors concluded that the right to privacy expires as soon as the facts are published by the media with its consent. The concept created by Warren and Brandies directly influenced the subsequent evolution of American law, and in particular the formulation of a series of four torts aimed at protecting the privacy of individuals.

These cases include:

- invasion of the so-called isolation, i.e. in which the individual expects privacy;
- public dissemination of information from private life,
- providing false information from private life (defamation),
- misappropriation of someone else's image, good name, or other information identifying the person in order to achieve benefits.

These four categories of tort, which are attacked by the privacy of the individual, were developed by William Prosser as *invasion of privacy* (H. H. Perritt Jr., H.H., 1996:94) .

The concept *to be let alone* allows to distinguish two aspects of privacy: *seclusion* and the protection of personal information regarding the sphere of his private life. This leads to the conclusion that the right to privacy is characterized by three components: *secrecy*, *anonymity* and *solitude*.

The right to loneliness was also the basis for distinguishing individual spheres of individual life in Polish doctrine. The criterion used by A. Kopff (1972:31) for their distinction was the extent to which the individual has the opportunity to isolate himself from society in terms of their private life and in which they can demand that their private life not be interfered with. A. Kopff (1972:32) distinguished on this basis:

1) the sphere of intimacy,
2) the sphere of privacy, which also includes the sphere of social life,
3) the sphere of universal accessibility, in which he, in turn, distinguished two areas: the scope of the possibility of becoming acquainted with facts concerning other persons, but without the right to publicly disseminate them, and the scope of the possibility of public dissemination of these facts.

2 The right to be forgotten

The right to be forgotten is an instrument for protecting the right to privacy and protecting the personal data of an individual. It has been regulated in Article 17 of the GDPR. Strictly speaking, it refers to the right to remove certain personal data from virtual reality, change it or otherwise affect the content posted on the Internet (Szot 2018:36).

The literature on the subject emphasizes that the "right to be forgotten", which is innovative in nature and manifests itself in the possibility of interfering with its data on the Internet, refers to the legislation of European countries. Most often it is pointed out that the concept is a development of existing concepts in the legislation of Western countries such as "the right to forget" or "the right to delete data". These terms are often used interchangeably in the literature on the subject even though they are not identical. Each of the indicated concepts, as well as the concept of "the right to be forgotten" assumes the right of every person to delete information about him, after a certain period of time.

The structure "right to forget" from the French *le droit a l'oubli* was used to protect former convicts after serving a sentence. It consisted in deleting, after a specified period of time, some data about the convicted person and the act committed by them, a trial, serving a sentence, etc. This concept is justified by the idea of respecting the private life of the individual, and its purpose is to prevent violations of such personal rights as dignity, identity of the individual or reputation. It was part of a comprehensive civilist jurisprudence practice regarding the protection of personal rights (Szot 2018:43).

The second institution, the "right to erase data" is an institution similar to the "right to forget". It differs, however, in granting the legal entity concerned a legal claim to delete data of which it is the subject, processed by third parties. The justification for such a solution is based on the idea that everyone whose data is processed on the Internet has the right to delete such data under certain conditions, e.g. if the data was entered unlawfully or if the entity has previously revoked the consent for data processing. The goal of such a solution is to achieve a balance between the data subjects and processors.

It can be pointed out that the "right to forget" has evolved over time and evolved into a "right to delete data". As M. Krzysztofek (2014:155) aptly points out, work on the institution of the right to be forgotten was inspired by the conclusion that, on the Internet, as opposed to reality, there is no blurring of the conviction after a specified period.

The right to be forgotten has been specified in Article 17 of the GDPR. Pursuant to the content of this provision, the data subject may request the administrator to immediately delete personal data concerning him, and the administrator is obliged to delete personal data without undue delay if one of the following circumstances occurs: a) personal data are no longer necessary for the purposes in which they were collected or otherwise processed; b) the data subject has withdrawn the consent on which the processing is based and there is no other legal basis for the processing; c) the data subject raises an objection pursuant to Article 21 (1) or (2) GDPR towards processing and there are no overriding legitimate grounds for processing; d) personal data was processed unlawfully; (e) personal data must be deleted in order to comply with a legal obligation under Union or Member State law to which the controller is subject; f) personal data was collected in connection with offering information society services directly to a child over 16 years of age, and then, as an adult, requests that their personal data be deleted by the administrator.

3 Protection of information privacy and the processing of traffic data, location data and other user identification data

A common way to violate the privacy of electronic service recipients is to use operational data, i.e. *traffic data*. *Traffic data* is data that allows tracking users on the network. These data are necessary to establish and maintain electronic communications, including information about the pages to which the user was connected, as well as the time of establishing the connection and its duration. Operating data is data about the start, end and scope of the service provided, i.e. information about connections between computers, including their IP addresses, type of connection, date and time of its duration.

According to the definition expressed in Article 18 (5) of the Act on Rendering Electronic Services the service provider may process the following data characterizing the way the recipient uses the service provided electronically (operational data):

1) indications identifying the Customer based on the data referred to in section 1;

2) markings identifying the end of the telecommunications network or IT system used by the recipient; and
3) information about the start, end and scope of each use of the electronic service.

A characteristic feature of operational data is that on their basis it is possible to track and evaluate the service user's activity on the network. Such information gives the service provider the opportunity to determine which service the recipient has used electronically, including the addresses of pages viewed by the recipient of the service, records of messages sent via e-mail or via SMS. All data is saved in the system logs of the service provider's servers (Klafkowska-Waśniowska, 276). Thanks to this information, the service provider is able to determine which sites interest the customer, which ads attract his attention, and who he contacted, which violates the secret of the recipient's correspondence. Traffic *data* also includes data such as IP addresses. The service provider with the same IP number can identify the ICT system to which it belongs. The IP address alone does not identify the user and does not constitute personal data. Only when it is combined with other data does it obtain the status of personal data. Traffic data includes data about the location of the user's communication device. These data are extremely important in relation to mobile devices, with the help of which they can easily locate their location if they connect to the network. Thanks to *traffic data*, the service provider is able to determine the exact coordinates of the geographical location of the recipient and the direction of movement. With their help, the service provider is able to track every move of the recipient, which significantly violates his sphere of privacy. Directive 2002/58/EC in Article 9 allows the service provider to process the recipient's data that is not traffic data, i.e. data that is not necessary for them to send a transfer or charge fees. However, they can process them only in anonymous form or after obtaining the consent of the recipient, when they allow identification. These data are often used to provide services that consist of pointing the way, providing weather information about the whereabouts of the user, or traffic information. With such accurate data on the location of the recipient's devices, and thus their whereabouts, the service provider can control all their movement, not only on the network, but also on the ground.

Along with the development of technology, many new marketing opportunities have appeared, allowing a simple and cheap way to reach potential customers. It is the Internet that is used as the main means by entrepreneurs, not only those providing electronic services to communicate, transfer information, including all types of offers, and to acquire customers. Good advertising on the Internet is almost a guarantee of increasing the company's revenues as well as increasing brand recognition. The use of data collected and processed using advanced automatic processing systems allows you to personalize your ad as much as possible. Based on the user's preferences, time of service and other data such as location data, its consumer profile can easily be constructed. Sending graphic and text information via the Internet in the form of advertising banners, the message that appears when opening the page is an integral part of the functioning of social networks and the entire Internet. However, for an ad to bring a profit to the service provider, it must

reach the right group of Internet users. That is why so-called *cookies* that collect information about pages visited by the user were created, so that they can be qualified to specific consumer groups. *Cookies* are small text files sent by every website we visit and saved on a computer that we use when browsing websites. *Cookies* is "a web application used on servers and enabling tracking the order of web browser sessions generated by a single system user, it is a way to maintain cause-and-effect relationships between subsequent orders by storing small portions of data on the server" (Krasuski, 2008:86). *Cookies* consist of a series of letters and numbers that contain information needed for the proper functioning of websites. The default parameters of *cookies* allow them to be read only by the server that created them. Most often they are used to count visits to websites, polls, websites where there is the possibility of logging in, online stores, as well as ads and tracking their number of recipients (Kurek, 2013:60). Cookies improve the login process by remembering the login and password, and also remember the goods added to the basket even if we refresh the page. *Cookies* speed up the process of browsing websites, because we do not have to choose the language of the site each time, appropriate to our country of origin, or once again fill out the same form. They are necessary for positioning the client and selecting ads appropriate to his interests and preferences. The files are also used by service providers to create statistics of website visits (Hofmokl, 2009:16). On the one hand, *cookies* are designed to improve Internet users' use of the services provided on it, but on the other hand, *cookies* allow the creation of user profiles with their preferences, preferences, which can affect the violation of personal rights and even violation of users' privacy. This information is also used to create anonymous, aggregated statistics that help us understand how a user uses websites, which allows improving their structure and content, excluding personal user identification.

The operation of *cookies* is very simple – they remember our activity on the Internet. They allow the collection of statistical data as well as the optimization of the use of the website. *Cookies* allow websites to recognize user-preferred content. By accepting *cookies*, videos, photos, texts, ads and information are addressed to you because they reflect your preferences. The use of cookies is reciprocal - for both the user and the website owner. For the former, it makes easier to navigate the site thanks to remembered preferences, while for the latter, it helps improve the structure and content of the site. There is also a third group that gains on information stored in the form of *cookies* - these are companies analyzing intra-network traffic. The materials obtained allow them to generate statistical data on Internet users, and thus tailor advertisements, films or surveys to their activity.

The subscriber or end user may agree by using the software settings installed on the telecommunications terminal equipment used by him or by configuring the service. As a consequence of new ways of providing commercial information, the regulations contained in Article 9 of the Act on Rendering Electronic Services seem very outdated. Especially that in the conditions of using new advertising techniques, service providers are penetrating the private sphere. All the objectives of the action that will result in

entering the private space of the individual must be clearly defined, and legal norms related to such a situation adapted to the new digital reality. A similar remark applies to regulations related to *spamming* referred to in Article 10 of the Act on Rendering Electronic Services. Often, however, commercial information goes to people who have not agreed to receive them. This information is called unsolicited commercial information, but if it is sent to a large number of people at the same time, it is so-called spam. The service provider, having data enabling the construction of a consumer profile, can effectively control what ads the user will see when using the service. It is worth noting that this possibility is the foundation of business models of many audiovisual media service providers. Computer user information may be collected using so-called *cookies*, enabling the storage on the user's computer of information related to the use of the service, which the provider can then read.

In the Polish legal system, cookies apply to the Article 6 of the Act on Rendering Electronic Services, which regulates the information obligations of the service provider towards the recipient. The service provider has the right to use cookies if he fulfills the statutory information obligation. However, it should be noted that in both national and EU law, for cookies to be used by the service provider in accordance with the law, it is sufficient for the service provider to inform the recipient of this fact. The law does not require the service provider to obtain the user's consent to the use of cookies on devices through which he uses the Internet. Often, when browsing websites at the top or bottom of the screen, there is a brief information that this site uses cookies[1.]. It happens that users do not even pay attention to it. However, those who do not want their browser to use cookies must find in its settings the conditions for storage and access to cookies, and then turn them off there. Such behavior is often troublesome for Internet users and they do not change cookie settings, so that service providers can use them. It happens, however, that the service provider does not inform the user about the use of cookies, which makes monitoring his activity in the network and collecting data on e-mail addresses, the type of software used to browse websites or browser history, becomes a prohibited activity.

The importance of collecting data using cookies is whether it will be possible to determine the user's identity using the data that has been collected. If so, the use of cookies will constitute the processing of personal data in connection with this, the service provider will have to obtain the user's consent to the processing of his data using cookies (Chałubińska-Jentkiewicz, 2016).

The cookie policy is also regulated by the Telecommunications Act of 16 July 2004. Article 173 (1) of this Act says that "storing information or accessing information already stored on the telecommunications terminal equipment of the subscriber or end user is allowed provided that:

1. the subscriber or end-user will be directly informed in a clear, easy and understandable manner about:
   a. the purpose of storing and accessing this information,

   b. the possibility for him to specify the conditions for storage or access to this information by means of software settings installed on the telecommunications terminal equipment they use or the configuration of the service;
2. the subscriber or end user, after receiving the information referred to in point 1, agrees;
3. The information stored or access to it does not change the configuration of the subscriber's or end user's telecommunications terminal equipment and software installed on this equipment".

It should be noted that within the meaning of this Act, information is cookies and telecommunications devices, e.g. a computer or a telephone through which the user uses the Internet. Therefore, the service provider is obliged to inform the recipient about saving any cookies on his device. The recipient must agree to save cookies on his device. Before using the service, the recipient must be informed in a clear and understandable manner that the website he wants to use uses cookies, he must be informed how he can delete the software saving cookies, and then he must agree to the installation of cookies on his device and their use. In accordance with Article 209 of the Telecommunications Act whoever fails to fulfill the information obligation discussed above, is liable to a fine. Therefore, in order for cookies to be saved on the recipients' devices, they must knowingly agree to this. There are several types of cookies on the network, mainly session cookies (*transparent cookies*) and persistent cookies (*permanent cookies*). Session cookies consist in controlling user activity only during a given session, and after closing the browser, it is no longer possible to restore previously obtained data. Persistent cookies placed on the disk of a device through which the user connects to the network for a longer period until they are removed (Konarski, 2004:98).

4 Data retention and mass surveillance

Privacy, identity and security limiting these values are not the effect of civilization changes, a side effect of democracy imposed on an individual or group. An individual or society cannot develop properly without privacy and identity. Standards shaping the scope of identity and privacy protection allow us to assume that both privacy and identity constitute an element of human dignity and protect both the individual and the nation against interference. Since privacy is a means of safeguarding against external control or interference, as well as an element of human dignity – it leads to the individual's personality, then both privacy and identity constitute a security measure against external interference, but security itself may limit these values in legal situations. For example, this happens when data retention is used. Therefore, the individual has no real possibility of demonstrating that as a result of interception of electronic communications also their communication was collected by an authorized body. This applies in particular to criminal proceedings in matters related to offenses committed using ICT systems.

In such cases, procedural authorities need to collect a lot of different data to be able to identify the perpetrators of crime and prove their allegations. The provisions of the Code of Criminal Procedure contain standards that entitle procedural authorities to use traffic data (billing) of telecommunications service subscribers. From the perspective of Article 49 of the Polish Constitution, according to which freedom of communication and confidentiality are guaranteed, and the restriction of these freedoms can occur only in cases and in the manner specified in the Act, such regulation was required. The principles of data retention were specified primarily in the Telecommunications Act.

Pursuant to Article 180d of the Telecommunications Act, telecommunications undertakings are obliged, among others for recording and sharing the above data with authorized entities (e.g. Police, Border Guard or Internal Security Agency) at their own expense, as well as the court and the prosecutor, on the principles and in compliance with the procedures set out in separate provisions. Provision of Article 180a is an implementation into the national legal order of 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 the provision of public communications networks and amending Directive 2002/58/EC. This article indicates that data retention will be used in particular to detect offenses directed against defense, state security, public order and security, and fiscal offenses. Provision of Article 180a (1) (1) imposes on the public telecommunications network operator and the provider of publicly available telecommunications services the obligation to retain and store data for a period of 12 months. The justification for this regulation emphasized that such a need results from the fact that Poland is or may be used as a logistics base or transit point for terrorist groups.

Data retention was reviewed by the Court of Justice of the EU. The subject of the matter decided by the CJ in the judgment of 8 April 2014 (Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Irlandii i Attorney General C-293/12) was the issue of compliance of the so-called Retention Directive (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, p. 54) with the Charter of Fundamental Rights of the European Union. The High Court (Ireland) and the Verfassungsgerichtshof (Constitutional Court, Austria) asked the Court of Justice to examine the validity of the directive, in particular in the light of two fundamental rights under the Charter of Fundamental Rights of the European Union, namely the fundamental right to respect for private life and the fundamental right to the protection of personal data. The Court found that, by requiring the retention of those data and by allowing the competent national authorities to access those data, the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal

data. Furthermore, the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the persons concerned a feeling that their private lives are the subject of constant surveillance. The Court annulled this act completely. The directive was adopted by the European Parliament and the Council in 2006 and was the answer regarding the access of security services to telecommunications data. It imposed an obligation on Member States to collect certain telecommunications data by telecommunications operators. The purpose of such retention was to enable investigation, detection and prosecution of serious crimes specified in the legislation of each Member State – similarly to the Polish regulation in Article 180a of the Act. The Court found that the retention of data with a view to its possible disclosure to the competent national authorities did indeed meet the general interest objective of combating serious crime and, ultimately, public security.

However, the Court is of the opinion that, by adopting the Data Retention Directive, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality. The Court observed that, taking into account, firstly, the important role played by the protection of personal data in relation to the fundamental right to respect for private life and, secondly, the scope and gravity of the interference with that right, as pursued by the Directive, the discretion of the EU legislature shows limited. The Court based its analysis on allegations of violation of the right to privacy and protection of personal data. In the case of the right to privacy, he divided this right into intrinsic (resulting from the retention of data related to private life) and additional (which is the source of access to such data by competent national authorities). He noted that the fundamental importance of the achieved goal does not automatically indicate the necessity of the funds used to achieve it. Due to the fact that the directive did not include the obligation to store the content of messages, the Court assessed that there was no violation of the essence of the right to privacy. The Court also found that the directive does not provide for sufficient safeguards to ensure effective protection of the data against the risk of abuse and against any unlawful access and use of the data. It noted, inter alia, that the directive permits service providers to have regard to economic considerations when determining the level of security which they apply (particularly as regards the costs of implementing security measures) and that it does not ensure the irreversible destruction of the data at the end of their retention period.

The Polish Constitutional Tribunal also commented on data retention. In the judgment of 30 July 2014 (OTK-A 2014, nr 7, file 80), the Tribunal adopted a position on the constitutionality of provisions related to the order of operational control. The Constitutional Tribunal drew attention to the importance of the Internet and other modern forms of individual communication, but explained that the protection of constitutional freedoms and rights in connection with the use of the Internet and other electronic methods of distance communication does not differ from the protection of traditional forms of communication or other activity. The Tribunal did not determine what exactly the procedure of access to telecommunications data should look like, and in particular –

whether obtaining consent for their disclosure is necessary in relation to each type of retained data referred to in Article 180c and Article 180d of the Telecommunications Law. Not all such data cause the same amount of interference with human rights and freedoms. The Tribunal has also not determined whether prior checking is necessary in each case or whether a follow-up check may be sufficient. Currently, however, the Polish legal order lacks any control over data collection, and the applicable provisions do not even contain the minimum guarantees required by the Polish Constitution (Chałubińska-Jentkiewicz & Karpiuk, 2015:240).

According to the Constitutional Tribunal, privacy is constitutionally protected freedom with all its consequences. First of all, it means the freedom of action of individuals within the framework of freedom, until the law sets its limits. Only an unambiguous statutory regulation may impose restrictions on undertaking specific behaviors falling within a specific freedom. However, not every regulation is admissible in the light of constitutional norms, principles and values. Constitutional protection resulting from Article 47, Article 49 and Article 51 (1) of the Polish Constitution covers all means of transmitting messages, in all forms of communication, irrespective of their physical medium (e.g. personal and telephone conversations, written correspondence, fax, text and multimedia messages, electronic mail, transmission of messages via internet portals). This protection covers not only the content of the message, but also the circumstances of the communication process. As part of the constitutionally guaranteed man freedom and their information autonomy, there is protection against the secret monitoring of the individual and the conversations they conduct, even in public places. According to the Constitutional Tribunal, it does not matter whether the exchange of information concerns strictly private life or professional activity, including economic activity. There is no such sphere of personal life of a man whose constitutional protection would be excluded or inherently limited.

An analysis of Polish legislation indicates that the secret of communication (correspondence) is not unlimited freedom. The Polish Constitution provides for the possibility of limiting it by statute. This does not mean, however, that the legislator may freely decide on the content and scope of restrictions on the freedom of assembly. This provision does not exclude the application of Article 31 (3) of the Constitution (principle of proportionality), which speaks of the need for the legislator to maintain an ordinary measure of constitutional restrictions on freedoms and rights. Therefore, first of all, restrictions can be established only in an Act, and secondly, they can be established only when they are necessary in a democratic state to protect the values indicated (state security or public order, protection of the environment, public health and morality, freedom and rights of others) and thirdly, they cannot violate the essence of a given freedom or law.

In the context of data retention there is one more problem regarding the so-called mass surveillance.

The problem of mass surveillance that characterizes the functioning of modern media, especially social media, which affects an unspecified group of people was discussed in the ECtHR judgment in the *Klass et al. v. Germany* case, in which five German lawyers were the applicants (Application No 5029/71: Gerhard Klass and others v/the Federal Republic of Germany, Decisions and Reports, t. 1, Council of Europe, European Commission of Human Rights: Strasburg 1975, p. 20-30). The case took its name from Gerhad Klass - a senior prosecutor (Oberstaatswalt). The other applicants are: judge Jürgen Nussbruch and three lawyers: Peter Lubberger, Hans-Jürgen Pohl and Dieter Selb. The subject of the discussion was the definition of the victim of a violation of the Convention entitled to submit a complaint; admissible limits of violation of the right to privacy and the notion of law of effective means of protecting rights protected in the Convention. In that judgment, the Court recognized that an individual may, under certain conditions, claim to be a victim of a violation caused only by the mere existence of secret means or legislation authorizing the use of secret means - without having to show that such measures were in fact used against them. The Tribunal emphasized that when the State orders the use of classified control measures and when it is to become a secret to controlled persons and when they are not entitled to legal remedy against such an order, the content of Article 8 of the Convention protecting the right to privacy would be largely a fiction. In such a situation, the individual may be treated in a manner contrary to Article 8 or even be deprived of the right guaranteed in this provision without being aware of this fact and thus without the ability to use a legal remedy either at the national level or before the Convention bodies. As long as the decision of the authority authorized by the Act to adapt the control of correspondence, mail or telecommunications remains bindingly secret to the person concerned, as long as this decision is excluded, under the protection of Article 6 of the Convention, from judicial control undertaken at the request of that person and, as a consequence, escapes from necessity from the requirements specified in this provision.

Mass surveillance leads to social self-control, but in the most undesirable form – to limit the exercise of one's own rights, including freedom of expression, for fear of sanctions by public authorities. In this way, mass surveillance causes damage not only to each individuals, but to the entire state – it undermines its system foundations. Not without reason, according to the well-established jurisprudence of the ECtHR, the primary purpose of legal safeguards established for secret state surveillance programs is to reduce the risk of abuse of power. In accordance with the standard introduced by the ECtHR, statutory provisions should specify at least the category of offenses that may involve authorization of the use of surveillance measures, as well as a limitation on the maximum duration of their application.

In the case of mass surveillance, it is no longer possible to meet the first of the indicated safeguards, because the essence of the use of this type of measures is to intercept all communications, and not only regarding persons suspected of committing specific crimes. However, it is worth analyzing in more detail the reasons for the repeated belief

that non-offenders should not be afraid of surveillance. It is, in fact, the belief of supporters of this view that information that can be obtained about them does not reveal secrets that they would not like to share with others. According to another position, this belief completely omits one of the most important features of mass surveillance – data acquisition from various sources, their aggregation and correlation, and in the final stage - building new conclusions. In this opinion, such conclusions, as a rule, go beyond the original scope of information, thus creating new knowledge about the subjects (under surveillance). It can be knowledge about their preferences (not only shopping, but also e.g. political or sexual), expected behavior, profile of decisions made, but also a circle of friends or social relations built. The process of acquiring new knowledge from a large number of known facts is the basis of Big Data analytics, which is widely used in mass surveillance programs. As a result, measures of this type can not only provide detailed data on individuals, but also can be used to predict the behavior of selected social groups or the entire society.

On the one hand, it seems that registering electronic communications data for hundreds of thousands of housewives, workers, officials, children, as well as lawyers, politicians or clergy does not increase the defense capabilities of the state. On the contrary, it engages the services in analyzing huge data sets, worthless from the point of view of state security, but constituting an inexhaustible source of information and control over society. On the other hand, it is allowed to transfer data to large foreign corporations, which in turn transfer these information resources to their principals, sell them to other countries, etc.

The combination of the secrecy of surveillance activities resulting in their opacity, the participation of which is the State with a lack of independent supervision and unlimited collection of data on citizens clearly increases the risk of abuse of power. At the same time, it is difficult to determine today whether it leads to an increase in the ability of services to detect or prevent the most serious crime.

The European Parliament, dealing with the issue of extensive surveillance programs run by the Supreme Administrative Court, recognized electronic surveillance programs as "another step towards creating a fully preventive state in which the paradigm of criminal law established in democratic countries will change, according to which any interference with the fundamental rights of suspects requires approval by a judge or prosecutor on the basis of rational suspicion and regulated by law". In turn, the Court of Justice of the European Union, examining the compliance of the provisions introducing the general obligation to retain data with EU law (especially Article 7 and Article 8 of the EU Charter of Fundamental Rights) pointed out that "the fact that the retention and subsequent use of data is carried out without informing the subscriber (...) may (...) evoke a sense in persons whose data is being retained or used that their private lives are under constant surveillance. " Special Rapporteur on the Privacy of the UN drew attention to one more threat associated with running these types of programs – the danger that each subsequent authority can use the existing possibilities of electronic surveillance and accumulated

huge databases on citizens to achieve their own goals, which will not always be consistent with expectations and needs of the society. Only this argument should be a sufficient reason, also for supporters of conducting surveillance programs, that the manner of their implementation excludes the possibility of non-directional data collection, and established legal safeguards, including effective supervision measures, lead to strengthening, not weakening, mechanisms of building a modern society based on knowledge and information.

Based on the case law of the national courts of EU Member States, the recent judgment of the British Investigatory Powers Tribunal draws attention with partial non-compliance with Article 8 (2) of the ECHR, provisions that were no longer binding at the time of the ruling, constituting the basis for conducting secret electronic surveillance programs by the local special forces. The position of tribunals and international organizations, as well as ombudsmen and non-governmental organizations, which signal the incompatibility of extensive surveillance programs with fundamental rights, has not yet affected the strengthening of legal safeguards on the part of European legislators, including the national legislator. It should be noted, however, that it is difficult to withdraw from the legal order the general obligation to retain data, and in recent years new statutory regulations have been introduced aimed at weakening the right to privacy at the expense of the powers of special forces. These activities are always justified by concerns about violation of the public interest, special goods – the security of citizens.

5 Spam as an element of violations of the right to privacy

The issue of direct marketing and unsolicited communications in the Polish legal system is regulated by two provisions – Article 172 of the Telecommunications Act and Article 10 of the Act of 18 July 2002 on Rendering Electronic Services. The provision contained in Article 172 (1) of the Telecommunications Act states that "the use of automated calling systems for direct marketing purposes is prohibited, unless the subscriber or end user has given their prior consent".

In order for commercial information to be considered as ordered, the recipient's consent must be obtained. In the Act on Rendering Electronic Services, the issue of consent is regulated in Article 4, which stipulates that if the law requires the recipient's consent, that consent may not be implied or implied by a declaration of intent with a different content and may be revoked at any time. The term 'consent' has not been defined anywhere, but the Act on the provision of electronic services specifies several cases that require consent, for example:

1. Sending commercial information (Article 10 (2));
2. Processing of certain data of the recipient for advertising purposes, market research, as well as the recipient's behavior and preferences, also after the provision of services (Article 18 (4) and Article 19 (2) (2));

3. Not removing labels identifying the recipient as part of data processing (Article 19 (4) (Namysłowska, 2011:98).

In Article 9 (1) of the Act on Rendering Electronic Services, the legislator introduced the requirement that commercial information must be clearly separated and marked, so that it does not raise doubts that it is commercial information. As a result, the customer should easily distinguish commercial information from other information.

Commercial information is considered ordered if the recipient has agreed to receive it and has provided their electronic address for this purpose. After obtaining such consent, the service provider has the right to send the ordered commercial information, such as the current promotional offer, new products and they no longer constitute spam.

Therefore, the Polish legislator used an *opt-in system*, i.e. a solution that requires the user's active consent, unlike the *opt-out* system, in which messages can be sent even without obtaining such consent - all you need is no objection. Undoubtedly, the messages delivered "on the occasion" of the provision of on-demand audiovisual media services are transmitted to individual recipients - they are of this nature, as audiovisual media services on demand are directed to individual recipients, which is due to the very nature of these services. On the other hand, nothing precludes the automatic nature of such messages - human participation does not seem to be necessary.

With the development of services provided via the Internet, sending commercial information in the form of e-mail has become a very popular way to reach customers. Due to the lack of the possibility of personal contact with the customer and the electronic nature of commerce, this message has become almost a natural way of contact between service provider and recipient. Nevertheless, many customers perceive this way of service providers very negatively. With the rapid development of e-commerce, sellers began to place more and more emphasis on the development of advertising, and this is associated with a greater amount of unsolicited information, i.e. spam (Gancarz-Wójcicka, 2013:603). Perhaps every Internet user had to deal with spamming. From the beginning of its existence spam has been causing negative emotions among internet users because it is still used today by service providers in an unethical and often illegal way. Spamming (spam) poses a serious threat to the private sphere of individuals, via email. There are more and more abuses and attacks on individual or corporate computer network users (Hofmokl, 2009:113). Despite many attempts to define spam, it has not been possible to create a consistent definition of this issue. There are many definitions of spam that are used in a colloquial and general way, but they do not have the nature of legal definition. Broadly understood spam is unwanted correspondence that appears on communication platforms such as e-mail, instant messaging, telephone, fax, but also ads appearing on websites. The concept of spam has many definitions. According to A. Malarewicz (2009:218), all unsolicited commercial electronic communications are defined as spam, which are determined by its relationship with business activities sent without the

recipient's consent. A popular social networking site Facebook indicates that "spam means repeatedly contacting others to provide unwanted content or requests. This includes sending mass messages, posting links or images on other people's timelines too often, and sending friend requests to people you don't know personally" (Malarewicz, 2009:219). The definition of spam, i.e. unsolicited commercial information, can also be found in Article 10 of the Act on Rendering Electronic Services: "It is forbidden to send unsolicited commercial information addressed to a designated recipient who is a natural person by means of electronic communication, in particular electronic mail". The content of spam is usually advertising that is intended to encourage the purchase of goods or services offered by the sender. However, not only commercial content is spam. Through spamming, you can disseminate religious, social or political ideas. The essence of spam is to send a large amount of commercial information with the same content to unknown people (Namysłowska, 2012:450).

Based on the definition quoted by the US non-governmental organization *Mail Abuse Prevention System* (MAPS), the term "spam" should be understood as information sent electronically, not only commercial information that meets the following three conditions in total:

1. Its content is independent of the recipient's identity, i.e. the same message content can be directed to an unlimited number of recipients, which is why it is massive;
2. The recipient of this message has not previously agreed to receive such information. This consent should be explicit, informed and revocable at any time;
3. The recipient of the message may claim that the sender will benefit more from sending the correspondence than they do when receiving the message (Rogacka-Łukasik, 2012:237). So the message is of a commercial nature, and the sender sending spam is focused on achieving financial benefits.

There are also four forms of spam, i.e.:

1. Commercial spam – strictly spam, its main purpose is to encourage the recipient to buy a specific good or service;
2. Dangerous spam – this is information that contains programs that pose a danger to the recipient of spam, such as, for example, viruses, spy programs, Trojan horses;
3. Non-commercial spam – these are all unwanted messages advertising political parties, social and religious ideas, false warning information and letters asking for money to be provided to the account number for fraud purposes;
4. Social or private spam – such correspondence is usually not treated as unwanted by the recipient, it includes messages containing pictures, jokes, and videos whose sender are persons familiar to the recipient. Such emails are often sent by the recipient to downstream users who are in his address book. We are talking here about so-called chains (Malarewicz, 2009:220-221).

Spam is often identified only with unsolicited and unsolicited commercial information sent via email. However, this phenomenon has a much broader spectrum of impact. Spam can be found on many other communication platforms such as mobile phones; instant

messengers (e.g. Gadu-Gadu); chats and websites with the so-called pop-up, i.e. pop-up advertising windows.

Despite the fact that spam is very negatively perceived by Internet users, the number of unsolicited messages sent is still increasing. According to data provided by SophosLabs experts on the amount of spam in the world in the fourth quarter of 2014, the largest amount of spam is sent from China (16.7%). The United States is in second place (11.2%), followed by South Korea (8.8%). Poland is in 20th place in this ranking with 1.1% of spam sent worldwide in the given period. The chart below shows the countries that generated the largest amount of spam in the world in the last quarter of 2014.

Direct marketing is not defined in the regulations, but based on the analysis of various regulations, it is a broader concept than commercial information. This concept is understood as providing customers directly with information or proposals that relate to the sale of goods and services. In the light of the decision-making practice of the previous President of the Office of Competition and Consumer Protection, direct inquiry should be considered as the possibility of sending marketing information to the addressee. This creates a vicious circle, which de facto allows legitimate reaching customers by phone or email. The above issue is even more important for the current practice of entrepreneurs who use direct marketing, as failure to comply with the obligation to obtain such consent for sending commercial information may be subject to a fine of 3% of the revenue achieved through them in the given calendar year preceding the year of imposing the penalty (Wolife el al., 2012:44-45).

It should be remembered that the new regulations that apply to so-called mailing do not only apply to natural persons, but also to legal persons. Sending commercial information to the addresses of management offices, institutions and company branches will require the prior consent for this type of activity, according to Article 172 of the Telecommunications Act.

The rapid development of internet communication revealed its weaknesses. The current rules on the Internet have ceased to be effective and do not protect users from aggressive marketing practices. However, users can themselves take measures to protect it from unwanted messages. To this end, a Robinson list has been created to which you can enter your email address. This list includes addresses of people who do not want to receive unsolicited commercial information. Lists of this type can be kept by state institutions or entrepreneurs. In Poland, the International Direct Marketing Association is responsible for running the Robinson list. The big downside of this list is the limited access to it, which is only available to entrepreneurs who are members of the organization creating the list or will purchase access to this list (Rączka, 2007:101). The amount of spam received by email can also be reduced with the help of anti-spam filtering programs that recognize spam messages based on keywords and automatically transfer them to the spam folder.

6 Stalking

Stalking defines malicious and repetitive solicitation, obtrusion or harassment that threatens someone's safety. Stalking is often associated with criminal acts, i.e. insults. Examples of behaviors defined as stalking are following the victim, trapping him, and constant repetitive solicitation. These activities are particularly dangerous when they can take the form of physical violence that threatens the victim's life. The most common behaviors characterized by persistence of the perpetrator include the constant sending of SMSs, MMSs, e-mails, but also providing the real data of the victim in false internet advertisements (e.g. of a sexual nature), making public the images of the victim on the Internet violating his good name or dignity. In Poland, victims of stalking did not have grounds to assert their rights in the provisions of the Penal Code. So they chose the civil route to violate privacy or domestic peace - on the basis of the protection of personal rights provided for in Art. 23 and 24 of the Civil Code or a complaint regarding an offense, i.e. "teasing another person by maliciously disturbing the peace" Art. 107 of the Act of 20 May 1971 Code of Offenses. Today, in a stalking situation, we can talk about committing the crime of persistent harassment. In addition to many benefits, the Internet and all kinds of new technologies also pose threats in this area. More and more people are complaining about offensive posts, there are more and more press reports about slander or just stalking. These types of behavior have recently become offenses under criminal law (Kosińska, 2008:33-47). The issue of stalking is regulated in art. 190 a of the Penal Code.

7 Identity theft

The use of services provided electronically, as I mentioned earlier, in addition to many benefits also involves some risks. The availability of technology and the dissemination of network solutions has led to a change in forms of crime. Modern cybernetic criminals often treat breaking the law on the web as another test of their skills or having fun. Identity theft is also known as forgery, embezzlement or seizure of identity. It is a computer crime that affects more and more people. As many as 387 cases related to this problem were recorded in 2009. The crime of identity theft has been expressed in Art. 190 a § 2 of the Penal Code, according to which identity theft is impersonating another person, thereby using his or her image or other personal data to cause him personal or material damage. Identity theft is all actions taken to obtain real data from real people. These data are obtained with the use of various technical and ICT means using social engineering (Chałubińska-Jentkiewicz & Karpiuk, 2015:245). As for the principles of personal data protection in connection with the provision of electronic services, in accordance with Art. 18 section 1 of the Act of 18 July 2002 on the provision of electronic services, the service provider may process the following personal data of the recipient: According to K.J. Jakubski (1997:31), a computer crime is a criminological phenomenon, including all criminal behavior related to the functioning of electronic data processing, which directly harms the processed information, its medium and circulation in the computer and the

entire computer connection system, as well as in the computer hardware itself and the right to a computer program. Computer crime is a specific password that covers the issue of information protection in the conditions of its processing.

The phenomenon of eavesdropping is presented in Art. 267 of the Penal Code, according to which "Anyone who, without being authorised to do so, acquires information not intended for him or her, by opening a sealed letter, or connecting to a cable transmitting information or by breaching electronic, magnetic or other special protection for that information is liable to a fine, the restriction of liberty or imprisonment for up to two years."A criminal using computer programs (e.g. Sniffier), which are specialized in analyzing and receiving data, eavesdrops and has the ability to reach all private data. There are two types of information acquisition: one that stores data in files and interactive, which allows you to view the transmitted data on a regular basis (Chałubińska-Jentkiwicz & Karpiuk, 2015:248). There are:

- packet sniffing, or eavesdropping of transmission using software in computer networks. This eavesdropping can be compared to the eavesdropping of classic telephone lines. It captures data and analyzes it over a specific network. It can be used to steal passwords;
- eavesdropping on revealing emission (compromising emanation), this is eavesdropping on electromagnetic radiation emitted by devices that are involved in the transmission and/or processing of information. It should be pointed out

It should be pointed out that the above-described methods can also be used in the public interest by public authorities. As E. Ormsby (2019:370) emphasize, international law enforcement organizations are constantly trying to fight cybercrime but the methods of this fight are not obvious from a moral and ethical point of view. Sometimes methods used by law enforcement officers raise doubts. In 2015, the FBI took over and managed the Playpen website (similarly to Child's Play) one of the largest offering child pornography, introducing its software there and using the identity of users to identify criminals. One of the pedophiles who was identified by this method sued the government based on the argument that the access was provided by the services. Such absurd situations can also occur when using stalking. The fight against cybercrime is difficult and anonymity guaranteed by law and technology gives cybercriminals a sense of impunity.

Notes:

[1] For example, on the Allegro.pl website, at the top of the page there is a small bar with information in fine print with the following content: "The website uses cookies to provide services and in accordance with the Cookies Policy. You can define the conditions for storing or accessing cookies in your browser."

Chapter IV

Security and Protection of Identity as a Justification for Restrictions on the Right to Privacy

1 Restrictions on citizens' rights and freedom

Restrictions on the rights and freedoms of the citizen-citizen may be introduced in the event of specific conditions. These include security, public order, health, environmental protection, public morality, and the freedoms and rights of others. In the judgment of June 29, 2001, the Constitutional Tribunal (file no K 23/00, OTK ZU 2001, no 5, item 124) stated that Art. 31 3 of the Constitution of the Republic of Poland formulate the cumulative premises for the admissibility of restrictions on exercising constitutional rights and freedoms, and the limits of interference with constitutional rights and freedoms are determined by the principle of proportionality and the concept of the essence of individual rights and freedoms. "To say that restrictions can only be established when they are necessary in a democratic state, we must consider: whether the introduced regulation is capable of achieving its intended effects; whether this regulation is necessary to protect the public interest with which it is connected; whether the effects of the introduced regulation are in proportion to the burdens it imposes on the citizen. "

2 Personal data protection and operational activities

A citizen of a modern state that is entering the era of the information society expects protection against new threats to privacy. The simplicity of creating user profiles contributes to the ease of collecting information and poses serious threats related to the manipulation of personal data. The subject of data protection in the context of the constitutional principle of information autonomy has been the subject of interpretation of many judgments. As one of the examples can be given the judgment of September 21, 2005 (Fundowicz & Świtał, 2014:56), in which the Provincial Administrative Court ruled that "by applying the provisions of this Act on the protection of personal data, it is necessary to weigh the goods on which it is based each time. In practice, the right to the protection of personal data is limited due to the public interest or the justified interest of other people, i.e. it is not an absolute right, like most constitutionally protected rights. Further in the statemnts of grounds to the judgement, the Provincial Administrative Court states: The provisions of the Act cannot be understood in such a way that disclosing the debtor's personal data for the purpose of debt collection violates the good of that person, as it would be unjustified favoring him. When concluding a civil law contract, one should take into account its consequences, as well as the fact that the obligation to perform the contract applies to both parties, even if one of them is a consumer. The protection of some

goods cannot lead to violate the rights of others, which can be directly or indirectly derived from many provisions of the Polish Constitution. In accordance with Article 51 2 of the Constitution of the Republic of Poland "Public authorities shall not acquire, collect nor make accessible information on citizens other than that which is necessary in a democratic state ruled by law. As indicated by the Legislative Council acting at the Prime Minister, in its opinion of 22 June 2018, "Acquiring", "collecting" and "making accessible infromation", referred to in the above provision, can be considered as constituting "processing of personal data" within the meaning of legislation. Provision of Article 51 2 of the Constitution of the Reuplic of Poland means, therefore, that the processing by the public authorities of "information about the citizen" - that is, information enabling the person to be identified - is permissible only if it is necessary in order to achieve an objective justified by the public interest. The above provision should be read in conjunction with Art. 31 section 3 of the Constitution of the Republic of Poland, expressing the general principle of proportionality of state interference with the freedom or rights of individuals. The necessity criterion which is referred to in the Article 51 section 2 of the Constitution of the Republic of Poland, however, does not apply to information that does not allow identifying a given person (e.g. due to anonymisation), or in a situation where identification of a person is significantly difficult (e.g. due to pseudonymisation). With regard to the processing of this type of information, the legislator's freedom is much wider, which means that such information can be processed not only in situations where it is necessary in a democratic state to protect the values listed in Art. 31 section 3 of the Constitution of the Republic of Poland.
After entering into application on May 25, 2018 Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation "GDPR"), *the role of professional support for data controllers and processors is played by data protection* officers (called "DPO"). The task of data protection officers - just like currently Information Security Administrators (ISA) is to act in accordance with data protection law-compliant data processing, both in public administration and the private sector.

The GDPR is an act that is binding in member states directly, without the need to issue legal acts implementing them to the national order. The Directive of the European Parliament and of the Council (EU) 2016/680 will also be a novelty in the Polish legal system, as the principles contained in this act are not present in the Polish legal regulations existing today. In the directive, the provisions regarding the data protection officer are shaped similarly to the GDPR. The status and tasks of the officer were regulated in a similar way, except that the provisions of the Directive, unlike the Regulation, require implementation by our legislator.

Another important act regulating personal data protection issues in the context of operational activities is the Directive (EU) 2016/680 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 by competent authorities for the purposes of crime prevention, conducting preparatory proceedings, detecting and prosecuting criminal offenses and

enforcing penalties on the free movement of such data and repealing the Council Framework Decision 2008/977 / JHA. In the new Directive, the general principles of data protection apply to police cooperation and judicial cooperation in criminal matters. The provisions of the directive concern data transfers, both domestic and for cross-border transfers.

The European legislator has intentionally excluded from the scope of application of Regulation 2016/679 the processing of personal data by competent authorities for the purposes of crime prevention, conducting preparatory proceedings, detection and prosecution of prohibited acts or execution of penalties, including protection against threats to public security and prevention of such threats, regulating these issues - due to the special nature of such activities - in a legal act of another rank, i.e. Directive 2016/680. An important reason for adopting such a solution was on the one hand the need to ensure a consistent, high level of protection of personal data of individuals, and on the other hand to facilitate the exchange of personal data between competent authorities of Member States enabling effective cooperation in criminal matters and police cooperation, as well as ensuring the possibility of data transfer to a third country, provided that the purpose of such action is to prosecute crime while ensuring an adequate level of data protection by the third country. At the same time, the Directive includes among the competent authorities - in addition to public authorities such as the Police or other law enforcement authorities - any other authority or body to which the law of a Member State entrusts the exercise of public authority and the exercise of public powers for the purposes set out in Directive 2016/680. Law enforcement authorities will therefore have to comply fully with the principles of purposefulness, adequacy and legality. This trend is also reflected in the possibility to appoint the same supervisory authorities.

Directive 2016/680 regulates the exchange of information regarding personal data between law enforcement authorities of the Member States of the European Union and third countries. The existing regulations in this area, in the form of the repealed Directive 95/46/EC of the European Parliament and of the Council, were applicable to all processing of personal data within Member States, both in the public and private sectors. However, it did not apply to the processing of personal data "in the course of an activity which falls outside the scope of Community law", such as activities in the areas of judicial cooperation in criminal matters and police cooperation. Similarly, the repealed Council Framework Decision 2008/977/JHA was applicable to judicial cooperation in criminal matters and police cooperation limited to the processing of personal data sent or made available only between Member States. These regulations turned out to be insufficient due to the dynamic development of cross-border and international crime, which is largely the result of technological progress in the field of information exchange. In Polish legal realities, the issues of personal data protection are reflected in a number of other acts regulating the operation of law enforcement and judicial authorities, as well as other entities operating within the sphere of the subjective scope of Directive 2016/680. One of

the key legal acts currently regulating these issues is the Act of 14 December 2018 on the protection of personal data processed in connection with preventing and combating crime.

The reform of the rules for the processing and protection of personal data in the European Union was also caused by the need to ensure more effective protection of individuals' data, due to the rapid pace of technological changes resulting in an increase in the amount of processed data. The existing legal instruments were not sufficient, which meant that personal data of individuals was increasingly exposed to a threat. One of the main assumptions of the new regulations is to maintain balance between the right to privacy and the necessity for the Police - and other entities operating in the area of preventing and combating crime, including protection against threats to public security and order and prevention of such threats - to maintain confidentiality in data processing in proceedings conducted by competent authorities in this respect. The Act also uses the recommendations formulated in the opinion on the implementation of Directive 2016/680 of the Article 29 Working Party on Personal Data Protection (17/EN WP 258 Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), adopted on 29 November 2017.

The above-mentioned rules constitute the basis for fulfilling the obligations of the State and public authorities in ensuring public safety and order. Actions taken by the services are actions taken in the public interest in the exercise of public authority.

3 Privacy protection and the responsibility of digital service providers

Over the past few years, we have seen an increase in the popularity of on-demand audiovisual services. The development of means of communication and dissemination of content changes the view not only on technological issues related to the transmission of information in the communication system. Increasingly, such services are offered by various types of providers (operators of digital satellite platforms, website operators or mobile phone operators - in a word, digital service providers), which significantly expands the range of entities actively participating in the communication process. There is no doubt that the medium, which is the internet, allows the provision of audiovisual media services on demand to the extent that was not possible before, due to technological restrictions. Appropriate applications, available in the most popular operating systems of various devices, allow you to access these services anytime, anywhere. It should be noted that providers of electronic communications services are often also providers of on-demand services. However, the essence of the latter is completely different, because the basis of electronic communications services is the transmission of signals in electronic communications networks, while on-demand audiovisual services provide content. The basis of the differences between these services is consequently the scope of responsibility for the content transmitted. The information carrier itself, by means of which the content is transmitted, cannot constitute a decisive criterion for assessing whether the liability related to the provision of a given type of service falls within the limits of the media law

system or is excluded from it. This responsibility also involves the right to privacy and identity protection.

On the one hand, it should be assumed that if the purpose of the action is to publicly disseminate information, opinions or thoughts through any medium, such activity should be subject to the standards of protection of fundamental rights adopted in the classic, traditional approach. On the other hand, it should be emphasized that in the current development conditions of digital services, especially the one closely related to the freedom of expression and communication is not restricted only to large media companies, it is often associated with a monetary goal and may become an area of marketing interaction between the content provider and its user with the risk of entering the private sphere of the latter.

Constant conflicts of various goods and interests also occur in the conditions of development of new digital services. An example of such a conflict is on the one hand the protection of privacy and on the other hand the freedom of expression. Responsibility for audiovisual media services, covered by the fundamental right to freedom of expression, may be limited. Such a situation will take place if it is necessary to reconcile the freedom of expression with the provisions relating to the protection of privacy, or vice versa, when the provisions related to the right to privacy will be limited by the requirements related to certain concessions for the freedom of expression. All such restrictions must be dictated by reasons of security or public order, or the protection of the environment, public health and morality, or the freedoms and rights of others. Provided that these restrictions may not violate the essence of freedom and rights.

There is no doubt that the development of digital services will be more and more dynamic in the future. These types of services give the recipient an opportunity to choose unprecedented in the age of traditional media, because unlike a traditional system, the recipient decides what kind of services will be provided to him. In the current legal situation, the issue of responsibility for the content transmitted in this way, digital content seems to be established. However, the opportunities offered by new technological solutions are associated with many moral dangers, which in turn creates legal controversy, and sometimes even a sense of legal uncertainty. In a situation where the recipient indirectly gives the digital service provider the opportunity to learn their preferences and a number of other information about himself that can be used by the service provider even in its advertising activities, the recipient is not, or for various reasons, can not be fully aware of how the information provided as part of this particular interaction with the service provider will be used in the future.

Reflection on the sphere of privacy has accompanied mankind for centuries and is present in various philosophical concepts. Over the years, both judicial decisions and doctrine have broadened the scope of the notion of the right to privacy, indicating further spheres of privacy and giving this law a fundamental character. It is declared and protected at all

levels of regulation. H. Wang N. Kee and C. Wang in the article *Consumer Privacy Concerns about Internet Marketing* (1998:63) proposed systematics of violations of the right to privacy in the sphere of information autonomy.

The first category that the authors distinguish are violations of unauthorized access to data. Another category is the unauthorized collection of data, which consists of collecting data from the internet without notifying the consumer. According to the authors, this type of information is: e-mail address, type of software used to browse the Internet, web browsing history, private files or databases. The category of prohibited monitoring consists in monitoring the consumer's activity on the Web without his notification and consent. By using *cookies*, websites can collect information about consumer activities on the web. Illegal analysis is an infringement of analyzing the consumer's private data without notifying him. Such analyzes can lead to conclusions including patterns of consumer behavior and preferences related to buying. Violations in the category of unauthorized transfer are violations related to the transfer of private consumer information to another entrepreneur, without his notification and consent. Internet companies often sell, publish and distribute their clients' databases containing private information. Another category of violation, highlighted in the cited article, is the unwanted offering of its services. The last category of violations is illegal storage. This violation consists in storing private consumer information in a way that does not meet the relevant security standards, enabling unauthorized access to this information.

In the context of the abovementioned violations of the right to privacy, it should be emphasized that in practice the digital service provider has the ability to collect a wide range of data regarding each recipient - his preferences related to the program offer, habits, etc. Thus, it is possible to use this data for marketing purposes. Thus, the supplier may directly or indirectly present the personalized advertising offer to the consumer, using the data collected in this way. He may also abuse this information by going to dishonest practices. This issue is important because of the specific nature of the relationship between the digital service provider and the consumer. Technological changes have affected the scope of liability for criminal acts related to information and for the provision of electronic services. New rules related to the limitations of this liability have emerged. In EU law, the liability of online service providers is regulated by Directive 2000/31/EC. This directive includes provisions related to the most popular network services*: mere conduit*, caching and hosting. It should be emphasized here that European regulation adopts a horizontal model. This means that the exclusions it provides apply to all legal liability, including civil, criminal and administrative liability. The e-commerce directive creates rules for exclusion of liability at the maximum level. Therefore, individual Member States may decide to introduce less restrictive solutions.

The implementation of the provisions of the Directive on electronic commerce in Polish law are Art. 12-15 of the Act on Rendering Electronic Services. In accordance with Art. 12 of this Act, referring to the *mere conduit* service, the person who by transmitting data:

1) is not the initiator of the transmission, 2) does not select the recipient of the data and 3) does not delete or modify the data being the subject of transmission, is not responsible for the information provided. The exclusion of liability referred to in paragraph 1 also covers the automatic short-term intermediate storage of transmitted data, if this action is only intended to carry out the transmission and the data is not stored longer than it is normally necessary to carry out the transmission (*caching*) (Article 12 Sec. 2 of the Act on Rendering Electronic Services). *Caching* - a word etymologically derived from the French word cacher, *which* means to hide, conceal, and is an automatic process of creating a temporary copy of digital data in order to allow greater availability of data for frequent use265. The admissibility of caching as an exception to the reproduction right is provided for in Article 5 Section 1 of Directive 2001/29/EC. This provision sets out the principle that cases of temporary reproduction of works, of a temporary or incidental nature and constituting an integral and essential part of the technological process, the sole purpose of which is to enable transmission in the network between third parties through an intermediary or to enable the lawful use of a work or other protected good, are excluded from reproduction.

In the case of the caching service, the exclusion of liability for stored data applies to the entity that transmitting them and ensuring automatic and short-term indirect transmission of these data in order to accelerate re-access to them at the request of another entity: 1) does not delete or modify the data, 2) uses recognized and IT techniques usually used in this type of activity specifying technical parameters of data access and updating, and 3) does not interfere with the use of IT techniques recognized and usually used in this type of activity in the field of collecting information on the use of collected data (Art. 13, Section 1 of the Act on Rendering Electronic Services). Therefore, respecting the integrity of stored data remains a necessary condition to avoid legal liability. In accordance with Article 13, section 2 of the Act on Rendering Electronic Services the person who shall not be liable for the stored data is the person who, under the conditions referred to in paragraph 1, immediately deletes the data or prevents access to the stored data when he receives a message that the data has been deleted from the initial transmission source or access to them has been prevented, or when the court or other competent authority ordered the deletion of data or access to them, storage of data by the recipient, they are not aware of the unlawful nature of the data or related activities, and in the event of receiving official notification or obtaining reliable information about the unlawful nature of the data or related activities, they will immediately prevent access to such data.

Regardless of the issues related to the processing of the information itself, the liability of the digital service provider is also related to the content of the transmitted information. To assess the degree of legal protection in this area, first of all the regulations contained in the provisions relating directly to on-demand audiovisual media services should be analyzed.

4 Content regulation on the Internet

The issue of security in the network and the network itself is determined by the development of new technologies, digital processes and the progress of computerization of the state. The basic issue of legal protection in the new media system - of all kinds - is determining the subjective and objective scope of liability for the content made available. An example of problems with determining responsibility for online activities is determining responsibility for content made available in the media. It should be assumed that the scope of editorial responsibility covers all entities that process digital content that have their registered office or place of residence in the territory of the Republic of Poland or in a third country, provided that the content is processed using technical means located on the territory of the Republic of Poland.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce in the internal market, was of fundamental importance for the development of e-commerce. The EU and national legislator also identified three basic types of services provided through intermediaries on which the three-level responsibility depends. The first range of the so-called *mere conduit* means ordinary transmission services – consisting of passive participation in data transmission in the network only for the purpose of data transmission. In the light of Article 12 section 2 of the Act on Rendering Electronic Services on the exclusion of liability also applies to situations when the storage and transmission of data is automatic and short-lived, and most importantly, "if this action is only for the purpose of carrying out the transmission and the data is not stored longer than is normally necessary to complete the transmission". The second scope covering the so-called *caching* is a service consisting of automatic and short-term indirect storage of data, the purpose of which is to accelerate re-access to them. The purpose of this service is to increase the efficiency and speed of the system. Data storage under *caching* differs from *mere conduit* mainly in the period of storage of these data, because in the case of *caching*, the storage period is definitely longer than what is actually necessary for the transmission.Pursuant to the provision of Article 13, section 1 of the Act on Rendering Electronic Services, service provider that provides *caching* service, will not be responsible for automatic and short-term indirect storage of data if:

1) he does not change the information stored;
2) observes the conditions of access to them and their updating;
3) does not interfere with the use of permitted and special IT techniques used in this field in the collection of information on the use of collected data;
4) immediately deletes or prevents access to stored information if it receives notification that it has been removed from the initial transmission source or access to it has been prevented, or when a court or other competent authority has ordered the removal or disabling the access to it.

The third range is the so-called *hosting* – this term means sharing the memory of servers connected to the network to store various types of data that comes from the recipient himself. The main feature of *hosting* that distinguishes it from *mere conduit* and *caching* is the so-called source storage, which means spontaneous and unlimited storage of data and making them available to other entities. In accordance with Article 14 section 1 of the Act on Rendering Electronic Services, the entity providing the hosting service will not be responsible for the stored data against the person whose rights have been possibly violated, if they are not aware of the unlawful nature of the data or related activities. Lack of knowledge about the unlawful nature of data means that the service provider cannot have knowledge that the data stored by them is contrary to the law or principles of social coexistence. Consequently, the *hosting provider* will be responsible for the stored data if they know it and know about its unlawful nature.

The question here is whether and to what extent these regulations apply to providers of audiovisual media services on demand. Certainly, these provisions apply when the providers of electronic communications services are the same entities that also provide on-demand audiovisual media services. As already mentioned, the provisions of the Act on Rendering Electronic Services do not apply, inter alia to:

1) dissemination or distribution of radio programs or television programs and related text messages within the meaning of the Radio and Television Act, with the exception of programs distributed only in the ICT system;
2) the provision of telecommunications services by a telecommunications undertaking, with the exception of Articles 12-15.

Therefore, on-demand audiovisual media services would be subject to the provisions of the Act in the relevant, i.e. the broadest scope of liability, as related to the responsibility for the content provided. In addition, these services will meet the conditions for applying the provisions of this Act. The service provided electronically, subject to the provisions of this Act, should jointly meet the following conditions:

1) the service is performed by sending and receiving data using ICT systems;
2) the service is performed without the simultaneous presence of the parties to the contract;
3) the service is provided at the individual request of the recipient.

The scope of liability of the provider of audiovisual media services is influenced by the type of these services. If we assume that we are dealing with a service that meets the definition of the press, such activity is subject to the provisions of this Act regarding the right to privacy. However, if they are audiovisual services on demand, then the relevant regulation can be found under the provisions of the Radio and Television Act using subsidiary provisions of the Press Act.

In each case, the responsibility of the same entity will be different depending on whether they conduct service activities referred to in the Act on Rendering Electronic Services, or

is a provider of audiovisual media services on demand or "only" publisher. As already indicated, as a result of technological as well as economic convergence, the same entity can perform all of these functions. This situation indicates the need to synchronize issues at each stage of substantive arrangements as to the nature of the service. This is an essential element of a coherent regulatory framework system enabling the development of on-demand audiovisual media services, taking into account elementary standards ensuring the right to privacy.

The type of service influences the liability of the website provider. If we assume that we are dealing with a service that meets the definition of the press, such activity remains an activity subject to the press register in accordance with the procedure set out in the Press Act (Article 20 of the Press Act – a register in the district court with jurisdiction over the publisher's seat; services of audiovisual media service providers are exempted from such an obligation pursuant to Article 24 of the Press Act). However, if they are audiovisual services on demand, then the relevant regulation can be found under the provisions of the Radio and Television Act (Article 41 of the Radio and Television Act – KRRiT register or concession depending on the nature of dissemination - the register in the case of programs disseminated in ICT systems), but if the content provider is also the sender, he will have to apply for a concession (Article 33 of the Radio and Television Act - KRRiT license).

The aforementioned examples justify the thesis that in each case the responsibility of the same entity will be different depending on whether it conducts service activities referred to in the Act on Rendering Electronic Services, or is the sender or publisher. As a result of technological and economic convergence, the same entity can perform very different functions and it is not a foregone conclusion that its status is and thus the scope of responsibility is finally established. This situation indicates the need to introduce appropriate regulations, subject to the need to synchronize issues at every stage of substantive legislative activities. This is an essential element in creating a coherent system of regulatory frameworks in the media system.

The right to privacy is one of the most common violations on the web. This phenomenon is related to the problem of the lack of proper regulatory solutions, especially in this space where private interest with the public interest is at stake. Privacy is the highest value, as it should be protected in the network, at the same time actions to exclude threats or counteract online crime also require certain restrictions with respect to privacy. Privacy is a good that is of value not only for the individual, because we can speak of it as an economic good, of significant economic value. According to M. Catinat, "most attempts to heal the current legal situation fail due to business lobbying (including the advertising industry), federal intelligence agencies and other institutions. All of these entities have an interest in maintaining easy access to individual data" (Catinat, 1997:53). This duality of the importance of personal data contributes to the difficulties in their legal protection. Currently, most network users have an account on the social networking site Facebook.

Every time an Internet user is a user of this website, Facebook receives newer and newer data about this person. The website has access to information about a computer, mobile phone or other devices that are used in everyday communication. Therefore, each action is controlled. By publishing various materials, Facebook reserves the right to obtain further information about where and at what time, e.g. a given photo or video was taken. The portal also works with the GPS system. It stores recent user location data in order to send relevant notifications. Facebook also provides information about us, such as age, place of origin or even a list of friends to various applications, as well as advertisers. The rules for the use of data by the portal (privacy policy) do not include information on how to store information. It is therefore uncertain whether the data is properly protected. The user has no influence on who uses their data. In the document containing the "Data protection rules", it reads as follows: "We always receive data about you when you use Facebook, for example by browsing another person's timeline, sending or receiving messages, searching for a person or page, clicking and displaying content or using them in a different way by using the Facebook application for mobile devices or making purchases on Facebook", as well as "The user allows us to use their name, profile picture, content and information in connection with commercial content provided or enriched by us, sponsored or similar (such as the brands they like)". It should be added that the fate of all songs shared on the forum is unknown. The Regulations reserve the administrator the right to grant sub-licenses to further share od any materials that have been found on Facebook on a global scale. A characteristic element of the portal is total control over the website user, while they themselves cannot maintain any control over the fate of the information placed. The privacy policy presented here is a classic example of the regulations, in which the portal reserves the right to a wide range of data processing, while obtaining, of course, financial benefits in the form of a database and a set of information about its users. These types of information processing policies often allow further actions, which are not necessarily in accordance with our will or the law.

Chapter V

Exercise of the Right to Privacy Versus Security and Public Order – Conflict of Interests

1 Public subjective rights and privacy protection

Public subjective law is a concept closely related to the rights and competences acquired by an entity under a specific legal relationship related to the entity's situation in public law (Bigo, 1928; Jaworski 1924; Szpunar, 1947; Jakimowicz, 2002). According to Z. Ziembiński (1980:365), this is a concept referring to a set of functionally related freedoms, rights and competences of a given entity.

Public subjective rights externalize the fundamental rights arising from the Polish Constitution, features of public subjective rights indicate their separate nature from fundamental rights, because public subjective rights arise as a result of establishing an administrative and legal relationship. Public subjective law may also contain negative content, which is manifested in the entity's right to claim the administration to refrain from interfering in the sphere of previously recognized freedom (Kulesza, 1985:135). Therefore, as part of these considerations, the issue of protecting the privacy of individuals should be analyzed in the context of the powers of public authority in its organizational and regulatory role. The individual citizen-state relationship as well as the rights to perform the organizational and regulatory function of public administration should be considered taking into account the concept of duty. This is due to the fact that the state has an obligation to protect fundamental freedoms and rights of man and citizen, including the right to privacy. In the traditional science of administrative law, to illustrate the relationship between the individual and the state, arising from public subjective law, an analogy to private law was pointed out, in which area the individual in relation to public authority remains in the same relationship as the creditor (individual) to the debtor (public authority). However, this does not mean that the purpose of public authority are the particular interests of individuals. The protection of civil rights and freedoms remains in the public interest. The construction of public subject law determines the status of the individual vis-à-vis public authority.

When determining the basis for the rights of the individual citizen by referring to public institutions of subjective rights, attention should be paid to the issue of right and obligation. The legal situation of the individual citizen consists of a number of specific rights, including fundamental rights, the implementation of which takes place, as already indicated above, at the level of often difficult relationships of the individual - public administration. It is the sphere of administrative law and the competence norms of

administrative bodies resulting from it that set the limits of state interference in the rights and freedoms of the individual. At the same time, the individual citizen is obliged in certain situations to perform certain behaviors. We are then talking about the obligation to act or inaction.

According to J. Bocia (2010:444), obligations and entitlement are two contemporary types of behavior characteristic for the relationship between the state and the administrative body within the administrative law relationship. With the proviso that, compared to civil law relationships in which this correlation of rights and obligations as the basis for the actions of its parties occurs, in the administrative law sphere the administrative body is not the recipient of the citizen's behavior, but only the entity designating and verifying or enforcing this behavior. However, the citizen does not fulfill the obligation to the administrative authority but under its control. This means that both in the situation of the citizen's obligation as well as the norm of the established entitlement, specific behavior of the administrative authority authorized by the regulation of the law is his obligation (Boć, 2010:444). At the same time, this does not mean that the citizen is not subject to coercion.

The goals of the state are connected with the obligations of an individual - a citizen. The goals of a police and law-abiding state differ radically. According to W. Kawka (1939:25), "In a police state, a citizen is threatened with coertion at every turn, while in a law-abiding state a citizen has a lot of freedom and coertion is excluded at least from some areas of his life. Coercion is a phenomenon that is inseparable from a state organization, therefore it is impossible to exclude it at all and at the same time maintain a state organization, so a law-abiding state applies it as well, although not in every area of an individual's life". A reservation should be made here that the action of a public authority includes also omission. The concept of an "action" of a public authority body has no constitutional definition. This concept includes both the active behavior of this body as well as omission. The scope of the definition of "active actions of a public authority" includes individual decisions. On the other hand, the notion of omission of public authority is associated with situations in which the obligation of a specific action of public authority is specified in detail in a legal provision and it can be determined what exactly would be the behavior of a public authority.

The limits of freedom and civic rights are determined by legal norms determining the scope of competence of public authorities acting to protect the public interest. The correlation between public interest and private interest, the interest of the individual, is important here. Personal safety and public security will also compete here. Where human life is regulated by law, there is a restriction of liberty. Therefore, it can be said that the restriction of individual freedom results from the essence of the right norm. These restrictions occur more clearly in the sphere of public law, especially administrative law. Public law pursues a public interest and this has an advantage over private, so in the event

of a conflict of both interests private will give way to public - and personal security will give way to public security - in this way the freedom of individuals is limited.

In the case of offenses in the private sphere of the entity, the administrative body, even if it is required to comply with fundamental rights, must apply the law. According to W. Kawka (1939:91), this is the only way for the operation of state organs and consists in applying laws. It follows that the construction of fundamental rights in a law-abiding system loses its meaning, and the claim that fundamental rights form the boundary of the activity of state organs is deprived of proper grounds. W. Kawka (1939:96) argued that only laws set the boundaries of state bodies and not some soulless fundamental rights. At the same time, it should be emphasized that this is not synonymous with the fact that the administrative body is to apply the law in a soulless manner. According to O. Mayer, in carrying out protection of security, peace and public order, the police authority is obliged to use the necessary means, not any means. A strategic approach to views on security, peace and public order is not a state police task. It is the subject of arrangements under the so-called public custody. Today we will say that it concerns arrangements at the level of strategy and *state policy*.

2 The individual citizen as a subject of personal rights and obligations

The individual's situation in the context of their personal rights and obligations includes both obligations, which may include the above-mentioned personal rights and freedoms, which are listed in the catalog of the Basic Law, as well as a number of other rights and freedoms that have not been explicitly and directly specified. The basic right is the right to life and personal freedom. These include the right to physical integrity, the right to inviolability of residence, the right to secret communication and sharing information about yourself, the right to live in a family. These are just a few rights and freedoms from a wide catalog of rights and freedoms. Administrative law refers to these rights and freedoms by granting competences to specific administrative bodies including obligations and rights towards the individual citizen. The limits of the rights and freedoms of the individual citizen are evidenced by the scope of public administration rights determined, as already indicated above, in competence norms, as well as the scope of the obligations of the individual citizen, which relate to personal rights and freedoms. The right to personal integrity is closely linked to the basic right to life.

In the judgment of 9 June 1998 (file no K 28/97), the Constitutional Tribunal, in a case concerning the constitutionally admissible scope of limiting the right to a professional soldier's court in cases of military service of professional soldiers, referred to the essence of the legal relationship, which is the service relationship connecting a professional soldier with state organs. The Constitutional Tribunal indicated that "the service relationship of professional soldiers is based on subordination to military authorities and the possibility of unilateral shaping of the status of professional soldiers by these authorities. One of the basic elements of the service relationship in the army is the

obligation to comply with orders issued by superiors. Professional nature of service requires, by its very nature, full availability and dedication. Persons joining this service submit voluntarily to its rigors".

The Constitutional Tribunal distinguished matters of service subordination, matters belonging to the sphere of internal military administration, from matters of "service relationship" in which a soldier asserting his rights acts as the subject of rights and obligations which he is entitled "within the scope of service relationship". The Tribunal considered that in this sense the internal sphere should be combined with matters that arise "as part of official relations" and not "from official relations". According to the Tribunal, only cases "from official relations" are covered by the constitutional right to court, which results in the possibility of limiting the right to a professional soldier's court in cases related to ensuring that the Armed Forces can implement the tasks and objectives set out in Article 26 of the Constitution, i.e. protecting the independence of the state and the indivisibility of its territory, and ensuring the security and integrity of its borders.

Restrictions on exercising the constitutional rights of individuals are permissible if they are necessary in a democratic country to implement one of the values listed in Article 31 (3) of the Constitution, in this case security, may also be introduced in official relations with special characteristics, which is the public service of a professional soldier. In the opinion of the Constitutional Tribunal, the rights and obligations of professional soldiers are closely related to the requirements arising from Article 26 of the Constitution (The Armed Forces of the Republic of Poland serve to protect the independence of the state and the indivisibility of its territory and to ensure the security and integrity of its borders. The Armed Forces remain neutral in political matters and are subject to civil and democratic control). The Tribunal has found that restrictions on access to the court of a professional soldier in cases related to ensuring that the Armed Forces can fulfill their tasks and goals, which are the protection of the independence of the state and the indivisibility of its territory, as well as ensuring the security and integrity of its borders, meet the necessity requirement. It would not be possible to reconcile the coherent and efficient operation of the Armed Forces with full judicial control over the decisions of superiors regarding matters related to the service relationship of professional soldiers. Ensuring adequate defense potential of the state is the primary goal over the rights and freedoms of the individual, and limitations of these rights are in accordance with the principle of proportionality (see the judgment of the Constitutional Tribunal of 12 July 2012, file no. SK 31/10, OTK ZU, no 2012, items 80).

3 Freedom of speech and confidentiality of correspondence

Freedom of expression and the right to disseminate information are guaranteed in Article 54 (1) of the Polish Constitution referring generally to the freedom of expression and the acquisition and dissemination of information. This provision remains in connection with

Article 14 of the Constitution, which states that "the Republic of Poland shall ensure freedom of the press and other means of social communication".

Freedom of expression is one of the foundations of a democratic society, a condition for its development and self-fulfillment of individuals. This freedom cannot be limited to information and views that are received favorably or viewed as harmless or indifferent. The role of journalists is to disseminate information and ideas on matters of public interest and significance. This is closely related to the public's right to receive information. Freedom of expression may experience restrictions. However, there is no doubt that the most elementary condition for restricting this freedom is the requirement of statutory regulation. Due to the fundamental role of freedom of speech in a democratic state ruled by law, it is particularly strict to control the precision of the provisions of laws introducing restrictions on the exercise of this freedom.

In accordance with Article 49 of the Constitutionof the Republic of Poland freedom and protection of confidentiality of correspondence, are guaranteed, which may be *restricted* only in cases specified in the Act and in the manner specified therein. This provision ensures the right and freedom of communication and the protection of confidentiality of correspondence, and thus essentially concerns two rights and freedoms closely related to each other and often covered in the literature by the term "right to communicate". It should be emphasized, however, that freedom of communication is one of the consequences of broadly understood civil and personal freedom, encompassing all forms of communication between people, while the secret of correspondence is a much narrower concept, associated primarily with the right of everyone to respect their private life, their right to keep secret the content of the message addressed to other persons or institutions.

3.1 Wiretapping

The issue of wiretapping is related to issues regarding freedom of communication. An example of the restriction of the right to privacy are the provisions governing the admissibility of wiretaps contained in Article 237 of the Code of Criminal Procedure[1] and in Article 19 of the Police Act of 6 April 1990. In the context of access and the right of data preservation, attention should be paid to the issues of telecommunications wiretapping. This issue is regulated by, among others Chapter 26 "Control and consolidation of conversations" of the Code of Criminal Procedure. Article 241 of the CCP decides that the provisions of this chapter shall apply mutatis mutandis to the control and recording by technical means of the content of other conversations or information transfers, including correspondence sent by electronic mail. Thus, the scope of operational activities undertaken is wide. In a judgment of 19 September 2000 (file no V KKN 331/00), the Supreme Court explained that "Article 237 of the Code of Criminal Procedure only applies to telephone wiretapping carried out in the course of proceedings pending in Poland, and the formal conditions of wiretapping legality provided for in it (e.g. management or approval by the court) cannot be required when establishing the

legality of wiretapping by the authorities of another country. The legality of the telephone wiretapping carried out by the authorities of a foreign country in the context of pending proceedings should be assessed in accordance with the provisions in force in the country in which the activity is carried out." In addition, the provisions of the chapter shall apply accordingly to control and to the recording by technical means of the content of other conversations or information transfers, including electronic mail. In accordance with Article 242 of the Code of Criminal Procedure, the Minister of Justice, in consultation with the minister competent for computerization, the Minister of National Defense and the minister competent for internal affairs, defines by way of ordinance the method of technical preparation of networks used to transfer information, to control telephone conversations or other transfers of information made using these networks, the method of making, registering, storing, reproducing and destroying records of controlled telephone conversations and the content of other conversations or information transfers, including e-mail correspondence, bearing in mind the need to properly protect the records made against their loss, distortion or unauthorized disclosure.

Process wiretapping and operational wiretapping are legal as long as they relate to the catalog of the offenses listed therein, as well as in a situation in which a district court, in the face of specific conditions and with certain procedures being followed by law enforcement authorities, agrees to them (see judgment of the Supreme Court of 24 October 2000, file no V KKN 331/00, Lex no 332949). The limits set by the legislator specifying the conditions of admissibility of wiretapping orders exclude any deviation from this legal rule. Even the public interest cannot justify breaking the rules governing the search for and obtaining evidence from telephone wiretapping, as this would undermine the constitutional protection of civil rights. In the judgment of the Court of Appeal in Lublin of 18 May 2009 (file no II Aka 122/08), it was found that the finding of the illegality of wiretapping causes that this evidence loses its raison d'être and cannot be used in proceedings, i.e. taken into account when passing the sentence even despite the reproduction of the medium containing the registration conversations held. The Court of Appeal in Poznań made a similar statement in its judgment of 10 January 2008 (file no I Aca 1057/07, OSA 2009, no 11, pp. 56-71) regarding evidence of wiretapping in civil matters. The insidious recording of a private conversation violates the constitutional principle of freedom and protection of communication. Evidence of this type obtained in a manner contrary to the law, even if its use was justified also by reasons of national security, should not in principle be admitted in proceedings.

3.2 Anti-terrorist activities

According to ECtHR case law, interference with private life and correspondence is not only individual secret control measures directed against designated entities, but also strategic monitoring of connections and obtaining related personal data of communicating entities. This issue was considered in the *Weber and Saravia v. Germany* case, which challenged the German provisions regulating the strategic monitoring of

telecommunications connections, consisting in recording telephone conversations of an unspecified group of interlocutors, and then identifying, using keywords, information contained in those conversations, which may potentially identify the perpetrators of crime or plans to commit them (Case *Weber and Saravia*, No. 54934/00). The entry into the sphere of privacy of an individual is also the collection and storage of data on individuals by state services, regardless of the way in which they were collected (Case *Rotaru v. Romania*, complaint No. 28341/95). To assume that there has been an interference with the right guaranteed by Article 8 of the ECHR, it is sufficient to establish that data on units has been collected, regardless of how they will be used in the future. However, the admissibility of secretly obtaining information about persons by public authorities was not denied at all. The Tribunal even indicates their necessity as a tool enabling effective guarantee of security and protection of institutions of a democratic state against sophisticated forms of threats, in particular espionage or terrorism (see the judgment in the case of *Klass and Others v. Germany*, complaint No. 5029/71).

Standards for the collection and processing of data by the competent authorities are laid down in the judgments in *Zakharov v. Russia*, complaint No. 47413/06 or *Szabó and Vissy v. Hungary*, complaint No. 37138/14. The complainant used the services of several networks of mobile operators.

On 23 December 2003 Zakharov brought a case against three network operators, claiming that they violated his right to privacy of telephone communications. He submitted that, in accordance with Regulation No. 70 of the predecessor of the Ministry of Communication, telephone network operators had installed a device that enabled the Federal Security Service to intercept telephone conversations without prior court permission. Regulation No. 70, which was never published, unduly limited his right to privacy. Roman Zakharov asked the court to issue an order to remove the device installed under Regulation No. 70, and to make telephone communications available only to authorized persons. Laws in Russia regulating the interception of communication transmissions do not provide adequate and effective guarantees against the risk of fraud, which is inherent in any surveillance system, and which is particularly high in a system where special forces and the police have direct access, through technical means, to all telephone communications. In particular, the circumstances in which public authorities are authorized to use secret surveillance measures are not clear enough. The provisions on discontinuing covert surveillance measures do not provide sufficient guarantees against arbitrary interference. National law permits the automatic storage of inadequate data and it is not clearly defined in which cases the capture material will be stored or destroyed after the process.

Authorization procedures cannot ensure that secret surveillance measures are ordered only when it is "necessarily in a democratic society". The supervision over interception of communications does not currently meet the requirements of independence as well as those related to the entrusted authority and competences that would be sufficient to perform effective and constant control. The effectiveness of remedies is impaired by the

failure to notify the person whose communications are being intercepted or by the lack of adequate access to interception documents. It would be contrary to the rule of law to give the executive organs unfettered discretion in matters of national security. The law must indicate the limits of any decision-making freedom granted to the competent authorities and the manner in which it is exercised with sufficient clarity, bearing in mind the legal purpose of these measures, so as to give individuals adequate protection against arbitrary interference. This requires prior judicial authorization, which is a significant safeguard against arbitrariness.

Similarly, the European Court of Human Rights found that the Hungarian Police Act violates the right to privacy. After the changes introduced in 2011, the Act allows special anti-terrorist units to covertly search house, install wiretaps, open letters and parcels, as well as uncontrolled browsing and recording of electronic correspondence. The Court reiterates consistently: provisions regarding the powers of special forces should provide for strong control over their activities and for informing citizens about surveillance. In the case of *Szabo and Vissy v. Hungary*, the Court held that the contested provisions could affect any person residing in that country and any property located there, and citizens did not have any means of verifying whether they were under supervision. According to the Court, the introduction of special powers for the forces to fight terrorism is justified, however, Hungary should at the same time guarantee sufficient protection for the rights of its residents. The law should indicate that wiretapping and intercepting communication is possible only against persons suspected of being terrorist. The measures taken should be subject to external, preferably judicial, follow-up control.

The Court also criticized that Hungarian law does not provide for the deletion of collected data that has proved to be useless, as well as the lack of clear indication as to whether it is possible to extend the use of privacy-sensitive control measures several times. This should be done through external control and providing citizens with effective tools to assert their rights. The first of them, though insufficient, is information that you have been subjected to special control.

It should be emphasized that States have, as defined by the Tribunal, a margin of appreciation; in other words, the scope of freedom to balance individual rights against national security interests (see 5 *Leander v. Sweden*, 9248/81, § 59, 26 March 1987). As early as the 1970s, the Tribunal acknowledged that legislation allowing secret monitoring of mail, emails and telecommunications in a democratic society was necessary in exceptional circumstances, in the interests of national security and/or to prevent riots or crimes. Recently, the Court found that the surveillance of suspected terrorists using the GPS system did not violate their right to privacy guaranteed in Article 8 (*Lass and Others v. Germany*, complaint No. 5029/71 and *Uzun v. Germany*, complaint No. 35623/05). The Court found that adequate safeguards existed against the arbitrary use of such methods. On the other hand, the powers given to the police, by special anti-terrorist legislation, to detain and search persons without any sufficiently specific grounds for suspected

misdemeanors were found to violate the applicant's right to respect for their private life (*Gillan i Quinton v. United Kingdom*, 4158/05, § 87, 12 Jaunary 2010).

To date, there was no single legal act in the Polish legal system that comprehensively regulated the issue of recognizing, preventing and combating terrorist threats, and removing the effects of an attack. The basic goal of the prepared regulation is to increase the effectiveness of the Polish anti-terrorist system, and thus to increase the security of all citizens of the Republic of Poland, by ensuring the possibility of effective action in the event of suspected terrorist offenses, including in the field of preparatory proceedings. The basic regulations in this respect are contained in the following acts:

- in the Act of 6 June 1997 - the Penal Code (Journal of Laws, item 553, as amended), which, among others contains a definition of a terrorist offense (Article 115 (20)), and also penalizes the establishment, management and participation in an organized group or association aimed at committing a terrorist offense (Article 258 (2) and (4)), financing of a terrorist offense (Article 165a) and the dissemination or public presentation of content that may facilitate the commission of a terrorist offense (Article 255a);
- in the Crisis Management Act of 26 April 2007 (Journal of Laws of 2013, item 1166, as amended), which defines the authorities competent in matters of crisis management as well as their tasks and principles of operation in this field, and also defines, among others concept of a terrorist event;
- Anti-Money Laundering and Terrorism Financing Act of 16 November 2000 (Journal of Laws of 2014, item 455, as amended), which defines the principles and mode of counteracting terrorist financing.

The issue of responding to terrorist threats is also included in emergency regulations. In addition, issues related to the tasks and powers of services and institutions with regard to terrorist threats are contained in the competence laws regulating their operation (e.g. the Police Act of 6 April 1990, the Border Guard Act of 12 October 1990, the Internal Security Agency and the Foreign Intelligence Agency Act of 24 May 2002), as well as other legal acts covering selected aspects related to a specific type of threat (such as the Protection of Shipping and Sea Ports Act of 4 September 2008 or the Protection of the State Border Act of 12 October 1990). In order to strengthen the state's preparation for the possibility of occurrence of terrorist events, it is necessary to integrate the activities implemented by individual participants of the multi-stakeholder anti-terrorist system of the Republic of Poland. Ensuring optimal coordination of activities and cooperation mechanisms at both the strategic, operational and tactical levels plays a key role in the efficiency of the functioning of the Polish anti-terrorist system. To this end, the Anti-Terrorist Activities Act of 10 June 2016 was adopted. In Article 23 the Act provides a special procedure of preparatory proceedings in the event of suspected or attempted commitment or preparation of a terrorist offense, in order to detect or detain or forcibly bring a suspected person, as well as to find things that could constitute evidence in the case or subject to attachment in criminal proceedings. This mode applies to, among others

to the ability of the prosecutor to issue a decision to search the premises and other places in the area indicated in the decision, or to detain a suspected person - if there are reasonable grounds to believe that the suspected person or the items listed are in that area. In order to find things that may constitute evidence in the case or subject to attachment in criminal proceedings, this article also provides for the possibility of searching the area of the persons specified in the decision, their clothing and hand items. Aforementioned activities can be done at any time of the day. The European Court of Human Rights in the judgment of *Sher and Others v. The United Kingdom* (complaint No. 5201/11) held that in case of proceedings related to a terrorist offence, enabling of search or detention on grounds further specified than in other cases was justified. In particular, the Court has indicated that it does not constitute a violation of the European Convention on Human Rights and Fundamental Freedoms to conduct a search under the conditions specified above in a situation where it is possible to appeal against the abovementioned operations. In accordance with the proposed Article 23 of the Anti-Terrorist Activities Act and the amendment of some other acts, to an extent not regulated in this article, Article 236 of the Code of Criminal Procedure, according to which persons whose rights were violated may appeal. In addition, in Article 24, referring to the case of suspicion of committing a terrorist offense, it was pointed out that if it is required by the good of the preparatory proceedings, the decision on the presentation of charges may be made on the basis of information obtained as a result of operational and investigative activities, including the activities referred to in Article 8, i.e. ordered by the Head of the Internal Security Agency against a person who is not a citizen of the Republic of Poland, in relation to whom there is a fear that he may conduct terrorist activities, for a period not longer than 3 months, secretly operational and reconnaissance activities. Moreover, in this case the court, on the prosecutor's request, may apply temporary detention for a period not exceeding 14 days. The very premise of applying temporary detention will be the probability of committing, attempting or preparing to commit a terrorist offense. In accordance with Article 6 of the Act, the Head of the Internal Security Agency, subject to the requirements for the protection of classified information, maintains a list containing information about: persons undertaking activities for terrorist organizations or organizations associated with terrorist activities or members of those organizations; wanted persons conducting terrorist activity or persons suspected of committing terrorist offenses, against which a detention order, search or decision on arrest warrant was issued in the Republic of Poland, and wanted on the basis of a European arrest warrant; persons for whom there is a reasonable suspicion that they may carry out activities aimed at committing a terrorist offense, including persons posing a threat to civil aviation security; persons participating in terrorist training or undertaking travel to commit a terrorist offense.

3.3 Operational activities in selected areas of the service activities

The scope of use of personal data, and therefore the extent of permissible interference with the personal rights of the individual citizen is determined by legal provisions regulating the scope of competence of the aforementioned bodies. However, this does not

only cover personal data protection. This applies to all other rights and personal freedoms. Here, several examples of restrictions that arise from the competences of, for example, selected services should be cited.

Military Police within the limits of tasks specified in Article 4 (1) of 24 August 2001 on the Military Police and military law enforcement agencies and in relation to the persons indicated in Article 3 (2) (1), (3) (b) and (5) of this Act, subject to the restrictions arising from Articles 30-33 and taking into account the provisions of the Protection of Personal Data Act of 29 August 1997, may obtain information, including classified information, collect, store, check, process and transfer information. In addition, the Military Police can collect, gather and use for detection and identification purposes fingerprints, photos and personal data, including those revealing ethnic origin, religious affiliation and data on the state of health, persons suspected of committing offenses prosecuted by public prosecution, as well as persons of unknown identity or attempting to hide their identity, without the consent and knowledge of the data subject. These data, except for data revealing ethnic origin or religious affiliation, are stored for the period necessary for the performance of statutory tasks by the Military Police. The Military Police authorities verify these data at least every 10 years from the date of obtaining the information. For the implementation of statutory tasks, the Military Police may use information about a person, including personal data obtained by authorized organs, services and state institutions as a result of performing operational and reconnaissance activities or conducting operational control, and process it within the meaning of the Protection of Personal Data Act of 29 August 1997 without the knowledge and consent of the data subject.

In accordance with the terms of reference of officers of the **Central Anti-Corruption Bureau (CBA)** expressed in the Central Anti-Corruption Bureau Act of 9 June 2006, within the limits of their tasks, CBA officers perform:

1) operational and investigative activities to prevent, recognize and detect the commission of crimes, and, if there is a reasonable suspicion of committing a crime, investigative measures to prosecute perpetrators of crimes;
2) control activities to disclose cases of corruption in state institutions and local government as well as abuse of persons performing public functions, as well as activities detrimental to the economic interests of the state;
3) operational and reconnaissance and analytical and information activities in order to obtain and process information relevant to combating corruption in state institutions and local government as well as activities detrimental to the economic interests of the state.

Within the limits of its tasks, the **Police** perform operational and reconnaissance, investigative and administrative and order activities in order to recognize, prevent and detect crime and offenses. The Police also perform actions at the behest of the court, prosecutor, state administration bodies and local government to the extent that this

obligation is specified in separate laws. During the performance of official duties, police officers are obliged to respect human dignity and to respect and protect human rights (Article 14 (3) of the Police Act).

In order to perform statutory tasks, the Police may use data about the person, including the form of an electronic record, obtained by other authorities, services and state institutions as a result of operational and reconnaissance activities, and process them without the knowledge and consent of the data subject.

The President of the Council of Ministers determines, by regulation, the scope, conditions and procedure for providing the Police with information about a person obtained by the authorities authorized to perform operational and reconnaissance activities while performing these activities, taking into account the requirements arising from the provisions on the protection of classified information.

In order to recognize, prevent and detect crimes and offenses, **Border Guard** officers perform border service, carry out border activities, carry out operational and reconnaissance and administrative and order activities, and conduct preparatory proceedings in accordance with the provisions of the Code of Criminal Procedure, as well as carry out actions at the request of the court and prosecutor's office and other competent state authorities. In order to carry out statutory tasks, the Border Guard may use information about a person, including personal data obtained by authorized bodies, services and state institutions as a result of performing operational and reconnaissance activities or conducting operational control, and process it without the knowledge and consent of the data subject.

The tasks of the Internal Security Agency include: identifying, preventing and combating threats to the internal security of the state and its constitutional order, in particular the sovereignty and international position, independence and inviolability of its territory, as well as national defense; recognizing, preventing and detecting espionage, terrorism, unlawful disclosure or use of classified information and other offenses detrimental to state security, detrimental to the economic foundations of the state, corruption of persons performing public functions referred to in Articles 1 and 2 of the Restriction of Business Activity by Persons Performing Public Functions Act of 21 August 1997, if this may harm the security of the state in the field of production and trade in goods, technologies and services of strategic importance for state security, illegal production, possession and trade in arms, ammunition and explosives, weapons of mass destruction and narcotic drugs and psychotropic substances, in international trade and the prosecution of their perpetrators; carrying out, within its jurisdiction, tasks related to the protection of classified information and performing the functions of the national security authority in the field of protection of classified information in international relations; obtaining, analyzing, processing and forwarding to competent authorities information that may be of significant

importance for the protection of the internal security of the state and its constitutional order.

The issue of operational and reconnaissance activities in the field of obtaining, information and storage of this information essentially concerns various aspects and ways of the executive entering the privacy of the individual, in terms of their constitutionally regulated freedom of communication and protection related to the private sphere, by the police, exercising their competence through operational and reconnaissance activities. These activities are inherently classified (also towards the person concerned), carried out in conditions that give the services a wide margin of discretion, with limited guarantees for the rights of the person subjected to these activities, as well as limited external control, including judicial. It should be emphasized that the unquestionable rule is that such a way of operating the police is indispensable in the modern state. The transparency of operational activities would render them ineffective. The modern state, obliged to ensure security (which is also a constitutional obligation), faces a difficult task due to the threat of terrorism and crime (including organized crime). Technical facilities affecting the speed of communication and movement can be used equally to protect the security of the state and by criminals. Operational activities, e.g. of the police, regulated in ordinary legislation, carried out in secret, remain in natural, irremovable conflict with some of the fundamental rights of the individual. In particular, this applies to the individual's right to privacy, constitutional freedom of communication and related protection of the secret of communication, protection of information autonomy (which in Poland is determined by Articles 49 and 51 of the Constitution of the Republic of Poland), as well as with the constitutional guarantee of judicial protection of individual rights.

The confidentiality of the services and the lack of external control may lead to excessive autonomy or subjectification of the very purpose of operational activity and failure to exercise due restraint in encroaching on civil rights and freedoms. Sometimes, however, such a situation may result from excessive ideological or political considerations in the execution of the executive. In other words, the secret feature of operational control makes it vulnerable to abuse. Public security, as a good that, in principle, justifies the legislator's limitation of the exercise of civil liberties, therefore requires that proportionality of permissible encroachment be maintained in the name of security protection and an efficient system of monitoring compliance with this proportionality in practice. Otherwise, measures to protect this security, in the form of legally permissible operational activities, in themselves pose a threat to these freedoms. This will be the case when, firstly, the restrictions imposed will be arbitrary, disproportionate to possible threats, and, secondly, when they are excluded (whether legally or in fact) from the control exercised by democratic institutions". The conflict between the need for legal and legitimate operational activities and the threat to constitutional freedoms and rights of the individual requires weighing two goods, always in the individual assessment, dictated by the principle of proportionality. The conflict related to the limits of the use of operational and technical activities is known in all democratic states of law, as well as in the practice of

international bodies, where, against the background of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, universal standards have been developed to assess the proportionality between the interference of the authorities and the rights of the individual in the sphere under consideration. The experience of modern democratic states indicates that the executive power responsible for public security and order, including its subordinate entities conducting operational and reconnaissance activities, have at their disposal resources which, in the name of defending public order, may destroy democratic institutions and reduce civil rights. According to the position of the European Court of Human Rights in the scope protected in Article 8 of the Convention on the Privacy of an Individual, it is potentially permissible for the authority (legislative, executive, judicial) to interfere in the sphere of this privacy, provided that it meets certain criteria. However, any trespass must withstand the three-level evaluation test. This means that it is not allowed to introduce restrictions (privacy) by acts of a different rank[2].

In cases against France (*Kruslin v. France*, complaint No. 11801/85 and *Huvig v. France*, complaint No. 11105/84), it was pointed out that the Convention requires national legislation to define the category of persons to whom operational control may be applied, based on court order; type of offenses against which such an order may be issued; maximum length of control time; procedure for reporting the content of recorded conversations (the case concerned telephone tapping); measures to ensure that the records are transferred intact and in their entirety enabling their review by the judge and the defense; determination of cases when records can or must be destroyed, especially when the investigation was discontinued or the court acquitted the convict. French legislation was found not to meet these criteria, as did national legislation in the *Malone v. United Kingdom* case (8691/79), judgment of 2 August 1984 (cases concerned the collection of information and wiretapping). It was recognized that local laws were too vague and non-specific, and this meant that although these activities were indeed provided for by law. It is not enough to refer to the purpose factor. It is necessary to prove the necessity and the specific (described in terms of scope and manner) restriction introduced in the ordinary act. That is why the collection of information in the operational control mode must be treated in the legislation and, moreover, in practice of police action as a subsidiary mode of the purpose of the interference (the rank of the protected public interest), listed in the same Article 8 of the Convention: national security, public security, economic prosperity of the country, protection of order and prevention of crime, protection of health and morality, and freedom of others. It is necessary (and demonstrated) for a real need to take restrictive measures, and in the name of protecting the very principles of democratic order. Excess, consisting in the fact that "on the occasion" of collecting operationally useful material, operational control will also collect data on private, moral issues - beyond the purpose of conducting control, means the action of the authority outside the scope of the allowed entry into the sphere of privacy.

In this case, the European Court of Human Rights found controlling individuals in a secret way "necessary in the reality of today in a democratic society for the security of the state

and for reasons of order protection and crime prevention", and assumed that the fact of "failure to report observation" does not violate Convention (see justification of the judgment of 6 September 1978 in the case of *Klass and Others v. Germany*, complaint No. 5029/71) (Gajdus & Gronkowska, 1994:115-116). Although the judgment in *Klass and Others v. Germany* was favorable to the German legislator, the German legislator amended the said act after the sentence in Strasbourg. The result of this amendment was (inter alia) an increase in the protection standard, by introducing the obligation to notify ex post the person against whom operational activities were carried out under the G-10 Act that such control was carried out against him (§ 5 (5) of the Act)[3].

However, in the face of escalating terrorist attacks, especially with the use of new technologies, the limits of interference with the right to privacy are widening. The use of classified control by executive authorities is becoming a natural consequence of the forms of combating terrorism. The use of the latest technologies by governments to anticipate such attacks, including mass monitoring of communications that may include indications of impending incidents. The techniques used in such monitoring operations show significant progress in recent years. These techniques have reached the level of sophistication that the average citizen can hardly imagine, especially with the technological enabling and dissemination of automated and systematic data collection. In view of this progress, the Strasbourg Court has to examine the question of whether the development of control methods resulting in the mass of data collected is accompanied by the simultaneous development of legal safeguards to protect respect for citizens' Convention Rights. These data often contain further information about the conditions under which the basic elements captured by the authorities, elements such as time and place, and equipment used to create computer files, digital photographs, electronic and text messages and the like were created. Indeed, the purpose of the government's efforts, which seeks to limit terrorism and thus restore citizens' confidence in the government's ability to maintain public security, would be undermined if the terrorist threat were paradoxically replaced by a perceived threat caused by the unlimited powers of the executive to intervene in the sphere of private life of the citizens using uncontrolled, yet far-reaching control techniques and prerogatives. Potential interventions in e-mail, mobile telephony and internet services, as well as covert mass surveillance, are even more appealing to the conventional protection of private life. The interference can only be justified on the basis of the provisions of Article 8 (2), if provided for by law, pursues one or more legitimate purposes indicated in Article 8 (2) and is necessary in a democratic society to achieve any of these goals. This provision, as it provides an exception to the law guaranteed by the Convention, must be interpreted narrowly. The powers to covertly control citizens, which are a hallmark of a police state, are tolerated under the Convention only to the extent that they are strictly necessary for the protection of democratic institutions. The Court states that the purpose of the interference is to protect public security and/or to protect order and prevent crime, in accordance with Article 8 (2). This issue is not the subject of dispute between the parties. On the other hand, it is necessary to assess whether the measures envisaged on the basis of the contested legislation to

achieve the stated objective remain in all respects within what is necessary in a democratic society.

4 Security for the right of the individual citizen to privacy in the aspect of cyber terrorism

The information revolution, manifested primarily in fast communication and data transfer, promotes the development of each individual. In addition to many advantages, it also has disadvantages, which include cyberterrorism. The ideas of terrorists hacking into computer systems to introduce viruses, stealing sensitive information is the essence of cyber terrorism, also known as infoterror (Bolechów, 2002:51).

Cyber terrorism is not a new phenomenon. Already in 1979, the Swedish Ministry of Defense included cyber terrorism in a threat report, recommending that the government be involved in monitoring public and private computer networks (Hołyst, 2011:956).

It should be emphasized that a lot of network information has an impact on the types of targets and weapons chosen by terrorists and the methods of their operation. Cyber terrorism involves the use of information techniques, i.e. computers, software, telecommunications devices, the Internet, to achieve the goals intended by a given group. As B. Hołyst (2011:952) rightly observes, "like many corporations using the Internet for more efficient and flexible operations, terrorists harness the power of technical information (IT) to create new operational doctrines and organizational forms". The emergence of networked terrorist groups is part of the concept of "*net war*" (Sienkiewicz, 2009:46). Network war, cyber war, consists in disrupting or destroying the opponent's information systems, acquiring their strategic data (Sobczak, 2017:44).

Analysis of the security issue for the right of the individual citizen to privacy in the aspect of the phenomenon of cyber terrorism requires attention to the problem of the target of the attack. Classic terrorism is defined as the so-called blind crime, through random selection of victims. The purpose of the attack is not so much to commit a specific crime, e.g. murder, often of innocent people, but to create a specific effect and reaction from the throne of the authorities and public opinion. The literature on the subject indicates that "terrorism is intended for those who look, not for those who have become victims" (Aleksandrowicz 2015:29).

Similarly in cyberterrorism, attacks on information stored on a computer system can have two types: as a desire to undermine the credibility of the system or the theft of information. In the first case, online terrorists enter their own data or manipulate the data in the system. These attacks are designed to disorganize their actions, which is to the detriment of society. These activities may be directed towards critical infrastructure, water and energy supply, telecommunications infrastructure, etc. Influencing these systems can also lead to material damage or casualties, e.g. in the event of a train collision.

A cyber attack of theft of information can affect both domestic resources and information owned by an individual citizen.

In the light of the above considerations, the thesis that cyber terrorism constitutes a violation of human rights seems to be irrefutable. The European concept of human rights primarily concerns the state - citizen/individual relationship, and its basis is the protection of individual freedom against violations by the state. On the other hand, the state is also obliged to protect the rights and freedoms of the individual against violations by other persons, including cyber terrorism.

In 2005, the Strategy on combating terrorism was adopted in the European Union (14469/05 of 30 November 2005). One of the tasks set for the Member States was to correlate Community mechanisms designed to protect citizens. The issue of respecting the rights of the individual citizen, including the right to privacy, in the sphere of combating cyberterrorism implies two problems:

1) cyber terrorism is a serious threat to the privacy of the individual,
2) preventive actions by the state (police services) may conflict with the right to privacy.

The thesis on the violation of human rights by cyber terrorism is beyond doubt. Cyber terrorism has a negative effect on the full exercise of the right to privacy.

The second issue - implies a serious problem, the choice between freedom and security. On the one hand, the state is obliged to protect citizens against cyber attacks. However, the main method of combating and preventing cyber terrorism is limiting the right to privacy and subjecting the state to control more and more numerous areas of citizens' lives and increasing the powers of security services. This shows that the conflict between fragrance and security is becoming more pronounced.

In 2005, a convention was signed in Prüm in Germany between Belgium, the Netherlands, Luxembourg, Germany, France, Spain and Austria on the introduction of specific forms of cross-border cooperation, in particular in combating terrorism, international crime and illegal immigration (Dock. Council of the European Union 10900/05 of the 7th day of 2005 CRIMORG 65, ENFOPOL 85, MIGR 30).

The analysis of the provisions of the Convention allows the thesis that the head method of combating terrorism is to strengthen the powers of the state at the expense of the rights and freedoms of the individual citizen. Measures to directly combat terrorist offenses are set out in Chapter 3 of the Convention. They include exchange of information (personal data) to prevent criminal acts. The convention allows the use of armed *sky marshal*son aircraft that are registered in your country. In Poland, they are known as protective guard. The guard should not include less than two officers and it is performed secretly.

The 21st century sets new challenges for humanity. As M. Ciesielski (2017:56) notes, we are dealing with huge technological development and the choice between freedom and security is a very difficult choice. The threat of cyber terrorism implies two problems. On the one hand, cyber attacks pose a threat to the rights and freedoms of the individual, on the other, the excessive powers of the state to protect the individual against these threats can also be considered a threat. It is important to be aware not to break the rules you defend. If, by fighting cyber terrorism and defending democratic values, the state begins to unduly restrict the rights and freedoms of the citizen-individual, the choice between freedom and security will be false. It is important that the state manages to defeat terrorism by maintaining its principles of freedom on which it is built.

Notes:

[1] The subject-matter control and recording of the content of telephone conversations are permissible only if the pending proceedings or a justified fear of committing a new crime concerns: 1) homicides, 2) exposure to general danger or bringing about a catastrophe, 3) trafficking in human beings, 4) kidnapping a person, 5) a ransom note, 6) hijacking an aircraft or a watercraft, 7) armed robbery, robbery or extortion, 8) an attack on the independence or integrity of the state, 9) an attack on the constitutional system of the state or its supreme organs, or on a unit of the Armed Forces of the Republic of Poland, 10) espionage or disclosure of classified information classified as "secret" or "top secret", 11) collecting weapons, explosives or radioactive materials, 12) forgery and trading in counterfeit money, means or payment instruments or negotiable documents entitling to receive a sum of money, goods, cargo or material prize or containing an obligation to pay capital, interest, share in profits or confirm participation in the company, 13) manufacturing, processing, trading and smuggling of narcotic drugs, precursors, substitutes or psychotropic substances, 14) an organized criminal group, 15) property of significant value, 16) use of violence or an unlawful threat in connection with criminal proceedings, 17) bribery and paid protection, 18) pimping, 19) crimes specified in Chapter XVI of the Act of 6 June 1997 - Penal Code (Journal of Laws No. 88, item 553, with amended).

[2] Even if it has been done in an act, it is too general, blanket, and not very specific in nature, when it is a competence act from which inference is derived from the end to the means - then the premise of a specific statutory basis will not be met.

[3] It should be noted that, for example, the German anti-terrorist legislation of 1968 (the Act of August 13, 1968, limiting the confidentiality of correspondence and telephone conversations, the so-called G-10 Act) has successfully passed the test of concreteness and compliance "with the necessary goal in a democratic society" (and it was about wiretapping in connection with suspected terrorism, which was supposed to remain a secret for the interested parties), as well as the proportionality of the restriction applied and the provision of appropriate appeal and control measures (although these were not judicial measures, but control by a specially created, representative body).

Summary

Social changes related to the development of civilization stimulate democratic processes, provide space for achieving various economic, economic, organizational and socially desirable goals, but may also be the cause of regressive activities. This applies to virtually every sphere of human activity. This applies in particular to fundamental rights and freedoms. The risk of threats to an individual increases in proportion to the process of weakening the state as a structure and institution. Consequently, the individual citizen loses a sense of security. This feeling is associated with new situations in which the individual citizen operates. Globalization, the crisis of the institution of the state - the regulator, doubts related to the territory, exchange of information, mixing cultures, identity crisis, crisis of the world economy and terrorism with its completely new sources, create a new space in which fundamental rights and freedoms require special social attention, redefining goals choosing the right protection instruments. An additional aspect of these changes is the issue of ensuring national security, which also, for the reasons indicated above, is subject to redefinition. The protection of national security is one of the most important goals of the state's activities, and consequently public authorities and the entire public administration. It should be emphasized that national security consists of various elements, including personal, individual and personal security.

The state, using its attributes of power, uses various legal instruments and legal institutions, the purpose of which is to protect the public interest, public morality and national security. The situation of weakening the state, like no other, directly threatens national security and, as a consequence, individual and personal security. For this reason, it became necessary to determine the status of the individual towards the state in the area of public authority activities aimed at protecting national security. If the state of guarantee for this protection is analyzed, it becomes necessary to supplement its scope with a diagnosis of obligations and civic restrictions related to national security, including those spheres of the entity's functioning that relate to its privacy and its associated identity. Following the principle of Christian Wolff, a continuator of Pufendorf's thought, that *homo persona moralis est quaternus spectatur tanquam subiectum certarum obligationum atque iurium certarum* (Sójka-Zielińska, 2006:170).

Digital democracy, as a contemporary reflection basis, whose model was created in the conditions of digitization, must absolutely ensure the protection of individual freedoms and rights. As part of creating digital democracy, more and more public institutions are creating an information space (pages related to the data access database - collected by the state) and an exchange area (portals) that are used to build information sources. Due to the development of the network and activities related to the development of the information space, there has been a need to choose the concept of digital democracy, taking into account the issues of protection of the right to privacy, the need to secure

systems that are private property and the growing participation of the individual in the activities of power. As a result of these phenomena, there are questions about legal regulations that can provide protection against threats by introducing the necessary restrictions at a given level of activity, also in the area of civil rights and freedoms. Under these conditions, not only the issue of new regulatory solutions is the basis for consideration. The main and priority question will be the issue of defining public interest objectives, which constitutionally justifies all restrictions but is also the basis for the operation of public administration in the conditions of developing new technologies. This will refer to research questions about the level of defining the objectives related to the premise of security as the purpose of acting in the public interest, the scope of this definition and competence in achieving them. This issue concerns the role of the state, the scope of public tasks, the responsibility of public administration bodies and the obligations of the individual. Boundaries must be designated by fundamental rights, and within them also the right to privacy and identity. In this area, it is important to specify the regulatory goals expressed in the strategies and assumptions underlying the regulatory policy based on development trends related to the ideology of individual freedom in the full area of its activity.

One of the key regulations is the transatlantic data transfer agreement called *the Piracy Shield*, which is a service certification character. The basic right to privacy is guaranteed primarily by art. 8 Charter of Fundamental Rights of the European Union. A new Directive will apply general data protection principles and rules for police and judicial cooperation in criminal cases. The rules will apply to both domestic and cross-border transfers of data. The reform of EU data protection rules strengthens citizens' rights, giving them greater control over their data in the digital age related to the development of new technologies. In the light of the Personal Data Protection Act, each data controller must supervise personal data processed in its organization. The personal data protection reform meets the expectations related to the security of the individual, however, doubts still arise regarding operational and exploratory issues.

In democratic countries, even those that introduce restrictions on the constitutional freedoms of the individual, due to the need to fight crime and terrorism, universal legislation regulating operational and investigative activities must have constitutional foundations. There are two models of this constitution: in the German model, the operational activity itself finds a specific constitutional regulation. The provision of the constitution explicitly refers to the objectives, scope and criteria for restricting freedom of communication and privacy through operational activities. In turn, in Poland, operational activities are not explicitly mentioned in the Constitution as a permitted limitation of individual rights. However, some constitutional rights and freedoms of the individual (e.g. art. Article 49, Article 50 and Article 51 section section 3 of the Constitution of the Republic of Poland) provide that an ordinary law will specify "cases and manner" of limitation of constitutional freedom/law (Article 49 and Article 50) or (Article 51 section 3). In turn e.g. Article 47 or Article 51 section 4 of the Constitution of the Republic of Poland do not provide for any restrictions on their own regulation at the

constitutional level. However, Article 31 section 3 of the Constitution of the Republic of Poland formulates the general principle of maintaining the proportionality of any restrictions on constitutional freedoms / rights in the event that they would experience (regardless of their subject) restrictions in ordinary legislation. This rule applies both to the situation when the Constitution itself provides for the creation of exceptions by statutes, and to the situation when the ordinary legislator, by regulating another matter, and not exercising the constitutional authorization to co-define a certain sphere, falls into a collision with the constitutional freedoms/rights of the individual. Thus, in the Polish legal system, the assessment of the compliance of operational activities with the Constitution of the Republic of Poland requires an analysis from the point of view of the method of constitutionalization of protected freedom threatened by operational activities, as well as an analysis of the proportionality of the ordinary legislator's activities in both of the abovementioned aspects (substantive and procedural). This is necessary in order to determine the proper (proportional) relationship between the constitutional order to guarantee the rights and freedoms of the individual and the necessary protection of the value of state security and public order. The subjective constitutional rights include freedom and protection of the secret of communication (Article 49 of the Constitution of the Republic of Poland), the right to request correction and removal of false, incomplete or collected information in a manner contrary to the Act (Article 51 section 4 of the Constitution of the Republic of Poland). Among the constitutional models, Article 31 section 3 of the Constitution of the Republic of Poland (principle of proportionality). Operational activities with the use of observation, especially wiretapping, remain in opposition to the right to privacy. These laws are traditionally assessed in the practice of European countries, taking into account the scope of encroachment of operational activities in the private sphere of the individual when analyzing proportionality. Constitutional rights regarding privacy are regulated at many levels in the constitutional level, protecting privacy in its various aspects and in various areas. One of them is the telecommunications sphere and the area of electronic services provision.

The means at the disposal of the public authorities allow for far-reaching interference with the right to privacy, and if proportionality determining the extent and procedure of this interference is not observed, it is even able to cross the essence of the right to privacy. Due to the immanent relationship between privacy and dignity, it could threaten the dignity of the individual, even depriving him of information autonomy consisting in - as stated by the Constitutional Tribunal - the protection of any personal information and the fundamental meaning of the premise of the consent of the person concerned to disclose information (see the judgment of the Constitutional Tribunal of 20 June 2005, file no. K 4/04, OTK-A 2005, No. 6, item 64). This applies to the possibility of practically unlimited surveillance as part of operational activities, as well as the possibility of dissemination - with or without the participation of authorities - of information collected in this way. This leads to the deprivation of the individual's right to privacy and thus can lead to a fundamental violation of human dignity. It should be remembered that the indicated operational measures can only be considered justified if their own goal is to defend the value of a democratic state ruled by law. The minimum constitutional requirement is that

they pass the test of "the necessity in a democratic state ruled by law." Therefore, it is not enough to have purposefulness, utility, cheapness or ease of use by the authority - in relation to the measure used. The comparative argument that similar measures are generally used in other countries is also irrelevant. It is therefore about the use of necessary measures in the sense that they will protect certain values in a way or to a degree that could not be achieved by other means, and at the same time they should be the measures that are the least burdensome for entities whose right or freedom is limited (see the judgment of the Constitutional Tribunal of 3 October 2000, file no. K 33/99, OTK-ZU 2000, No. 6, item 188). These principles will remain valid in weighing the public interest objectives, which are the individual's right to privacy and security in digital conditions.

In the case of clear competitiveness of constitutionally protected goods, the conflict between the constitutional right to privacy, confidentiality of correspondence and the protection of information autonomy and reasons of public security requires that the legislator regulates disputed issues while maintaining constitutional normation requirements and a clear and legible balance between the interests remaining in permanent collision. Essential for determining the status of operational and reconnaissance activities in a democratic state of law is the determination that they must not lead to the erosion of the foundations of the state, including its identity, which includes human dignity on the one hand, and avoidance of arbitrariness in the actions of the authorities - on the other. This conflict will remain current in a problematic situation related to state supervision in the conditions of digitization of the life of the individual, which enters into every corner of our being, including the most intimate sphere, related to our biology and genotype.

However, as already stated at the beginning when assessing whether there has been a encroachment on the field of private life protected by law, this concept should not be absolutized. Due to the degree of its generality, it requires interpretation, which must take into account the specific circumstances of the individual situation. The private sphere of life primarily includes situations that create the sphere of personal and family life. The special nature of this area of human life justifies giving it strong legal protection. This does not mean, however, that any information about a particular person will refer to the private sphere. The assessment will depend on the entire context and circumstances of the case, and above all on what information is specifically disclosed and to whom it has been disclosed. Neither the normative state nor the considerations for the purposes of the regulations analyzed at work provide sufficiently strong grounds for claiming that the protection of personal data "is one of the aspects of the right to privacy". The view that the regime for the protection of the right to privacy within universal personal rights (based on the provisions of the Constitution and civil law) and the regime for the protection of personal data (based on the provisions of the Constitution of the Republic of Poland and the Act on the protection of personal data) should be considered convincing. They are connected to each other, where we touch upon the issue of the identity of the individual, his personality identification and independent in the context of related rights, the

regulation of individual goods. In this respect, the right to privacy still remains an unregulated sphere to the extent that this regulation should be expected due to personal security, individual units in the conditions of digitization of life. The fact of using personal data without the consent of the person concerned does not prejudge the infringement of personal rights and the grounds for obtaining protection. If, in specific circumstances, the processing of personal data constitutes a violation of the right to privacy, the interested party will of course be able to seek protection but then it will be necessary to prove the violation of the personal good in a manner consistent with the meaning of the Code, i.e. art. 23 and 24 of the Civil Code, i.e. the civil law basis. This means that, first of all, a person whose rights have been violated in her opinion will have to show that the use of his personal data constituted in the given circumstances a violation of one of the common personal rights - the right to privacy (see the judgment of the Supreme Court of 28 April 2004, file no. III 442/02, Lex nr 1125280). The notion of "private life" within the meaning of art. 8 Convention is a broad term that cannot be comprehensively defined. The concept of personal autonomy can take into account a number of aspects of the physical and social and individual identity of a person. The basic subject of the said Art. 8 is to protect the individual against arbitrary interference by public authorities, this article forces you to refrain from such interference: in addition to this negative obligation, there may be positive obligations inherent in effective respect for private life. Such a regulation is necessary and obvious. These obligations may include the adoption of measures to safeguard respect for private life even in the sphere of relationships between individuals. The line between positive and negative obligations of the state is not an easy task. As emphasized by J.H. Lorenzi, M. Berrebi (2019:226) in 2015 and 2016 there was a change in thinking about privacy, which consists in the fact that the rule related to the concept of ensuring security so that people could enjoy full rights was replaced by an idea, that for our safety our rights must be limited.

Answering the question about the scope of these restrictions is difficult, but it will undoubtedly cover areas that constitute the unbelievable and today unknown sphere of human action. On the other hand, information self-determination rights are necessary, i.e. information autonomy, perhaps with significantly expanded rules for monitoring data about yourself - including rigidly set rules for accessing and retaining data in conditions where such activities are necessary; the principle of neutrality of telecommunication entrepreneurs and their use of data for their intended purpose; the principle of the right to withdraw from the contract and exercise the right to be forgotten by network users, guaranteed by the CJEU in 2014, the principle of anonymisation and pseudonymisation, which should accompany all registers, especially medical registers. This is just the beginning of the necessary arrangements for future regulations.

However, the rules for implementing these restrictions applicable here are similar to those set out in the provisions on the protection of personal data. In both cases, there should be a fair balance that should be maintained between the competing interests of the individual and society, in particular when the individual is unable to identify the threat on his or her own (an example is the information war). However, it should be taken into account that

in the context of protecting human privacy, the most severe restriction, which always is and will be the restriction of his freedom, is of significant importance.

References

Aleksandrowicz, T. R. (2015) *Terroryzm międzynarodowy* (*International terrorism*) (Warszawa: Editions Spotkania Spółka).

Angwin, J., (2015) *Społeczeństwo nadzorowane, w Poszukiwaniu prywatności, bezpieczeństwa i wolności w świecie permanentnej inwigilacji* [Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance] (New York: Paperback – Bargain Price).

Banaszak, B. (2012) *Konstytucja RP. Komentarz* (Warszawa: Wydawnictwo C.H. Beck).

Baumann Z. (2010) *Kultura w płynnej nowoczesności* (Warszawa: Wydawnctwo Agora S.A.).

Biernat, K. (2013) *Ustawa o ewidencji ludności. Komentarz* (Warszawa: Wydawnictwo Wolters Kluwer Polska).

Bigo, T. (1928) *Związki publiczno-prawne w świetle ustawodawstwa polskiego* [Public-legal relationships in the light of Polish legislation) (Warszawa: Wydawnictwo "Przemiany").

Borski, M. (2014) Godność człowieka jako wartość uniwersalna, *PPP*, 3, pp. 15-26.

Boć, J. (2010) *Prawo administracyjne* [Administrative Law] (Wrocław: Wydawnictwo Kolonia Limited).

Bolechów, B., (2002) *Terroryzm w świecie podwubiegunowym. Przewartościowania i kontynuacje* [Terrorism in the Subpolar World. Revaluations and continuations] (Toruń: Wydawnictwo Adam Marszałek).

Catinat, M. (1997) The „National Information Infrastructure Initiative" in USA. Policy or Non-Policy, *Computer and Telecommunication Law Review*, 3, pp. 68-86.

Ciesielski, M. (2017) Terroryzm w ponowoczesnym świecie: charakterystyka relacji pomiędzy globalizacją a struktura zjawiska [Terrorism in the postmodern world: characteristics of the relationship between globalization and the structure of the phenomenon], In: Herbowski, P., Słapczyńska, D. & Jagiełło, D. (eds) *Pozyskiwanie informacji w walce z terroryzmem* [Obtaining information in the fight against terrorism] (Warszawa: Wydawnictwo Difin).

Chlewiński, Z. & Zaleski, Z. (1997) *Godność*, In: Herbut, J. (ed.) *Leksykon filozofii klasycznej* (Lublin: Wydawnictwo Katolicki Uniwersytet Lubelski).

Chałubińska – Jentkiewicz, K. & Karpiuk, M. (2015) *Prawo Nowych Technologii* (Warszawa: Wydawnictwo Wolters Kluwer Polska).

Chałubińska-Jentkiewicz, K. & Karpiuk, M. (2015) *Prawo nowych technologii* [New technologies law] (Warszawa: Wydawnictwo Wolters Kluwer Polska).

Chałubińska–Jentkiewicz, K. (2015) *Ochrona prywatności w audiowizualnych usługach medialnych na żądanie* [Protection of privacy in on-demand audiovisual media services], available at: http://ikar.wz.uw.edu.pl/numery/30/pdf/86.pdf (October 20, 2020).

Coomaraswamy, R. (2002) Identity Within: Cultural Relativism, Minority Rights and the Empowerment of Women of Women, *George Washington International Law Review*, 34, pp. 483-490.

Complak, K. (1998) Uwagi o godności człowieka oraz jej ochrona w świetle nowej konstytucji, *Przegląd Sejmowy*, 5, pp. 45-51.

Czarnik, Z., Maciejko, W. & Zaborniak, P. (2016) *Ustawa o ewidencji ludności. Komentarz* (Warszawa: Wydawnictwo Wolters Kluwer).

Czaja, J. (2005) *Bezpieczeństwo kulturowe Rzeczypospolitej Polskiej* (Warszawa: Materiały AON. ZUMS BN).

Dybowski, M., (2007) *Prawa fundamentalne w orzecznictwie ETS* [Fundamental rights in the jurisprudence of the ECJ] (Warszawa: Wydawnictwo C.H. Beck).

Doroszewski, W. (1968) *Słownik języka polskiego* (Warszawa: Wydawnictwo PWN).

Domańska, M. (2019) *Zakaz dyskryminacji ze względu na więcej niż jedno zabronione kryterium* (Warszawa: Wydawnictwo Wolters Kluwer Polska).

Donnan, H. & Wilson, T. (2007) *Granice tożsamości, narodu, państwa* (Kraków: add publisher).

Dunn, J. (2007) Introduction: Crisis of the Nation State?, *Political Studies*, 62, pp. 3-15.

Fundowicz, S. & Świtał, P. (2014) *ABC Administracj* [Administration ABC] (Radom: Skauth).

Gałdowa, A. (2000) *Tożsamość człowieka* (Kraków: Wydawnictwo Uniwersytetu Jagiellońskiego).

Gancarz-Wójcicka, B. (2013) *Biblia e-biznesu* [The e-business bible] (Gliwice: Wydawnictwo HELION).

Gajdus, D. & Gronowska, B., (1994) *Stosowanie podsłuchu telefonicznego w ocenie Europejskiej Komisji i Europejskiego Trybunału Praw Człowieka (Refleksje na tle rozwiązań polskich)* [The use of wiretapping in the opinion of the European Commission and the European Court of Human Rights (Reflections against the background of Polish solutions)], Palestra, 11, pp. 115-116.

Jakimowicz, W. (2002) *Publiczne prawa podmiotowe* [Public subjective rights] (Warszawa: Wydawnictwo Zakamycze).

Jaworski, W. L. (1924) *Nauka prawa administracyjnego, zagadnienia ogólne* [Science of administrative law, General issues] (Warszawa: Instytut Wydawniczy "Bibljoteka Polska").

Jarymowicz, M. & Szustrowa, T. (1980) *Poczucie własnej tożsamości - źródła, funkcje regulacyjne*, In: Reykowski, J. (ed.) *Osobowość a społeczne zachowania się ludzi* (Warszawa: Wydawnictwo Książka i Wiedza).

Jakubski, K. J. (1997) *Przestępczość komputerowa – podział, definicja* [Computer crime - division, definitione], *Przegląd Kryminalistyki*, 2, pp. 31-33.

Jellinek, J., (1921) Ogólna nauka o państwie, In: Kitler, W., Czuryk, M. & Karpiuk, M. (Warszawa: Księgarnia F. Hoesicka).

Habermas, J. (1994) Struggles for recognition in the democratic constitutional regime, In: Gutman, A. (ed.) *Multiculturalism* (Princeton: Princeton University Press).

Herbut, J. (1997) *Leksykon filozofii klasycznej* (Lublin).

Hofmokl, J. (2009) *Internet jako dobro wspólne* [Internet as a common good] (Warszawa: Wydawnictwo Akademickie i Profesjonalne).

Hołyst, B. (2011) *Terroryzm*, T. I (Warszawa: Wydawnictwo LexisNexis).

Kawka, W. (1939) *Policja w ujęciu historycznym i współczesnym* (Wilno: Zakład Administracji i Prawa Administracyjnego U.S.B.)

Kitler, W. (2013) *Bezpieczeństwo państwa a bezpieczeństwo narodowe,* In: *Aspekty prawne bezpieczeństwa narodowego RP. Część ogólna*, ed., (Warszawa:)

Klafkowska-Waśniowska, K. (2011) Zasady ochrony danych osobowych w związku ze świadczeniem usług drogą elektroniczną [The rules for the protection of personal data in connection with the provision of electronic services], In: Lubasz, D. & Namysłowska, M. (eds) *Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustaw* [Provision of electronic services and conditional access. Commentary] (Warszawa: Wydawnictwo Lexis Nexis).

Kopff, A. (1972) Koncepcja praw do intymności i do prywatności życia osobistego. Zagadnienia konstrukcyjne [Concept of the rights to intimacy and privacy of personal life. Design issues], *Studia Cywilistyczne*, 20, pp. 3-40.

Kondratiewa-Bryzik, J. & Sękowska-Kozłowska, K., (2013) *Prawa człowieka wobec rozwoju biotechnologii* [Human rights in relation to the development of biotechnology] (Warszawa: Wydawnictwo Wolters Kluwer).

Kondratiewa-Bryzik J. & Sękowska-Kozłowska, K. (2013) *Prawa człowieka wobec rozwoju biotechnologii* (Warszawa: Wydawnictwo Wolters Kluwer Polska).

Konarski, X. (2004) *Komentarz do ustawy o świadczeniu usług drogą elektroniczną* [Commentary to the act on the provision of electronic services] (Warszawa: Wydawnictwo Difin).

Kopff, A. (1972) Koncepcja praw do intymności i do prywatności życia osobistego. Zagadnienia konstrukcyjne [Concept of the rights to intimacy and privacy of personal life. Design issues], *Studia Cywilistyczne*, 20, pp. 3-40.

Kosińska, J. (2008) Prawnokarna problematyka stalkingu [Criminal law issues of stalking], *Gdańsk*, 10, pp. 33-47.

Koziej, S. (2011) Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja, *Bezpieczeństwo Narodowe*, 2, pp. 18-28.

Kozielecki, J. (1981) *Psychologiczna teoria samowiedzy* (Warszawa: Wydawnictwo PWN).

Kopff, A. (1972) Koncepcje prawa do intymności i do prywatności życia. Zagadnienia konstrukcyjne, *Studia Cywilistyczne*, 20, 20-36.

Krasuski, A. (2008) *Dane osobowe w przedsiębiorstwie* [Personal data in the enterprise] (Warszawa: Wydawnictwo Lexis Nexis).

Krzysztofek, M. (2014) *Ochrona danych osobowych w Unii Europejskiej* [Personal data protection in the European Union] (Warszawa: Wydawnictwo C.H. Beck).

Krąpiec, M. A. (2003) *Godność* in: *Powszechna encyklopedia filozofii*, t. 4 (Lublin: Wydawnictwo Polskie Towarzystwo Tomasza z Akwinu).

Kuźniar, P. (1996) Po pierwsze bezpieczeństwo, *Rzeczpospolita*, January 9, 1996.

Kurek, J. (2013) *Ochrona przed niezamówioną korespondencją w komunikacji elektronicznej* [Protection against unsolicited correspondence in electronic communication] (Warszawa: Wydawnictwo C.H. Beck).

Kulesza, M. (1985) *Materiały do nauki prawa administracyjnego* [Materials for learning administrative law] (Warszawa: Wydawnictwo Uniwersytetu Warszawskiego).

Lorenzi, J. **&** Berrebi, M. (2019) *Przyszłość naszej wolności, czyli należy rozmontować google'a …i kilku innych* **[**Progress or Freedom. Who Gets to Govern Society's Economic and Technological Future?**]** (Warszawa: Państwowy Instytut Wydawniczy).

Longchamps, F. (1966) Współczesne problemy podstawowych pojęć prawa administracyjnego [Contemporary problems of basic concepts of administrative law], Państwo i Prawo, 6, 891-865.

Lunenfeld, P. (2010) Generacje: Jak komputer stał się maszyną generująca nasza kulturę?, In: Celiński, P. (ed.) *Mindware. Technologie dialogu* (Lublin: Wydawnictwo UMCS).

Mandrosz-Wróblewska, J. (1988) *Tożsamość i niespójność ja, a poszukiwanie własnej odrębności* (Warszawa: Ossolineum).

Malarewicz, A. (2009) *Konsument a reklama: studium cywilnoprawne* [The consumer and advertising: a civil law study] (Warszawa: Wydawnictwo Wolters Kluwer Polska).

Młynarska-Sobaczewska, A. (2009) In: Skrzydło, W., Grabowska S. & Grabowski, R. (eds) *Konstytucja Rzeczypospolitej Polskiej. Komentarz encyklopedyczny* [Constitution of the Republic of Poland. Encyclopedic commentary] (Warszawa: Wydawnictwo Wolters Kluwer).

Namysłowska, M. (2011) Zgoda usługobiorcy [Service recipient consent], In: Lubasza, D. & Namysłowska, M. (eds) *Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz o ustawy* [Provision of electronic services and conditional access. Commentary] (Warszawa: Wydawnictwo Lexis Nexis).

Namysłowska, M. (2012) *Reklama: aspekty prawne* [Advertising: legal aspects] (Warszawa: Wydawnictwo Wolters Kluwer).

Ormsby, E. (2019) *Darknet* [Darknet] (Warszawa: Wydawnictwo Społeczny Instytut Wydawniczy Znak).

Perritt Jr. H. H. (1996) *Law and the Information Superhighway. Privacy, Access, Intelectual Property, Commerce, Liability* (New York, Chichester, Brisbane, Toronto, Singapore: John Wiley & Sons, INC).

Radwański, Z. (1997) *Prawo cywilne - część ogólna* [Civil law - general part] (Warszawa: Wydawnictwo C.H. Beck).

Rączka, G. (2007) *Ochrona usługobiorcy usług elektronicznych* [Protection of the recipient of electronic services] (Toruń: Wydawnictwo Towarzystwo Naukowe Organizacji i Kierownictwa).

Rogacka-Łukasik, A. (2012) Naruszenie dóbr osobistych w internecie oraz ich ochrona na podstawie ustawy o świadczeniu usług drogą elektroniczną [Infringing of the personal goods on the internet and their protection on the basis of the bill concerning providing services by the electronic way], *Roczniki Administracji i Prawa. Teoria i Praktyka*, 12, 233-252.

Stalla - Bourdillon, S., Phillips, J. & Ryan, M. D. (2014) *Privacy vs. Security* (New York: Dordrecht).

Sienkiewicz, P. (2009) Terroryzm w cybernetycznej przestrzeni [Terrorism in cybernetic space], In: Jemioło, T., Kisielniecki, J. & Rajchel, K. (eds.) *Cyberterroryzm – nowe wyzwania XXI w.* [Cyberterrorism - new challenges of the 21st century] (Warszawa).

Sarnecki, P. (2003) Uwagi do art. 41 Konstytucji RP, In: Garlicki, L. (ed.) *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, vol. 3, (Warszawa: Wydawnictwo Sejmowe).

Safjan, M. (2002) *Refleksje wokół konstytucyjnych uwarunkowań rozwoju ochrony dóbr osobistych* [Reflections on the constitutional conditions for the development of protection of personal rights], *Kwartalnik Prawa Prywatnego*, 1, pp. 234.

Sobczak, J., (2017) Cyberprzestrzeń jako obszar ochrony bezpieczeństwa narodowego, w optyce dokumentów europejskich [Cyberspace as an area of national security protection, in the view of European documents], In: Herbowski, P., Słapczyńska, D. & Jagiełło, D. (eds) *Pozyskiwanie informacji w walce z terroryzmem* [Obtaining information in the fight against terrorism] (Warszawa: Wydawnictwo Difin).

Sokolewicz, W. (1985) Prawo do prywatności, In: Pastusiak, L. (ed.) *Prawa człowieka w Stanach Zjednoczonych* (Warszawa: Książka i Wiedza).

Sójką – Zielińska, K. (2006) *Jednostka a państwo w dziejach europejskiej kultury politycznej* **[**The individual and the State in the history of European political culture **],** In: Wyrzykowski, M. (ed.) *Prawa stają się prawem. Status jednostki a tendencje rozwojowe* **[**Rights Become Law. Individual status and development trends**]** (Warszawa: Wydawca Liber).

Smoleński, P. (2013) Syn idzie do wojska. Boję się, *Wysokie Obcasy*, 28(735), pp. 22-23.

Stańczyk J. (1996) *Współczesne pojmowanie bezpieczeństwa* (Warszawa: ISP Polska Akademia Nauk).

Sieńczyło-Chlabicz, J., Zawadzka, Z. & Nowikowska, M. (2019) *Prawo prasowe* [Press Law] (Warszawa: Wydawnictwo Wolters Kluwer).

Sienkiewicz, P. (2009) Terroryzm w cybernetycznej przestrzeni [Terrorism in cybernetic space], In: Jemioło, T., Kisielniecki, J. & Rajchel, K. (eds) *Cyberterroryzm – nowe* Szot, L. (2018) *Protection of personal data in the context of the right to be forgotten*, In: Taczkowska-Olszewska, J., Brzostek, A., & Nowikowska, M. (eds) *Reform of the protection of personal data system. Purpose. Tools. Effects* (Poznań: Wydawnictwo Siva Rerum) pp. 23-40.

Szpunar, A. (1974) *Nadużycie prawa podmiotowego* [Abuse of subjective law] (Kraków: Wydawnictwo Polska Akademia Umiejętności).

Wang, H., Lee, M. K. & Wang, C. (1998) Consumer privacy concerns about Internet marketing, *Communications of the ACM*, 41(3), pp. 63-70.

Winczorek, P. (2003) *Prawo Konstytucyjne Rzeczypospolitej Polskiej* (Warszawa: Wydawnictwo Liber).

Wilk, A. (2014) *Akt urodzenia* (Warszawa: Wydawnictwo LexisNexis).

Wolfe, P., Scott, M. & Erwin, M. W. (2012) *Anti – spam Tool kid* (Warszawa: Wydawnictwo Helion).

Zakrzewski, W. (1998) *Podstawowe wolności, prawa i obowiązki człowieka i obywatela* In: Skrzydło, W., (ed) *Polskie prawo konstytucyjne* (Lublin: Wydawnictwo VERBA).
Ziembiński, Z. (1980) *Problemy podstawowe prawoznawstwa* [Fundamental problems of jurisprudence] (Warszawa: Wydawnictwo PWN).

Institute for Local Self-Government Maribor

www.lex-localis.press
info@lex-localis.press