Adam Rogala-Lewicki

CLASSIFIED METHODS OF COLLECTING INFORMATION ON THE CITIZENS –COMPARATIVE LEGAL STUDY OF INVIGILATION IN POLAND

Classified methods of obtaining information should be secured with a higher degree of caution and civil supervision. The paradox of Western democracies is that officially human rights are at the epicenter of the legal system, but in reality, covert techniques for obtaining data about citizens are complex and used to such an extent that they clearly disregard the universal right to privacy. In order to recognize the secret activity of intelligence services as compliant with the requirements of a democratic rule of law, there must be an adequate legal protection tools that will allow effective counteracting information arbitrariness. Meanwhile, the cases of recent years indicate the dominant trend of extending the sphere of competences of state services in the field of obtaining data (most often under the guise of ensuring security) with interference to the private domain of citizens.

Keywords: *security, intelligence, government, political system, privacy, secret services, information, invigilation.*

NIEJAWNE METODY POZYSKIWANIA INFORMACJI O OBYWATELACH – STUDIUM PRAWNOPORÓWNAWCZE INWIGILACJI W POLSCE

Tajne sposoby pozyskiwania informacji winny być zabezpieczone podwyższonym stopniem ostrożności i nadzoru cywilnego. Paradoks państw demokratycznych świata zachodniego polega na tym, że oficjalnie prawa człowieka znajdują się w epicentrum systemu prawnego, w rzeczywistości jednak niejawne techniki pozyskiwania danych o obywatelach są rozbudowane i wykorzystywane do tego stopnia, iż w sposób oczywisty lekceważą powszechne prawo do prywatności. Aby uznać tajną działalność służb za zgodną z wymogami demokratycznego państwa prawnego muszą istnieć odpowiednie narzędzia ochrony prawnej, które pozwolą na skuteczne przeciwdziałanie samowoli informacyjnej. Tymczasem przypadki ostatnich lat wskazują na dominujący trend poszerzania sfery kompetencji służb państwowych w zakresie pozyskiwania danych (najczęściej pod pozorem zapewnienia bezpieczeństwa) kosztem ingerencji w domenę prywatną obywateli.

Słowa kluczowe: *bezpieczeństwo, wywiad, rząd, system polityczny, prywatność, służby specjalne, informacja, inwigilacja.*

Introduction

The paradox of the intelligence world in the democratic countries of the Western world is that officially human rights are in the first place, including, for example, the protection of the privacy of the individual and society, but in fact the security sphere has taken place for its information comfort of work, largely using the domain of confidentiality[1]. Christopher Adrew distinguished three main reasons for maintaining the cult of secrecy in the public sphere: the historical legacy of assigning excessive importance to all public activities, the obsession with secrecy, and finally international law prohibiting the interception of diplomatic correspondence[2].

The explicit compulsion of citizens to provide certain information to the relevant public authorities, or *vice versa* - the disposition requiring the state authorities to search for specific data, contain legal procedures. The state may require from citizens only such information (and in no case other) that is described in a generally binding normative acts (consistent with the Constitution) and is necessary for the activity of the state, and does not violate the civil right to privacy. In this respect, the methods of obtaining data may not be incompatible, for example, with the provisions on the protection of personal data. The *ex definitione* model of law-making eliminates cases of open obtaining information about citizens, which would violate the relevant standards in this regard. It can be argued whether a certain type of information is really needed. However, one should certainly strive to ensure that the state observes the principle of restraint in collecting data and does not relativize the general clause of indispensability for its own needs. While overt information tools have a clearly defined beginning and end, the case is not so obvious in the case of secret methods. Thus secret methods of obtaining information should be accompanied by a greater degree of caution and supervision[3].

William E. Colby, a longtime CIA chief, presented an excellent analysis of the compatibility of secret sphere in a free society. Colby believes that the hidden and open sphere in a democratic state cannot be treated dichotomously, because both (exposure, secrecy) are necessary for a truly free society[4]. Without secrecy, democracy could not function (e.g. secret voting in elections, patient-doctor, lawyer-client relationship). In this regard, a proper (well-balanced) concept of confidentiality must be established for the new technological society. Traditional

[1] See Dufresne R.L. Offstein E.H., On the Virtues of Secrecy in Organizations, „*Journal of Management Inquiry*" 2008, no. 17 (102). See more Little L. Privacy, Trust, and Identity Issues for Ubiquitous Computing, „*Social Science Computer Review*" 2008, no. 26; Garson G.D., Securing the Virtual State: Recent Developments in Privacy and Security, „*Social Science Computer Review*„ 2006, no. 24 (489); Gadzheva M., Privacy in the Age of Transparency, „*Social Science Computer Review*" 2007, no. 26 (60).

[2] Whitehall Ch.A., Washington and the Intelligence Services, „*International Affairs*" 1977, vol 53, no. 3, pp. 390-404.

[3] See Rogala-Lewicki A., Participation of intelligence services in political decision-making process – evolution of coordination patterns in Poland, "*Studium Europy Środkowej i Wschodniej*" 2020, no. 13.

[4] Flanagan, S.J. Managing the Intelligence Community, „*International Security*" 1985, vol 10, no. 1, pp. 58-95. See more Davis P.H.J. Intelligence and the Machinery of Government: Conceptualizing the Intelligence Community, „*Public Policy and Administration*" 2010, no. 25 (29); Omand D. Creating Intelligence Communities, „*Public Policy and Administration*" 2010, no. 25 (99); Smith M.J. Intelligence and the Core Executive, „*Public Policy and Administration*", 2010, no. 25.

power using secret services, unlike the citizen, historically had more means of obtaining information at their disposal, including modern tools, such as: satellites, data capture systems, eavesdropping tools, communication networks (once used only for military, academic purposes and transformed into a global network – e.g. the Internet)[5]. This includes the first satellite world map, now available on the Internet, previously used only by special services, or the Echelon system, which is a global electronic intelligence channel[6]. The system was created under the AUSCANNZUKUS agreement and is managed by the American NSA[7], being installed in different parts of the world. The system is equipped with technical devices for eavesdropping and intercepting information sent *via* telecommunication channels and its task is to collect and analyze electronic messages occurring around the world in the form of faxes, e-mails, file transfers or telephone calls. All captured data is transferred to the US headquarter in Fort Meade, where supercomputers automatically select the collected material in terms of passwords, language and other categories. It is estimated that at the beginning of the 20th century, the system was able to intercept approx. 3 billion electronic information transfers per day[8]. Moreover, since 2007, the National Security Agency has been administering a secret spy program called PRISM, which allows US intelligence to access data stored on the servers of the largest Internet companies, such as: Google, Facebook, Microsoft, Jahoo! Inc, Youtube, Skype, AOL or Apple[9].

Of course, secret services cannot be treated as institutions acting to the detriment of citizens and against their interests. Rather, the issue is about how the authorities use information. As one knows, the information revolution apparently changed the shape of these relations. The process of obtaining information about the assets and activities of citizens is carried out on many different levels and by almost all state agencies. However, while the boundaries of overt methods of collecting information are clearly delineated by legal regulations, confidential methods leave free space for abuse, over-interpretation and instrumental use.

[5] See Siemiątkowski Z. *Wywiad a władza. Wywiad cywilny w systemie sprawowania władzy politycznej PRL*, Warszawa 2009. See also Rogala-Lewicki A., *Informacja jako autonomiczny czynnik wpływu. Studium władztwa informacyjnego*, Częstochowa 2013.

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

[7] Colby W.E. Intelligence Secrecy and Security in a Free Society, „International Security 1976", vol 1, no. 2, pp. 3-14. In the United States, the unit responsible for the information security of the state – the National Security Agency – equipped with all possible channels (radio, telephone, IT) intercepting information that may be important for the state, *de facto* has for years been constantly tracking its own citizens. Already in the 1960s it was revealed that it had all the recordings of telephone calls from the US residents. The decree of the President of the United States, Harry S. Truman in 1952 establishing the NSA, was top secret. Until today, the statute of the NSA is mostly secret, which means that the average citizen has no right to know what this organization does and to what extent it interferes with his private life. For many years, NSA employees and their family members were not entitled to use the employer's name when asked about their workplace. The version in force was employment with the US Department of Defense (DoD). Agency employees are constantly subject to numerous restrictions. They are obliged, for example, to use only the help of dentists approved by the NSA security office. Moreover, they must inform about people with whom they have relationships or about each trip abroad. Such forms of security and secrecy led to the fact that over time the agency developed a grotesque abbreviation of its name: NSA – No Such Agency. See Thompson E.P. The secret state, „Race Class" 1979, no. 20 (219).

[8] See Rogala-Lewicki A., Struktura organizacyjna służb specjalnych – ilustracja w oparciu o wybrane modele państw i systemy polityczne, „*Studium Europy Środkowej i Wschodniej*" 2016, no. 6.

[9] NSA Prism program taps in to user data of Apple, Google and others, „*The Guardian*", 7.06.2013, http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data (access: 22.12.2020)

International law aspect

The Polish legal order cannot contradict the principles established in international law. The starting point are international regulations to which Poland is a signatory and party[10]. For example, art. 17 of the International Convention on Civil and Political Rights[11] proclaims that no one can be exposed to arbitrary or unlawful interference with his private life, family, home or correspondence. The disposition of this norm also extends to such broad and capacious material values as the honor (honor) and good name (reputation) of each individual. Convention for the Protection of Human Rights and Fundamental Freedoms together with the case law of the European Court of Human Rights[12] outlines a clear guideline for national legislators on the construction of standards governing the covert operation of law enforcement agencies and secret services. Art. 8 sec. 1 shows that everyone has the right to communicate with whomever he wishes and in this respect he is entitled to have respected confidentiality of his correspondence. According to art. 8 sec. 2 of the European Convention, the interference of public authorities with the exercise of the right to respect for correspondence is unacceptable, except in cases provided for by law and necessary in a democratic society for the sake of state security, public safety or economic well-being of the country, protection of order and prevention of crime, protection of health and morals. or protection of the rights and freedoms of others. The right to respect the confidentiality of correspondence and communication is not an absolute right, nevertheless any restrictions in this respect must refer to the protection of the critical interests of the state and citizens, which expressly results from the content of the norm regulated in the Convention. Article 49 of the Polish Constitution clearly corresponds to the norm contained in the European Convention on Human Rights[13]. The breach of the basic principle is allowed only in the

[10] Kosmaty P., Granice tajnej inwigilacji obywateli w demokratycznym państwie prawa, „Prokurator", no. 3, 2008, pp. 4

[11] Adopted by the United Nations General Assembly in 1966. (Journal of Laws 1977 No. 38, item 167).

[12] The case law of the European Court of Human Rights defines the concept of necessary interference, as referred to in art. 8 sec. 2 of the European Convention on Human Rights, specifying that the interference is related to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued, but also to the specific nature of the interference in question. Such interpretations can be found, among others: (a) in the judgment of the ECtHR of March 26, 1987, in the case of Leander v. Sweden (complaint no. 9248/81); (b) in the judgment of 16 February 2000 - the case of Amann v. Switzerland, in which the ECtHR pointed out that the mere fact of collecting data about an individual is sufficient for interference with private life, regardless of the subsequent use; (c) in its judgment of 6 June 2006 in the case of Segerstedt - Wiberg and others v. Sweden, where the ECtHR stressed that when considering the need to protect security, the severity of interference with the right to respect for private life should be taken into account, and that every citizen must have a legal remedy enabling the control of data held by the security services (complaint no. 62332/00); (d) in the decision of 26 June 2006, in the case of Weber and Saravia v. Germany, in which the ECtHR summarized the previous case-law in this respect (complaint no. 54934/00).

[13] Art. 49 of the Polish Constitution in many material and legal situations is in line with art. 51 and art 31 of the Constitution. The circumstances in which the constitutionality of the provisions granting information rights to the authorities vis-à-vis citizens is considered oblige the norms of these three articles and are considered, as if by necessity, in their convergence and coincidence. Pursuant to art. 51 sec. 1, no one may be obliged, other than under the act, to disclose information about his person. Public authorities cannot obtain, collect and share information about citizens other than that necessary in a democratic state ruled by law. In turn, art. 51 sec. 4 stipulates that everyone has the right to demand rectification and removal of false, incomplete or collected information in a manner inconsistent with the act. The system of three constitutional norms creates the so-called the information autonomy of an individual, which implies: first, the right to independently decide about disclosing information about himself to others, and second, the right to control entities possessing such information in terms of their possession and use. This autonomy means the right to decide about the disclosure of information relating to yourself, as well as the right to control such information if it is in the possession of other entities.

cases provided in the act. The Constitution of the Republic of Poland allows limiting the exercise of civil liberties and rights only when it is necessary in a democratic state for its safety or public order, or for the protection of the environment, health and public morality, or the freedom and rights of other people. The basic law stipulates that the freedom and secrecy of communication are ensured. Their limitation may only take place in the cases specified in the act and in the manner specified therein. The jurisprudence of the Constitutional Tribunal ensures the interpretation of regulations. „Obtaining information about persons is permissible, but only in certain circumstances, subject to specific conditions, and (...) the legislator may in no case arbitrarily mitigate the conditions under which one may enter the sphere of private life without exposing himself to the accusation of unconstitutional arbitrariness"[14].

The Constitutional Tribunal has repeatedly expressed its unambiguous interpretation of norms when examining the constitutionality of various provisions. For example, in the case, at the request of a group of deputies of September 30, 2004, for examination of the constitutionality of art. 1 and art. 8 pts 27 (in the part amending articles 36-36e of the Act of 28 September 1991 on fiscal control) of the act of 27 June 2003 on the establishment of Provincial Tax Colleges and amending certain acts regulating the tasks and competences of organs and the organization of units subordinate to the minister competent for public finance[15], carefully examined the constitutionality of the prerogatives granted to the treasury intelligence. The Constitutional Tribunal considered that "the powers granted to the tax intelligence on the basis of the challenged amendment undoubtedly penetrate deeply into the sphere of an individual's private life. (...) Fact that this right is - pursuant to art. 233 paragraph. 1 of the Constitution - inviolable even in the acts limiting other rights, issued under martial law. This means that even such exceptional and extreme conditions do not allow the legislator to lose the conditions under which one may enter the sphere of private life without exposing himself to the accusation of unconstitutional arbitrariness (see the judgment of the Constitutional Tribunal of November 20, 2002, file no. K 41/ 02, OTK ZU No. 6/A /2002, item 83). (...) Protection of private life, constitutionally guaranteed in principle in art. 47, also includes information autonomy (article 51 of the Constitution), meaning the

[14] The judgment of the Constitutional Tribunal of 20 June 2005, K 4/04 OTK-A 2005/6/64. In the judgment cited, the Constitutional Tribunal repeatedly refers to the issue of moderation of the space of surveillance powers. Cases in which obtaining information about a citizen without his consent is permissible must be clearly described and defined. In order to recognize the secret activity of the services as compliant with the requirements of a democratic rule of law, there must be adequate legal protection tools that will allow for effective counteracting of information violation. Proper interpretation of the regulations by the competent courts is invaluable here. It is about balancing the centers of power. Only an independent judicial review can eliminate the arbitrariness of state institutions in this respect. The content of the above-mentioned model of control has been repeatedly specified and discussed in detail in the previous jurisprudence of Tribunal, including in the judgments of the Constitutional Tribunal of: June 24, 1997, file ref. K. 21/96 (OTK ZU No. 2/1997, item 23), of April 11, 2000, ref. No. K. 15/98 (OTK ZU No. 3/2000, item 86), February 19, 2002, ref. No. U 3/01 (OTK ZU No. 1 / A / 2002, item 3), November 12, 2002, ref. SK 40/01 (OTK ZU No. 6 / A / 2002, item 81), of November 20, 2002, ref. No. K 41/02 (OTK ZU No. 6 / A / 2002, item 83), of June 20, 2005, file ref. K 4/04 (OTK ZU No. 6 / A / 2005, item 64), of November 20, 2002, ref. K 41/02, OTK ZU no. 6 / A / 2002, item. 83 and in the decision of the Constitutional Tribunal of 2008-06-09 ref. K 8/04. As a result, jurisprudence has been developed in this respect.

[15] Journal of Laws 2003 No. 137, item 1302.

right to independently decide on disclosing information about oneself to others, as well as the right to exercise control over such information if it is in the possession of other entities (cf. February 19, 2002, file No. U 3/01, OTK ZU No. 1/A/ 2002, item 3). Information on the economic sphere of an individual are undoubtedly subject to privacy and informational autonomy, although in this sphere there are milder criteria for limiting it than in the purely personal sphere (see judgments of June 24, 1997, file no. K 21/96, OTK ZU No. 2/1997, item 23; April 11, 2000, ref. No. K. 15/98, OTK ZU No. 3/2000, item. 86; November 20, 2002, ref. No. K 41/02, OTK ZU No. 6/A/2002, item 83). (...) Analyzing the motives of the legislator when adopting the Act on fiscal control, the Constitutional Tribunal emphasized that one of the most important functions of a democratic rule of law is to effectively combat these negative phenomena, which may, to an extreme extent, threaten the very existence of this state. Therefore, the legislator has not only the right, but also the obligation to combat negative phenomena by granting such powers to control state agencies, while being in line with the principles of the Constitution, will have a direct impact on increasing the efficiency of control activities (...), the Constitutional Tribunal therefore allows special powers, stressing at the same time the necessity to ensure compliance of such regulations with the Constitution. (...) When assessing the admissibility of interference, it should be considered whether it meets the conditions set out in art. 31 sec. 3 of the Constitution. Besides, the legislator - in the light of art. 2 of the Constitution - has the constitutional obligation to define the conditions for interference in the sphere of privacy as precisely as possible, so as to limit the scope of the discretion left to the authorities applying the law, and at the same time has the obligation to create appropriate mechanisms of control over acts of public authority bodies affecting this sphere. When it comes to limiting constitutional human and civil rights and freedoms, the provisions must be characterized by precision and clarity. This order is functionally related to the principles of legal certainty and security and the protection of trust in the state and law. (...) In the opinion of the Constitutional Tribunal, it should be assumed that obtaining information about persons is permissible, but only in certain circumstances, with special conditions that the legislator did not indicate in the case of the discussed regulation. (...) In the opinion of the Constitutional Tribunal, the legislator outlined too broadly the area of interest of the tax intelligence in the context of the right to obtain information about persons. (...) Taking into account the previous findings, the Constitutional Tribunal decided that art. 8 point 27 of the Act on in the scope in which it amends art. 36 sec. 2 of the Act on fiscal control - in the part concerning obtaining, collecting, processing and using information about persons, is inconsistent with art. 2 of the Constitution due to the fact of imprecise nature of the provisions, it violates the principles of proper legislation and, as a consequence, unjustly enters the sphere of privacy, which is also inconsistent with art. 47, art. 49, art. 51 sec. 2 in connection with art. 31 sec. 3 of the Constitution. (...) For the same reasons, the amendment to art. 36a of the Act on fiscal control, which entitles employees of the tax intelligence who

perform the activities referred to art. 36 sec. 2, to observe and record, using technical means, the image of events and the sound accompanying these events in public places"[16].

The quoted sentence of the Constitutional Tribunal emphasizes the huge role of judicial decisions in the process of delineating the demarcation line for the actions of state agencies. In the cited judgment, the Constitutional Tribunal repeatedly refers to the issue of complex measurement of the space of surveillance powers. Cases in which obtaining information about a citizen without his consent is permissible must be clearly described and defined. In order to recognize the secret activity of public services as compliant with the requirements of a democratic rule of law, there must be adequate legal protection tools that will allow effective counteracting of information willfulness. Proper interpretation of the regulations by the competent courts is invaluable here. It is about mutual balancing of centers of power. Only independent judicial control[17] may eliminate the arbitrariness of state institutions in this respect.

Operational supervision

In the field of information rights of Polish officers, the most sensitive issues concern the operational control. The conditions and nature of operational control are determined, *inter alia*, by art. 19 of the Act of April 6, 1990 on the Police, art. 9e of the Act of October 12, 1990 on the Border Guard, art. 36c of the Act of 28 September 1991 on fiscal control, art. 31 of the Act of August 24, 2001 on the Military Police and military law enforcement bodies, art. 27 of the Act of May 24, 2002 on the Internal Security Agency and the Foreign Intelligence Agency, art. 31 of the Act of June 9, 2006 on the Military Counterintelligence Service and the Military Intelligence Service and art. 17 of the Act of June 9, 2006 on the Central Anticorruption Bureau[18].

Operational supervision is performed covertly and consists, in accordance with the standards, in controlling the content of correspondence, controlling the content of parcels, applying technical means enabling the covert acquisition of information and evidences and their recording, in particular the content of telephone calls and other information provided by telecommunications networks[19]. Apart from its structure, this legal instrument contains other, inseparable elements characterizing its system.

[16] Constitutional Tribunal sentence 20.06.2005, K 4/04 (OTK-A 2005/6/64).

[17] Judicial control of the usage of secret instruments enabling obtaining information about citizens is not the only model of supervision used in democratic countries. There are also constructions of extrajudicial control in the form of independent committees, or other bodies usually composed of representatives of the legislature. In June 2011, a ministerial proposal was made to establish an independent body to control operational work. Belgium, Canada, the Netherlands, Norway and Sweden were mentioned as examples of countries in which such bodies operate. Its members would be partly judges elected by the National Council of the Judiciary, and partly experts appointed by the Sejm. Such a committee would have more extensive powers than today's parliamentary special services committee. The new control body would be commissioned by the parliamentary commission, but it could also consider direct complaints from citizens. See *Koniec z podsłuchiwaniem obywateli*, http://prawo.gazetaprawna.pl/artykuly/534298,koniec_z_podsluchiwaniem_obywateli.html, (22.12.2020).

[18] Historically, in the public sphere, there was a concept of comprehensive organization of national regulations in the field of operational and investigative activities, in particular in the part concerning the rights of officers to operate. Act was even underway on a draft setting out the rules for the use of operational and reconnaissance activities by the services. The bill submitted to the Sejm in 2007, however, never entered into force.

[19] Art. 27 of 24.05.2002 Act of on the Internal Security Agency and the Foreign Intelligence Agency (Journal of Laws 2010 No 29, item 154).

Firstly, the operational control is ordered by the district court in Warsaw in the case of the Internal Security Agency, and in the case of the police, by the district court competent for the seat of the police authority submitting the request.

Secondly, in the case of the police, the process of launching operational control takes place upon a written request of the Chief Police Commander, submitted after obtaining the written consent of the Public Prosecutor General, or upon a written request of the Voivodship Police Commander, submitted after obtaining the written consent of the locally competent district public prosecutor. In the case of the Internal Security Agency, it takes place at the written request of the head of the Internal Security Agency, submitted after obtaining the written consent of the prosecutor general.

Third, the operational control relates to crimes exhaustively listed in the legal norms. The catalog of crimes in which the police may request the application of operational control is extensive and is precisely described in art. 19 paragraph 1, points 1 to 8 of the Police Act[20]. In the case of the Internal Security Agency, the description refers to specific categories of criminal offenses or concerns (using general clauses) broadly understood as an activity that may harm the interests of the state. In the act[21] the following categories of crimes are mentioned: espionage, terrorism, breach of state secrets and other crimes detrimental to state security; crimes affecting the economic foundations of the state, corruption of persons performing public functions[22] - if it may harm the security of the state, but also crimes in the field of production and trade in goods, technologies and services of strategic importance for the security of the state. Finally, the crime of illegal production, possession and trade in weapons, ammunition and explosives, weapons of mass destruction as well as narcotic drugs and psychotropic substances in international trade.

Fourth, the operational control is subsidiary, which means that it is admissible only if other measures have proved ineffective or there is a high probability that they will be ineffective or not useful. After the amendment of the regulations, the submission of an application for

[20] The catalog covers only intentional crimes or a series of intentional crimes prosecuted by public prosecution: (1) against life, as defined in Art. 148-150 of the Criminal Code; (2) specified in art. 134, art. 135 § 1, art. 136 § 1, art. 156 § 1 and 3, art. 163 § 1 and 3, art. 164 § 1, art. 165 § 1 and 3, art. 166, art. 167, art. 173 § 1 and 3, art. 189, art. 189a, art. 200, art. 200a, art. 211a, art. 223, art. 228 § 1 and 3-5, art. 229 § 1 and 3-5, art. 230 § 1, art. 230a § 1, art. 231 § 2, art. 232, art. 245, art. 246, art. 252 § 1-3, art. 258, art. 269, art. 280-282, art. 285 § 1, art. 286 § 1, art. 296 § 1-3, art. 296a § 1, 2 and 4, art. 299 § 1-6 and article. 310 § 1, 2 and 4 of the Criminal Code; (2a) specified in art. 46 sec. 1, 2 and 4, art. 47 and art. 48 sec. 1 and 2 of the Act of June 25, 2010 on sport (Journal of Laws of 2010, No. 127, item 857); (3) against the economic turnover, referred to in Art. 297-306 of the Criminal Code, causing damage to property or directed against property, if the amount of damage or the value of property exceeds fifty times the amount of the lowest remuneration for work specified on the basis of separate provisions; (4) tax, if the value of the subject of the act or the reduction of public law receivables exceeds fifty times the amount of the lowest remuneration for work determined on the basis of separate regulations; (4a) tax referred to in art. 107 § 1 of the Fiscal Penal Code; (5) illicit manufacture, possession or trade in weapons, ammunition, explosives, narcotic drugs or psychotropic substances or their precursors as well as nuclear and radioactive materials; (6) referred to in art. 8 of the Act of June 6, 1997 - provisions introducing the Penal Code (Journal of Laws of 1997 No. 88, item 554 and No. 160, item 1083 and of 1998 No. 113, item 715); (7) specified in art. 43-46 of the Act of July 1, 2005 on the collection, storage and transplantation of cells, tissues and organs (Journal of Laws of 2005, No. 169, item 1411); (8) prosecuted under international treaties and agreements.

[21] Art. 5 sec. 1 point 2 points a) to e) of the Act of May 24, 2002 on the Internal Security Agency and the Foreign Intelligence Agency (Journal of Laws of 2010, No. 29, item 154, as amended).

[22] Journal of Laws of 2006 No. 216, item 1584.

consent to apply an operational control was made conditional on the submission of materials justifying the need for it[23].

Fifthly, the regulations define the duration of operational control which is ordered for a period not longer than 3 months! The court may, at the written request of the Head of the Internal Security Agency, submitted after obtaining the written consent of the public prosecutor general, or in the case of the police, at the written request of the Police commander in chief or the provincial Police commander, submitted after obtaining the written consent of the competent prosecutor, extend the operational control for another 3 months, if the reasons for ordering this control have not ceased.

Sixthly, the legislator provided justification for the application of operational control - it should be completed as soon as the reasons for its order have ceased, but at the latest after the period for which it was introduced.

Seventh, if as a result of operational activities, no grounds for initiating criminal proceedings have been found, and the materials obtained as a result of the operational control turned out to be useless for the proceedings, they shall be immediately destroyed[24]. The amendment to these provisions of February 2011 introduced a general rule, which stipulates that the materials collected during the application of operational control that do not contain evidence allowing the initiation of criminal proceedings or evidence relevant to the pending criminal proceedings, shall be immediately, and officially destroyed. The destruction of the materials is ordered by the police authority that requested the operational control. The police authority is obliged to immediately notify the appropriate public prosecutor about the issuance and execution of the order concerning the destruction of materials[25]. In the case of wiretapping materials, which, in the opinion of intelligence, are not without significance for the security of the state, may be detained only after approval by the Warsaw district court, upon a written request from the head of the service and after obtaining the consent of the prosecutor.

---

[23] Art. 3 of the Act of February 4, 2011 amending the Act - Code of Criminal Procedure and certain other acts (Journal of Laws of 2011, No. 53, item 273).

[24] However, the implementation of this rule was not consistent. It turns out that pursuant to art. 19 paragraph 17 of the Police Act, the materials were stored after the end of the inspection for a period of 2 months. A similar solution was applied pursuant to art. 31 sec. 18 of the Act on Military Police and military law enforcement agencies. This meant that the legal order in this respect, which disciplined the police and military police, was different than that provided for the Border Guard, CBA, ABW, AW, SKW and SWW. The inconsistency and lack of legal equity in this matter was pointed out by the Ombudsman in his letter of 26 October 2009 to the Prime Minister (reference number RPO-631981-II-09 / ST), in which he noted that there was a justified doubt as to whether such a legal status corresponds to the constitutional principle of equality (Article 32 of the Polish Constitution). According to the Ombudsman, there is also a doubt whether it corresponds to the content of art. 51 sec. 2 of the Constitution, according to which public authorities may not obtain, collect and make available information about citizens other than necessary in a democratic state ruled by law. Ombudsman further emphasized that since the operational control was ordered for a strictly defined purpose, i.e. to detect and identify the perpetrators of specific crimes, and the materials collected in its course did not allow for the initiation of criminal proceedings, the purpose for which these materials were obtained was lost. As a result, their further collection is no longer necessary within the meaning of art. 51 sec. 2. In this situation, in the opinion of Ombudsman - Art. 19 paragraph 17 of the Police Act and Art. 31 sec. 18 of the Act on Military Police and military law enforcement agencies, does not refute the allegation not only of non-compliance with Art. 32 of the Polish Constitution, but also the allegation of non-compliance with Art. 51 sec. 2 of the Polish Constitution. See: Letter of the Ombudsman of October 26, 2009 to the Prime Minister (reference number RPO-631981-II-09 / ST).

[25] Art. 3 of the Act of February 4, 2011 amending the Act - Code of Criminal Procedure and certain other acts (Journal of Laws of 2011, No. 53, item 273) amending para. 17 and the introductory part 17a in art. 19 of the Police Act.

Eighth, on the basis of the provisions of the Act amending operational control, the principle of prohibiting the use of evidence obtained as a result of procedural and operational control in proceedings other than the criminal procedure (proceedings before civil courts or labor courts) was introduced[26].

Ninthly, the same amendment obligated the public prosecutor general to present to the Sejm and the Senate annual, public information on the number of applied operational techniques. The statistics are to contain data on the effects of judicial and prosecutor's supervision over these activities. The report must contain precise data on „the total number of persons against whom a request for an inspection and recording or an application for an operational inspection has been addressed, indicating the number of persons for whom: the court ordered inspection and recording or operational inspection, the court refused an order for inspection and recording or an operational inspection, the request for operational inspection did not obtain the prosecutor's consent. The information should be presented to the Sejm and Senate by June 30 of the year following the year covered by it"[27].

Wiretapping

The usage of wiretapping as an operational tool also takes place in the Polish criminal trial. The provisions mention both the wiretapping of telephone conversations (article 237 § 1) and other conversations or transmissions of information, including correspondence sent by e-mail (article 241) – in order to detect and obtain evidence for the pending proceedings or to prevent the commission of a new crime"[28]. This means that wiretapping (not the same as operational control), as a way of obtaining evidence (evidence in the proceedings), may be ordered only after issuing an order to initiate an investigation, and in extraordinary/urgent situations. Therefore, wiretapping cannot be used during pre-trial checking activities. The legislator provided categories of special cases. „In urgent cases, the control and recording of the content of telephone conversations may be ordered by the prosecutor, who is obliged to apply to the court within 3 days for approval of the decision. The court issues a decision on the request within 5 days at the meeting without the participation of the parties. In the event of non-approval of the prosecutor's decision, the court orders the destruction of all fixed records in the decision issued on the application. Appealing against the decision suspends its execution"[29]. The amendment to the Code of Criminal Procedure of June 2011 added the necessity to destroy the recorded content in the event that the court does not approve the prosecutor's motion. The situation in which

[26] Art. 3 of the Act of February 4, 2011 amending the Act - Code of Criminal Procedure and certain other acts (Journal of Laws of 2011, No. 53, item 273) introducing to Art. 19 of the Police Act after sec. 15 additional paragraph 15a - 15e.

[27] Art. 2 of the Act of February 4, 2011 amending the Act - Code of Criminal Procedure and certain other acts (Journal of Laws of 2011, No. 53, item 273), amending Art. 10e of the Public Prosecutor's Office Act (Journal of Laws of 2008, No. 7, item 39, as amended).

[28] Art. 237 § 1 of the Act of June 6, 1997 Code of Criminal Procedure (Journal of Laws of 1997, No. 89, item 555).

[29] Art. 3 of the Act of February 4, 2011 amending the Act - Code of Criminal Procedure and certain other acts (Journal of Laws of 2011, No. 53, item 273), amending Art. 237 § 2 of the Act of June 6, 1997. Code of Criminal Procedure (Journal of Laws of 1997, No. 89, item 555).

the wiretapping is established on the basis of a prosecutor's decision without the participation of a court is permissible only in urgent circumstances requiring urgent measures to preserve evidence in a situation where there is a serious fear of losing valuable information. The five-day time limit for the approval of the prosecutor's decision by the court is neither a strict nor a limiting period. The Supreme Court in its judgment of 3 December 2008 considered that „the approval by the court of the prosecutor's decision referred to in art. 237 § 2 of the Code of Criminal Procedure, but with failure to meet the deadline specified in this provision for a decision on such approval, it does not make the control itself and the recording of conversations beyond the deadline is illegal and does not have the effects specified in art. 238 § 3 of the Code of Criminal Procedure in fine, which refer only to the court's decision not to approve the prior decision of the prosecutor on such control by the court"[30]. The amendment to the provisions complied with the earlier interpretation of the Supreme Court, finally dispelling doubts related to the destruction of the collected operational materials.

The wiretap installation is allowed only in relation to the suspect in a criminal trial, to the accused, as well as to the aggrieved party or another person, but only to the person with whom the accused will most likely be in contact or who may be related to the perpetrator or the threatened crime[31]. The legislator allowed for the possibility of using control and recording of telephone conversations only when the pending criminal proceedings (or a justified fear of committing a new crime) concern the most serious crimes known in the Polish criminal system. The catalog of these prohibited acts has been enumerated in art. 237 § 3 of the Code of Criminal Procedure. Due to the fact that the provision „contains a closed catalog of acts in connection with the explanation of which telephone tapping may be ordered, it will not be possible to use it in trivial cases by initiating parallel, fictitious proceedings for one of the crimes listed. However, the information obtained in this way is still a source of operational knowledge and may constitute a premise for undertaking other types of explanatory activities"[32]. Telephone wiretapping may be used for a maximum period of 3 months, with a possible extension for a further 3 months in particularly justified cases. The Act of February 4, 2011, amending the provisions of the Code of Criminal Procedure, supplemented art. 238 of the Code of Criminal Procedure on the obligation to order the destruction of the recorded entries in the part in which they are irrelevant to criminal proceedings.

Data retention

The right to access information from billing is a result and derivative of the obligation imposed on the Polish legislator by so-called the 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

[30] High Court sentence V KK 195/08 (OSNKW 2009 No. 2, item 17).

[31] See art. 237 § 4 of the Act of June 6, 1997 Code of Criminal Procedure (Journal of Laws of 1997, No. 89, item 555).

[32] *Data retention: concern for safety or surveillance of citizens*, Report of the Human Rights Commission at the Supreme Bar Council, http://archiwum.adwokatura.pl/?p=3566, (access: 22/12/2020). http://adwokatura.pl/?p=3566, (access: 22/12/2020), pp. 54-55.

services or public communications networks and amending Directive 2002/58/EC[33]). The directive was adopted under pressure from international events (terrorist attacks in Madrid and London, and attacks on the WTC and the Pentagon). The purpose of the directive was to impose common standards in the Member States but data retention today has gone a long way, from the quick adoption of the directive to its repeal by the judgment of the European Court of Human Rights. To understand its essence, one needs to look at the original version of the directive. At the same time, it should be noted that in Poland, the provisions introduced by the Retention Directive - with a few exceptions - remained unchanged.

The European legislator stated at that time that there was a need (by requiring Member States to do so) to obtain at least the following information on EU citizens: (a) data necessary to establish the source of the connection; (b) data necessary to determine the recipient of the call; (c) data necessary to determine the date, time and duration of the connection; (d) data necessary to determine the type of connection; (e) data necessary to identify a communication tool or what can be used as a communication tool; (f) data necessary to identify the location of the mobile communication device. The legal nature of the directive forced national legislators to implement the provisions of this legal act in such a way as to achieve the desired goals, and effects postulated in the directive.

In Poland, the Act on the Internal Security Agency and the Foreign Intelligence Agency in art. 28 excludes the obligation to obtain the consent of the court to obtain the data referred to in art. 180c and 180d of the Act of 16 July 2004 - Telecommunications Law, i.e. identifying the entity using postal services and regarding the circumstances of providing postal services or using these services. These are not only the so-called billings, „but also all information necessary to determine who, where, when, with whom and how he or she tried to call. This is how the telephone number, connection time, relay station, within which both the callers and the recipients were present, which allows to determine the location of the person at the time of making the call"[34]. The operator of a public telecommunication network and a provider of publicly available telecommunications services are obliged at their own expense:

1. retain and store for a period of 24 months data generated in the telecommunication network or processed by them in the territory of the Republic of Poland, for the duration from the date of connection or unsuccessful connection attempt, to the expiry of this period (then destroy these data, except for those that have been secured in accordance with separate regulations);
2. provide data to authorized entities, as well as to the court and the public prosecutor, on the terms and in the manner specified in separate provisions;
3. protect data against accidental or unlawful destruction, loss or alteration, unauthorized or unlawful storage, processing[35].

[33] Official Journal UE L 105 of 13.4.2006.

[34] *Data retention: concern for safety or surveillance of citizens*, Report of the Human Rights Commission at the Supreme Bar Council, http://archiwum.adwokatura.pl/?p=3566, (access: 22/12/2020), pp. 4.

[35] Art. 180a of the Act of July 16, 2004 Telecommunications Law (Journal of Laws of 2004, No. 171, item 1800).

The obligation to retain, share and protect information covers the data necessary for: (a) determining the network termination, telecommunication terminal device, end user initiating the connection and the one to whom the connection is directed; (b) specifying the date, time of connection, duration, type of connection and location of the telecommunication terminal device. As regards authorized services, courts and the prosecutor's office, the exclusion of telecommunication secrecy and end-user data protection has been applied. Art. 180d of the Telecommunications Act implies easy access of these entities to such data as:

- user data;
- transmission data, which includes data processed for the purpose of transmitting messages on telecommunication networks or billing for telecommunication services, including location data, which means any data processed in a telecommunication network indicating the geographic location of the end device of a user;
- location data, which means location data that goes beyond what is necessary for the transmission of a message or for billing;
- data on attempts to establish a connection between network ends, including data on unsuccessful connection attempts, denoting connections between telecommunication end devices or network termination points that have been set up and have not been received by the end user or the connections set up that have been interrupted[36].

The area and scope of information that ultimately reaches the desk of the applicant officers include the following data of natural persons who are users: surname and first name, parents' names, place and date of birth, address of the place of permanent residence registration, PESEL registration number - in the case of a citizen of the Republic of Poland, the name, series and number of documents confirming identity, and in the case of a foreigner who is not a citizen of a Member State or the Swiss Confederation - the number of the passport or residence card. Officers also have information contained in documents confirming the possibility of performing an obligation towards a provider of publicly available telecommunication services, resulting from a contract for providing of telecommunication services, and other data processed by the operator. In particular, it concerns the tax identification number NIP, bank account number or payment card number, the user's correspondence address, if different from the address of the user's permanent residence address, as well as e-mail address and contact telephone numbers[37]. Finally, officers have access to the list of user subscribers or network termination points that the operator is obliged to keep, which includes the data obtained when concluding the contract[38].

[36] Art. 159 sec. 1 point 1 and points 3-5 of the Act of July 16, 2004 Telecommunications Law (Journal of Laws of 2004, No. 171, item 1800).
[37] Art. 161 of the Act of July 16, 2004 Telecommunications Law (Journal of Laws of 2004, No. 171, item 1800).
[38] Art. 179 sec. 9 of the Act of July 16, 2004 Telecommunications Law (Journal of Laws of 2004, No. 171, item 1800).

It should be noted that the Polish legislator performed the implementation of directive conscientiously exceedingly. In the report of the Polish Supreme Bar Council on data retention, it was emphasized that controlling and recording conversations „for obvious reasons, in the vast majority of cases happens without the knowledge and consent of the intercepted persons. Therefore, despite prior judicial review of the application of this operational measure, they cannot influence the decision to apply it or present their arguments. For this reason, the control and recording of telephone conversations must be subject to specific restrictions in the course of criminal proceedings. (...) There are frequent voices in the doctrine that the existing means of supervision over law enforcement agencies in this respect are insufficient"[39]. Statistics published in connection with the evaluation of the so-called the Retention Directive exposed prevailing practice. Public control of the billings based on data retention a few years after the introduction of the regulations was introduced as much as 1.3 million times, which places Poland at the top of this ranking. The press reported in an alarming tone at the beginning of 2011, giving these figures. „Poland is the EU leader in reaching out to the services, the police and the judiciary for our data from telephone operators. (...) Annually, without any control and restrictions, 1 million 60 thousand billing records, subscriber data and mobile phone owner movement (BTS) data were downloaded times. This means 27.5 checks per thousand adult Poles. The Czech Republic, second in the ranking, had 10 checks per thousand. Great Britain and France – approx. 8.5, Germany – 0.2 per thousand inhabitants (35 times less than in Poland)"[40]. Various European services generated approx. 2.5 million inquiries (of which 1.4 million in Poland), thanks to which they obtained information that was detailed enough and intrudes on citizens' closest privacy, to be able to create a psychological portrait of each of them. Summing up, it can be assumed that from 2008 to 2011 about 10 million inquiries were submitted. Each inquiry probably concerned a matter that covered at least a few people. Assuming randomly that on the basis of one query it is possible to create an economic and psychological picture of at least three people, this gives about 30 million citizens. It should be noted that there are inquiries thanks to which the officers obtained detailed information not about three, but about several dozen people.

There is a loophole in Polish law, which allows to bypass the strict regulations on the use of wiretaps in an investigation[41]. The law enforcement services, instead of submitting a motivated request to the courts for permission to install wiretapping, turn to mobile operators for telecommunication data, which contain a whole range of private information, from which it is often possible to learn more than through wiretapping. It takes such a long period and are suggestive enough to be able to create a psychological and economic portrait of a given person, which would

[39] *Data retention: concern for safety or surveillance of citizens*, Report of the Human Rights Commission at the Supreme Bar Council, http://archiwum.adwokatura.pl/?p=3566, (access: 22/12/2020), pp. 54.

[40] The prosecutor's office, courts and the police in total accounted for 56% of checks, the Border Guard (15% of all checks), the Internal Security Agency (13% of all checks), the Military Counterintelligence Service (11%), Central Anticorruption Bureau (4%) and tax intelligence (1%). See Nisztor, P., Polacy pod kontrolą służb, „*Rzeczpospolita*", no. 116 (8932), pp. 1.

[41] See Rogala-Lewicki A., Usytuowanie funkcjonalne służb specjalnych w systemie politycznym państwa na przykładzie Polski, „*Studium Europy Środkowej i Wschodniej*" 2016, no. 5.

be difficult with the use of wiretapping, which is inherently limited in time, object and person. The problem is that while normally the law enforcement services should obtain the consent of the court to use wiretapping, here they have access to the billing at their own discretion"[42]. Polish Ombudsman was often interested in irregularities in this area[43]. The record year was 2014, when the services downloaded the data of Poles 2.35 million times. In recent years, however, instead of a decline, one deals with a renewed increase in telecommunication data downloads. „According to the latest report of the Minister of Justice for the Senate, the services collected 1.15 million such data in 2016. In 2017, already 1.23 million. A year ago, as much as 1.356 million. Most of them, almost three quarters, went to the police (over 970 thousand data)"[44].

However, cases of abuse are not Polish specialty. Most of the European Union countries introduced provisions into their legal order which went far beyond the objectives the Retention Directive was to achieve. The Commission sees the need to develop more stringent standards harmonizing the situation in this respect. Member States were to ensure that access to these data was granted only to those authorities which, firstly, had the power to use them only for investigative and security purposes, and secondly, to provide them with adequate protection. All member states have provided access to retention data to police services (except for common law systems, i.e. in Ireland and Great Britain) and prosecutors. Interestingly, only fourteen countries have admitted special and military services to this information source. Six countries have included tax intelligence and three have included border guards. As regards the aspect of prior authorization for access to retention data, national legal systems also diverge significantly. „One Member State has envisaged access for public bodies equipped with this option under implementing regulations. In eleven countries, access is subject to prior approval by judicial authorities. In three cases it is a court consent, in the remaining cases - a superior authority. In two states, state authorities have access to such a privilege only upon written request"[45].

[42] Siedlecka E., KE: Za dużo podglądacie, http://wyborcza.pl/1,75478,9453157,KE__Za_duzo_podgladacie.html, (access: 15.12.2020); Siedlecka E., Służby zdradzają, jak często sięgały po bilingi, „*Gazeta Wyborcza*", 10.02.2011,http://wyborcza.pl/1,75478,9081579,Sluzby_zdradzaja__jak_czesto_siegaly_po_billingi.html#ixzz1TgKmikgS, (access: 15.12.2020); Siedlecka E., Kogo można podsłuchać, „*Gazeta Wyborcza*", 15.03.2011.

[43] In his letter to the Prime Minister of April 1, 2008 (RPO-578577-II/08/PS) Polish Ombudsman emphasized the issue of conducting operational activity by authorized bodies, including in particular, secret services - understood as classified activity consisting in: controlling the content of correspondence and the content of postal items, obtaining and recording the content of telephone calls and other information transmitted via telecommunication networks, results from the ease of exceeding the limits of state interference in the sphere of rights by public authorities and civil liberties. On January 17, 2011, Ombudsman addressed an open letter to the Prime Minister, in which he presented his position. According to the legal analysis conducted in his Office, the methods of obtaining information covered by the confidentiality are inconsistent with the Polish Constitution and the European Convention for the Protection of Human Rights and Fundamental Freedoms. The Ombudsman alleged that there is no external control over the downloading of data; there are no restrictions on the purpose of data collection; there is no protection of people using secrecy for professional purposes (journalists or lawyers); there is no obligation to destroy data that is not useful for detecting crimes; there is no requirement that telecommunication data can be downloaded, only if other means of reaching the evidence have failed (this is the case of wiretaps). See *Ustawa ograniczy podsłuchy i bilingi*, http://wiadomosci.onet.pl/kraj/ustawa-ograniczy-podsluchy-ibilingi,1,4012797,wiadomosc.html, (access: 20.12.2020).

[44] *Służby masowo inwigiluje. Pobierają dane od operatorów*, https://wyborcza.pl/7,156282,25225521,sluzby-masowo-inwigiluja-pobieraja--dane-od-operatorow.html, (access: 17.12.2020).

[45] *Report from the Commission to the Council and the European Parliament – Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)*, 3 COM(2011) 225 final, Brussels, 18.4.2011, p. 9.

Table 1. Access to retention data in Europe

Access to retention data in Europe		
	Relevant state agenicies	Procedures and conditions
Belgium	Courts, Police, Prosecutors Office	Prosecutor consent
Bulgaria	Law enforcement authorities Internal Affairs Ministry, Defence Ministry, Military Services, Police, Prosecutors Office, Courts	Court consent
Czech Republic	Non implemented	
Denmark	Police	Court consent
Germany	Non implemented	
Estonia	Police, Border Guards, Fiscal and Customs Agencies	Court consent
Ireland	Police, Military Services, Border Guards, Fiscal and Customs Agencies	Letter notion
Greece	Police, Courts, Prosecutors Office, Military Services	Court consent
Spain	Police, Border Guards, Fiscal and Customs Agencies, Intelligence	Court consent
France	Police, Courts, Prosecutors Office, Gendarmerie	Supervision office consent
Italy	Police, Courts, Prosecutors Office, Military Services	Prosecutor consent
Cyprus	Police, Courts, Prosecutors Office	Prosecutor consent, in some cases Court consent
Latvia	Police, Courts, Prosecutors Office, Law enforcement authorities,	Prosecutor consent, in some cases Court consent
Lithuania	Police, Courts, Prosecutors Office, Intelligence	Letter notion, in some cases Court consent
Luxembourg	Law enforcement authorities, Police, Courts, Prosecutors Office, Military Offices	Court consent
Hungry	Courts, Police, Law enforcement authorities, Intelligence, Prosecutors Office, Border Guards, Fiscal and Customs Agencies	Prosecutor consent, in some cases Court consent
Malta	Police, Law enforcement authorities	Letter notion
Holland	Prosecutors Office, Police	Prosecutor consent, in some cases Court consent
Austria	Non implemented	
Poland	Courts, Police, Prosecutors Office, Border Guards, Fiscal and Customs Agencies, Intelligence	Letter notion
Portugal	Courts, Police, Prosecutors Office, Border Guards, Military Services, Immigration Office, Maritime Services	Court consent
Romania	Non implemented	
Slovenia	Prosecutors Office, Police, Intelligence	Court consent
Slovakia	Courts, Law enforcement authorities	Letter notion
Finland	Courts, Police, Prosecutors Office, Border Guards, Fiscal and Customs Agencies, Maritime Services	Letter notion, in some cases Court consent
Sweden	Non implemented	
United Kingdom	Police, Prosecutors Office, Law enforcement authorities, Fiscal and Customs Agencies, Intelligence	Relevant procedures with proportionality test

Source: *Report from the Commission to the Council and the European Parliament – Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)*, 3 COM(2011) 225 final, Brussels 18.4.2011, p. 10-12.

In several EU countries, the provisions of the directive have been questioned as being in violation of the universal right to privacy. The Constitutional Court in Romania (October 8, 2009), the Federal Constitutional Court in Germany (March 2, 2010), the Constitutional Court

of the Czech Republic (March 31, 2011) unanimously declared the provisions implementing the Directive are unconstitutional.

In response to the avalanche of protests, the European Commission has decided to publish an evaluation report on the functioning of the directive and its effects. The report was released on April 18, 2011. At the very beginning, it is emphasized that data retention has become an extremely important tool for ensuring security in the European Union zone. The authors of the report point out the dangers of misusing information obtained on data retention. The directive was designed to facilitate the prosecution, and investigation of serious crime cases. Meanwhile, some national legislators, as emphasized in the report, used the circumstances related to the implementation of the EU act to increase the detection of all types of abuses. The differences between individual countries are visible. „Ten member states (Bulgaria, Estonia, Ireland, Greece, Spain, Lithuania, Luxembourg, Hungary, the Netherlands, Finland) have defined the possibility of using data retention only for the so-called categories of serious crime, enumerated. Eight member states (Belgium, Denmark, France, Italy, Latvia, Poland, Slovakia, Slovenia) for all crimes. The construction of the legal norms in four countries (Cyprus, Malta, Portugal, Great Britain) assigned data retention to the category of serious crimes, but without enumerating their types"[46].

The provisions of the directive were also strongly criticized by the non-governmental sector by publishing the so-called „Shadow report" to the Commission's report. The authors of the Digital Civil Rights in Europe foundation, which currently brings together 28 different organizations, indicated that „European citizens paid a very high price for the implementation of the directive. It is about not only limiting the right to privacy, but also chaos and lawlessness in the processing of personal data. Europe's hard-won credibility as a defender of fundamental rights has also suffered. The Commission's report and our shadow report show that the directive has been a failure at all levels: the fundamental rights of Europeans have been jeopardized, it has not been possible to harmonize data retention rules for the internal market, and these losses were not necessary in the fight against crime"[47].

The European Data Protection Supervisor also criticized the data retention formula. In his opinion, data retention is „the most invasive instrument ever adopted by the European Union". On May 31, 2011, EIDO gave its opinion[48], in which it indicates that the Retention Directive

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

[47] In the report of the Commission, one can find a general remark that the mechanism has become an extremely valuable weapon against crime prevention, detection and combat. Member States have generally reported that data retention has become a valuable, and in some cases irreplaceable, tool for crime detection and prevention and victim protection. The general wording referring to the general usefulness of data retention cannot be satisfactory in the face of actual, physical interference in the sphere of constitutionally protected privacy. *Nic nie zyskaliśmy, a straciliśmy prywatność – Komisja Europejska ocenia dyrektywę o retencji danych, my oceniamy Komisję…i sytuację w Polsce*, http://panoptykon.org/wiadomosc/nic-nie-zyskalismy-stracilismy-prywatnosc-komisja-europejska-ocenia-dyrektywe-o-retencji-d, (access: 21.12.2020).

[48] Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), European Data Protection Supervisor, EDPS/11/6, Brussels, 31.05.2011.

does not meet minimum standards with regard to the right to privacy and personal data protection. „EIDO emphasized that it had repeatedly indicated that it did not see the need to keep data to such a wide extent in the light of the guarantee the right to privacy and personal data protection. EIDO recalled the need to justify whether the retention is necessary and proportionate. After analyzing the Commission's report on the retention directive of 18 April 2011, EIDO concluded that the directive breached the guarantees of personal data protection and privacy for these reasons: (1) keeping the data retention obligation was not sufficiently justified, (2) data could be regulated in a much less interfering manner with the right to privacy, (3) the directive leaves too much discretion to the Member States as regards data processing, as well as determining who and to what extent should be able to access the data"[49].

The final blow to the Retention Directive was the judgment of the European Court of Human Rights of April 8, 2014, which stated that the directive on the retention of telecommunication data is invalid and the provisions that obligated member states to impose an obligation on telecommunication operators to store telecommunication data disproportionately interfere with privacy Europeans. This decision was fundamental to the protection of privacy in Europe[50].

Tightening the screw

The turning point in the scope of burdening the freedom of obtaining information by the public agencies (on the basis of increasing security) at the expense of privacy protection was undoubtedly the terrorist attacks on the World Trade Center of September 11, 2001 and the subsequent events that justified relevant legislative. The trend is visible all over the world. Unfortunately, at some point it took on a caricature. In Poland, the 8-year coalition rule until 2015 was characterized by numerous violations of the right to privacy. On the other hand, the new political team that took over the reins of governments after 2015, instead of strengthening the supervision of the system of covert obtaining data on citizens, shifted the focus even more towards surveillance[51].

[49] *Europejski Inspektor Danych Osobowych o dyrektywie retencyjnej*, http://www.europapraw.org/news/europejski-inspektor-danych-osobowych-o-dyrektywie-retencyjnej, (access: 07.12.2020).

[50] The European Court of Human Rights has also previously adjudicated in cases involving violations of privacy. The ECtHR on the basis of art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms signed in Rome on November 4, 1950, later amended by Protocols No. 3, 5 and 8 and supplemented by Protocol No. 2, stated that, by its very nature, billing must be distinguished from wiretapping, which is an undesirable phenomenon and unlawful in a democratic society, unless there are good reasons for it. But the use of billing data may, under certain circumstances, constitute a breach of art. 8 of the Convention. Billing data includes information about dialed numbers, which are an integral component of telephone communication. As a result, the disclosure of this information to the police, without the consent of the subscriber, also constitutes an interference with the rights guaranteed under art. 8 (ECtHR judgment of 2 August 1984 in the case of Malone v. Great Britain, application no. 8691/79). In turn, in the judgment of 30 July 1998, the European Court of Human Rights stated that "the control of the telephone line is an interference by public authorities in the exercise of the right to respect for private life and correspondence. It does not matter that only the system was used to record calls from a specific telephone. Therefore, in such a case, as in the case of wiretapping, the provisions should contain safeguards to avoid any abuse of power (Valenzuela Contreras v. Spain, no. 27671/95).

[51] See Rogala-Lewicki A., Security services after the terrorist attacks in the US and Europe. Patriot Act versus the Retention Directive, or the legitimization of abuses in the sphere of privacy in democratic states: a comparative study, "*Myśl Ekonomiczna i Polityczna*" 2015, no. 3 (50).

The changes took place quite fast in two steps: with the „surveillance act"[52] and with the „anti-terrorist act"[53]. In the first case, the Sejm adopted the document on January 15, 2016, the Senate did not amend it on January 29, 2016, President Andrzej Duda signed it on February 3, 2016, and the act entered into force on February 7, 2016. The dates are very important here[54]. The bill was to implement the judgment of the Constitutional Tribunal of July 2014, in which the Constitutional Tribunal questioned the provisions on surveillance based on operational control and billings. Interestingly, the law prepared by PiS referred directly to the criticized version of the original content of the amendment, prepared by MPs from the PO-PSL[55]. The difference was the use of an ideal opportunity to introduce a creative development consisting in smuggling under the cover of the implementation of the Constitutional Tribunal's judgment (in theory) the right for law enforcement services to obtain data from Internet operators without the consent of the court. The amendment *de facto* concerned several acts regulating the activities of the Police, Border Guard, Military Gendarmerie, Internal Security Agency, Foreign Intelligence Agency, Counterintelligence Service, as well as the Military Intelligence, Central Anticorruption Bureau, Customs Service and fiscal control[56].

The new provisions - in accordance with the judgment of the Constitutional Tribunal - were to ensure greater control over the collection of data by the Police and other services. Apart from one new control mechanism exercised by the district court in the form of checking (once every six months) the service report on the type of data collected[57], the adopted „surveillance" law introduced a number of controversial solutions to facilitate the use of postal, telecommunications and internet data by the services[58].

New legislation enabled to conclude agreements with companies providing electronic services on remote data transfer. Law enforcement services requests data to operators and Internet companies in writing „for the purposes of conducted proceedings" - and they received them this way. The amendment introduced online access to this data - through the so-called secure

[52] Act of 15 January 2016 amending the Act on the Police and certain others (Journal of Laws of 2016, item 147).

[53] Act of 10 June 2016 on anti-terrorist activities (Journal of Laws of 2016, item 904).

[54] If the amendment had not entered into force on February 7, the services would have had no basis for many actions. On February 6, the judgment of the Constitutional Tribunal of July 2014 entered into force. Tribunal then ruled that: part of the legal grounds for operational control are unconstitutional; lack of independent control of telecommunications data downloading by services; no rules for destroying wiretaps of persons of public trust (e.g. lawyers or journalists); no obligation to destroy the collected useless data by the ABW, CBA and SKW.

[55] The project was fundamentally criticized by the prosecutor general, the General Inspector of Personal Data Protection, the Government Legislation Center, the Bar Association and foundations: Helsinki and Panoptykon.

[56] The amendment was questioned by: the entire opposition, the Ombudsman Adam Bodnar (he announced that he would appeal it to the Constitutional Tribunal), GIODO, the National Council of the Judiciary, the Digitization Council, the Supreme Bar Council, the National Council of Legal Advisers and non-governmental organizations. See Nyzio A., Wokół „ustawy inwigilacyjnej": geneza, przepisy i konsekwencje Ustawy z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw, *„Jagielloński Przegląd Bezpieczeństwa*" 2017, no. 1.

[57] Supervision is *de facto* apparent control. Many courts limit their checks to looking at this list, without checking what is behind the numbers.

[58] Telephone data include billings, locations in the base station where phone logs in (this allows to specify where and when one has been), information about the type of phone. Postal data include address, places of sending parcels, their collection, postal services that was used. Internet data includes Internet connection reports, IP address, personal information (including e-mail addresses, popular „check-ins" and much more).

internet connection. Moreover, the services obtained the right to obtain information not only for the purposes of proceedings, but also for the purpose of „preventing or detecting crimes", „saving human life or health or supporting search activities" or „carrying out statutory tasks". Paradoxically, the act gave the services a wider field to hide how often and for what purpose they use telecommunications data. For example, data on how often the agencies reach for subscriber data - e.g. to whom a given telephone number belongs, were excluded from the report. The most dangerous novelty was ignoring constitutional doubts as to the collection of geolocation and internet data without the necessary court approval, and omitting the obligation to inform the citizen about such activities, and finally ignoring the principles of proportionality and necessity rule through the possibility of eavesdropping on citizens even when other methods of collecting information have not been exhausted[59].

Following the „surveillance act", in June 2016, the so-called the „anti-terrorism" law tightened the collar. The act granted a number of new powers to the Internal Security Agency. The head of the Agency obtained powers - without the need to ask for the consent of the court or any other authority - in the field of access to telecommunication and internet data of foreigners, in particular to decide on wiretapping, installing a hidden camera or reading e-mails. The Internal Security Agency has been given easy access by public recorders - by means of transmission, it has access to images and recordings from cameras located in public facilities and in all other public places. What's more, the Police, Border Guard and Internal Security Agency are able to take a fingerprint image, record the image of a face, and even biological material (DNA), including where there is doubt as to the identity. The only condition is that these activities concern a foreigner. As one can guess, the justification for specific actions theoretically concerning a foreigner is access to the domain, in which you can „see" others[60].

In 2020, the public opinion was raised by the Entrepreneurship Council gathering the largest Polish employer organizations (Confederation Lewiatan, ABSL, Federation of Polish Entrepreneurs, KIG, Polish Business Council, Employers of Poland, Polish Bank Association, BCC and Polish Craft Association), which revealed that Ministry of Justice is finalizing the project of preventive confiscation. The planned *in rem* confiscation provisions will allow prosecutors to seize taxpayers' property without a final judgment, breaking the fundamental principle of the presumption of innocence[61]. The Ministry of Justice wants to provide law enforcement agencies with easy access to the information about citizens. To make this happen, the catalog of law enforcement services' competences in this field is planned to be expanded[62].

[59] *Jak działa ustawa inwigilacyjna*, https://panoptykon.org/wiadomosc/jak-dziala-ustawa-inwigilacyjna, (access: 17.12.2020).

[60] *Ustawa inwigilacyjna i antyterrorystyczna. Sprawdzamy jak działają*, https://panoptykon.org/wiadomosc/ustawa-inwigilacyjna-i-antyterrorystyczna-sprawdzamy-jak-dzilaja, (access: 17.12.2020).

[61] *Konfiskata prewencyjna czyli udowodnij, że nie jesteś wielbłądem*, https://www.enodo.pl/aktualnosci/konfiskata-prewencyjna-czyli-udowodnij-ze-nie-jestes-wielbladem, (access: 17.12.2020).

[62] *Konfiskata prewencyjna od 2021r.*, https://ksiegowosc.infor.pl/obrot-gospodarczy/dzialalnosc-gospodarcza/4669997,Konfiskata-prewencyjna-od-2021-r.html, (access: 17.12.2020).

The state sector cynical approach was daylighted within the act of smuggling of expanding competence instruments of the secret services in the area of security inside „anticovid acts", which nominally were aimed at providing support to entrepreneurs, while in the normative recesses one could find surveillance provisions[63].

As if that were not enough, the Supreme Audit Office has published a report[64], which shows that since autumn 2017, the Central Anticorruption Bureau is in possession of a Pegasus system license, which is massive surveillance system based on a „helicopter" overview of telecommunications and internet data. The Pegasus system is a specialized spy program, produced by the Israeli company NSO Group, which is used to track specific users in detail. Pegasus works like malware - after installing spyware, it breaks the application's security and accesses private information through them. One can use it to break into Android and iOS phones and download all the data stored on them (SMS, correspondence from messengers, e-mails, passwords, audio recordings and information from installed applications, such as Facebook, Gmail, WhatsApp or Instagram). Pegasus allows to intercept calls, but also start and record video using cameras installed in smartphones. The field for abuses in the area of protection of citizens' privacy becomes endless, because the program allows unlimited control of the activity of the smartphone owner, and it has been designed in such a way that it does not leave any traces (it also has the ability to self-eliminate)[65].

The principles of surveillance of people by secret services in Poland are currently being assessed by the European Court of Human Rights, that undertakes checks of the feasibility of independent control over the activities of law enforcement and secret services that can exercise their extensive powers without real restrictions and supervision. This is the result of complaints from 2017 and 2018 by the lawyers: Dominika Bychawska-Siniarska and others against Poland and Mikołaj Pietrzak against Poland, as well as activists from the Panoptykon Foundation and the Helsinki Foundation for Human Rights. The applicants allege that the actions of the public agencies violated privacy (Article 8 of the Convention for the Protection of Human Rights) and the right to an effective remedy (Article 13 of the Convention)[66]. The Commissioner for Civil Rights Protection presented the Tribunal with postulates, including: (a) the establishment of a special, independent body which would supervise the activities of

[63] See act of March 2, 2020 on special solutions related to the prevention, counteraction and combating of COVID-19, other infectious diseases and crisis situations caused by them (Journal of Laws of 2020, item 374).

[64] NIK auditors and researchers from the Canadian laboratory The Citizen Lab have found footsteps. They discovered a strange transfer of money to the CBA from the Justice Fund dedicated to helping crime victims. Puzzling, as it amounts to as much as PLN 25 million. The inspectors also dug up the invoice issued by the CBA for nearly PLN 35 million for the purchase of specialist technology for detecting and preventing crime. In turn, Citizen Lab experts found Pegasus by analyzing traffic on the Polish Internet.

[65] Reczkowski G., *Pegasus to więcej niż inwigilacja*, https://www.polityka.pl/tygodnikpolityka/kraj/1924036,1,pegasus-to-wiecej-niz-inwigilacja.read, (access: 17.12.2020).

[66] Ombudsman Adam Bodnar withdrew the complaint from the Constitutional Tribunal in which he questioned the rules of surveillance amended in 2016. The notion was to be assessed in the Tribunal by judges whose judicial status may be questioned. The Ombudsman fears that in such a situation the judgment of the Tribunal could freeze the legal status, which is inconsistent with constitutional and European standards. In this context, the ruling of the ECtHR on two complaints from Poland will be important. Therefore, the Commissioner for Human Rights presented to the ECtHR an „amicus curiae" opinion, in which he referred in detail. See *Inwigilacja i uprawnienia polskich służb specjalnych w ETPC. Rzecznik przedstawia swą opinię*, https://www.rpo.gov.pl/pl/content/etpc-zbada-uprawnienia-polskich-sluzb-specjalnych-opinia-rpo, (access: 17.12.2020).

secret services and could hear individual complaints about the activities of the services; (b) granting the individual the right to be informed of the interest of the services and the right to access personal data processed[67].

Conclusions

The new information conditions, the control over the flow of information that slips out of the hands of the state, forces the search for new solutions. Although capturing the actual amount of information collected by law enforcement authorities is extremely difficult, through the disclosed statistics (for example in the data retention space), or the fact that there is widespread legal privacy interference, appropriate conclusions can be made[68]. Paradoxically, although state activity is necessarily becoming more transparent, at the same time, analyzing the state's approach to obtaining information, one can find confirmation of the assessment that states, regardless of their historical period, level of economic development or political system, show a natural tendency to appropriate and expand own zones and information competences.

References

Literature

1. Bielak F., *Służby wywiadowcze Republiki Federalnej Niemiec*, Warszawa 1985.
2. *Decydowanie publiczne*, Rydlewski G. (eds.), Warszawa 2011.
3. *Encyklopedia szpiegostwa*, SPAR, Warszawa 1995.
4. Faligot R., Kauffer R., *Służby specjalne*, Warszawa 1998.
5. Galicki Z., *Status prawny służb specjalnych w wybranych państwach zachodnich*, Warszawa 1996.
6. Hatch M. J., *Teoria organizacji*, Warszawa 2002.
7. Herman M., *Potęga wywiadu*, Warszawa 2002.
8. Karpiński M., *Historia szpiegostwa*, Warszawa 2003.
9. Kessler W., *CIA od środka*, Warszawa 1994.
10. Koch E. R., Sperber J., *Infomafia*, Gdynia 1999.
11. Martinet B., Marti Y. M., *Wywiad gospodarczy. Pozyskiwanie i ochrona informacji*, Warszawa 1999.
12. Misiuk A., *Służby specjalne II Rzeczypospolitej*, Warszawa 1998.
13. *Parlamentarny nadzór nad sektorem bezpieczeństwa. Zasady, mechanizmy i praktyki*, Unia Międzyparlamentarna i Genewskie Centrum Demokratycznej Kontroli nad Siłami Zbrojnymi, Warszawa 2004.
14. Pepłoński A., *Kontrwywiad II Rzeczypospolitej*, Warszawa 2002.
15. Pepłoński A., *Wywiad a dyplomacja II Rzeczypospolitej*, Toruń 2004.

[67] *Inwigilacja i uprawnienia polskich służb specjalnych w ETPC. Rzecznik przedstawia swą opinię*, https://www.rpo.gov.pl/pl/content/etpc-zbada-uprawnienia-polskich-sluzb-specjalnych-opinia-rpo, (access: 17.12.2020).

[68] See Rogala-Lewicki A., European Intelligence Community – the unfulfilled pillar of the European Union, "*Myśl Ekonomiczna i Polityczna*" 2016, no. 3 (54).

16. Piekałkiewicz J., *Dzieje szpiegostwa*, Warszawa 1999.
17. Rogala-Lewicki A., *Informacja jako autonomiczny czynnik wpływu. Studium władztwa informacyjnego*, Częstochowa 2013.
18. Rydlewski G., *Rządowy system decyzyjny w Polsce*, Warszawa 2002.
19. Schweizer P., *Szpiedzy wśród przyjaciół. Jak sojusznicy wykradają Amerykanom tajemnice technologiczne*, Warszawa 1997.
20. Smaga J., *Narodziny i upadek imperium – ZSRR 1917 – 1991*, Kraków 1992.
21. Suworow W., *Akwarium*, Warszawa 1990.
22. Suworow W., *Specnaz*, Gdańsk 1991.
23. Suworow W., *Lodołamacz*, Warszawa 1992.
24. Toffler A., *Trzecia fala*, Warszawa 1986.
25. De Villemarest P., *GRU – sowiecki super wywiad*, Warszawa 1998.
26. West N., *MI – 5*, Warszawa 1999.
27. West N., *MI – 6, Operacje brytyjskiej Tajnej Służby Wywiadu 1909-1945*, Warszawa 2000.
28. Westerby G., *Na terytorium wroga. Tajemnice Mosadu*, Warszawa 2001.
29. Zalewski S., *Ewolucja modelu polskich służb specjalnych*, Warszawa 2003.
30. Zalewski S., *Służby specjalne – programowanie, nadzór, koordynacja*, Warszawa 2003.
31. Zalewski S., *Funkcja informacyjna służb specjalnych w systemie bezpieczeństwa RP*, Warszawa 2005.
32. Zalewski S., *Służby specjalne w państwie demokratycznym*, Warszawa 2005.
33. Zięba R., *Instytucjonalizacja bezpieczeństwa europejskiego,* Warszawa 1999.
34. Żebrowski A., Żmigrodzki M., Babula J., *Rola służb specjalnych w siłach zbrojnych*, Kraków 1999.
35. Żebrowski A., Kwiatkowski W., *Bezpieczeństwo informacji III Rzeczypospolitej*, Kraków 2000.
36. Żebrowski A., *Kontrola cywilna nad służbami specjalnymi III Rzeczypospolitej (1989- 1999). Zagadnienia politologiczno-prawne*, Kraków 2001.

Articles

1. Bożek M., Współczesny model polskich służb specjalnych. Służby informacyjne czy policyjne?, „*Zeszyty Naukowe Akademii Obrony Narodowej*" 2005, no. 1 (58).
2. Chodak P., Zarządzanie w służbach – nadzór, kontrola i koordynacja realizowana przez Koordynatora Służb Specjalnych, „*Journal of Modern Science*" 2016 vol 2(29).
3. Colby W.E., Intelligence Secrecy and Security in a Free Society, „*International Security*" 1976, vol 1, no. 2.
4. Dufresne R.L. Offstein E.H., On the Virtues of Secrecy in Organizations, „*Journal of Management Inquiry*", 2008, no. 17 (102).
5. Gadzheva M. Privacy in the Age of Transparency, „*Social Science Computer Review*" 2007, No. 26 (60).
6. Galicki Z., Kontrola parlamentarna nad działalnością służb specjalnych (na przykładzie wybranych państw), „*Biuletyn – ekspertyzy i opinie prawne*" 1991, no. 1.

7. Garson G.D., Securing the Virtual State: Recent Developments in Privacy and Security, „*Social Science Computer Review*" 2006, No. 24 (489).
8. Kosmaty P., Granice tajnej inwigilacji obywateli w demokratycznym państwie prawa, „*Prokurator*", 2008, no. 3.
9. Little L. Privacy, Trust, and Identity Issues for Ubiquitous Computing, „*Social Science Computer Review*" 2008, No. 26.
10. Minkina M., Wywiad Sojuszu Północnoatlantyckiego i Unii Europejskiej, „*DOCTRINA Studia społeczno-polityczne*" 2008, no. 5.
11. Nisztor P., Polacy pod kontrolą służb, „Rzeczpospolita", no. 116 (8932).
12. Nyzio A., Wokół „ustawy inwigilacyjnej": geneza, przepisy i konsekwencje Ustawy z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw, „*Jagielloński Przegląd Bezpieczeństwa*", 2017, no. 1.
13. Rogala-Lewicki A., European Intelligence Community – the unfulfilled pillar of the European Union, "*Myśl Ekonomiczna i Polityczna*" 2016, no. 3 (54).
14. Rogala-Lewicki A., Security services after the terrorist attacks in the US and Europe. Patriot Act versus the Retention Directive, or the legitimization of abuses in the sphere of privacy in democratic states: a comparative study, "*Myśl Ekonomiczna i Polityczna*" 2015, no. 3 (50).
15. Rogala-Lewicki A., Struktura organizacyjna służb specjalnych – ilustracja w oparciu o wybrane modele państw i systemy polityczne, "*Studium Europy Środkowej i Wschodniej*" 2016, no. 6.
16. Rogala-Lewicki A., Usytuowanie funkcjonalne służb specjalnych w systemie politycznym państwa na przykładzie Polski, "*Studium Europy Środkowej i Wschodniej*" 2016, no. 5.
17. Rogala-Lewicki A., Participation of intelligence services in political decision-making process – evolution of coordination patterns in Poland, "*Studium Europy Środkowej i Wschodniej*" 2020, no. 13.
18. Siedlecka E., Kogo można podsłuchać, „*Gazeta Wyborcza*", 15.03.2011.
19. Thompson E.P., The secret state, „*Race Class*" 1979, no. 20 (219).
20. Vervaele J.A.E., Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law, "*Utrecht Law Review*" 2005, vol 1, no. 1.
21. Whitehall, Ch.A., Washington and the Intelligence Services, „*International Affairs*" 1977, vol 53, no. 3.
22. Zalewski S., Zadania i uprawnienia służb specjalnych w zakresie ochrony porządku konstytucyjnego RP, „*Zeszyty Naukowe Akademii Obrony Narodowej*" 2004, no. 2 (55).

Legal acts, court rulings, documents, www sources

1. Konwencja o ochronie praw człowieka i podstawowych wolności 4.11.1950 (Journal of Laws 1993 No. 61 item 284).
2. Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych

usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE 15.03.2006 (Journal of Laws EU z L 105,13.4.2006).
3. Konstytucja Rzeczypospolitej Polskiej 2.04.1997 (Journal of Laws 1997 No. 78, item 483).
4. Ustawa o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych 2.03.2020 (Journal of Laws 2020, item 374).
5. Ustawa o działaniach antyterrorystycznych 10.06.2016 (Journal of Laws 2016, item 904).
6. Ustawa o zmianie ustawy o Policji oraz niektórych innych ustaw 15.01.2016 (Journal of Laws 2016, item 147).
7. Ustawa o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw 4.02.2011 (Journal of Laws 2011 No. 53, item 273).
8. Ustawa Prawo telekomunikacyjne 16.07.2004 (Journal of Laws 2004 No. 171, item 1800).
9. Ustawa o Wojskowych Służbach Informacyjnych 9.07.2003 (Journal of Laws 2003 No. 139 item 1326).
10. Ustawa o Agencji Wywiadu i Agencji Bezpieczeństwa Wewnętrznego 24.05.2002 (Journal of Laws 2002 No. 74 item 676 as amended).
11. Ustawa o Urzędzie Ochrony Państwa 6.04.1990 (Journal of Laws 1990 No 30, item 180.
12. Rozporządzenie Prezesa Rady Ministrów 2.07.2002 w sprawie szczegółowego trybu i zasad funkcjonowania Kolegium do Spraw Służb Specjalnych oraz zakresu czynności sekretarza tego Kolegium (Journal of Laws 2002 No. 103, item 929).
13. Rozporządzenie Prezesa Rady Ministrów 18.11.2019 w sprawie szczegółowego zakresu działania Ministra - Członka Rady Ministrów - Koordynatora Służb Specjalnych (Journal of Laws 2019, item 2273).
14. Zarządzenie Prezesa Rady Ministrów 12.09.2003 w sprawie zasad zakresu i trybu współdziałania oraz szczegółowego rozdziału kompetencji pomiędzy Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu i Wojskowe Służby Informacyjne (M.P. 2003 No. 44, item 656).
15. Constitutional Tribunal sentence 20.06.2005, K 4/04 (OTK-A 2005/6/64).
16. Constitutional Tribunal sentence 20.04.2004, K 45/02 (OTK-A 2004/4/30).
17. Constitutional Tribunal sentence 20.11.2002, K 41/02, (OTK ZU 6/A/2002)
18. Constitutional Tribunal sentence 19.02.2002, U 3/01, (OTK ZU 1/A/2002).
19. Constitutional Tribunal sentence 11.04.2000, K 15/98 (OTK ZU 3/2000).
20. Constitutional Tribunal sentence 24.06.1997, K 21/96 (OTK ZU 2/1997).
21. High Court sentence V KK 195/08 (OSNKW 2009/2/17).
22. European Parliament - Temporary Committee on the ECHELON Interception System: Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system), (2001/2098 (INI)), 11.07.2001.
23. *Informacja o wynikach kontroli organizacji służb specjalnych oraz nadzoru nad nimi,* Najwyższa Izba Kontroli, Warszawa 2005.

24. Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), European Data Protection Supervisor, EDPS/11/6, Brussels, 31.05.2011.
25. *Report from the Commission to the Council and the European Parliament – Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)*, 3 COM(2011) 225 final, Brussels 18.4.2011.
26. *Europejski Inspektor Danych Osobowych o dyrektywie retencyjnej*, http://www.europapraw.org/news/europejski-inspektor-danych-osobowych-o-dyrektywie-retencyjnej, (access: 07.12.2020).
27. *Inwigilacja i uprawnienia polskich służb specjalnych w ETPC. Rzecznik przedstawia swą opinię*, https://www.rpo.gov.pl/pl/content/etpc-zbada-uprawnienia-polskich-sluzb-specjalnych-opinia-rpo, (access: 17.12.2020).
28. *Jak działa ustawa inwigilacyjna*, https://panoptykon.org/wiadomosc/jak-dziala-ustawa-inwigilacyjna, (access: 17.12.2020).
29. *Konfiskata prewencyjna czyli udowodnij, że nie jesteś wielbłądem*, https://www.enodo.pl/aktualnosci/konfiskata-prewencyjna-czyli-udowodnij-ze-nie-jestes-wielbladem, (access: 17.12.2020).
30. *Konfiskata prewencyjna od 2021r.*, https://ksiegowosc.infor.pl/obrot-gospodarczy/dzialalnosc-gospodarcza/4669997,Konfiskata-prewencyjna-od-2021-r.html, (access: 17.12.2020).
31. *Koniec z podsłuchiwaniem obywateli*, http://prawo.gazetaprawna.pl/artykuly/534298,koniec_z_podsluchiwaniem_obywateli.html, (access: 22.12.2020).
32. Małecki G., *Bezgłowe służby*, https://www.rp.pl/Publicystyka/305079942-Bezglowe-sluzby.html, (access: 07.07.2020).
33. *Nic nie zyskaliśmy, a straciliśmy prywatność – Komisja Europejska ocenia dyrektywę o retencji danych, my oceniamy Komisję…i sytuację w Polsce*, http://panoptykon.org/wiadomosc/nic-nie-zyskalismy-stracilismy-prywatnosc-komisja-europejska-ocenia-dyrektywe-o-retencji-d, (access: 21.12.2020).
34. *NSA Prism program taps in to user data of Apple, Google and others,* „The Guardian", 7.06.2013, http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data (access: 22.12.2020)
35. Reczkowski G., *Pegasus to więcej niż inwigilacja*, https://www.polityka.pl/tygodnikpolityka/kraj/1924036,1,pegasus-to-wiecej-niz-inwigilacja.read, (access: 17.12.2020).
36. *Reforma służb specjalnych z perspektywy 15 lat*, Fundacja im. Kazimierza Pułaskiego, Warszawa 07.05.2017, https://pulaski.pl/wp-content/uploads/2015/02/Raport_reforma_sluzb__FKP.pdf, (access: 07.07.2020).
37. *Retencja danych: troska o bezpieczeństwo czy inwigilacja obywateli* - Raport Komisji Praw Człowieka przy Naczelnej Radzie Adwokackiej, http://archiwum.adwokatura.pl/?p=3566, (access: 22.12.2020).
38. Siedlecka E., *Służby zdradzają, jak często sięgały po bilingi*, http://wyborcza.pl/1,75478,9081579,Sluzby_zdradzaja__jak_czesto_siegaly_po_billingi.html#ixzz1TgKmikgS, (access: 15.12.2020).
39. Siedlecka E., KE: *Za dużo podglądacie*, http://wyborcza.pl/1,75478,9453157,KE__ Za_duzo_podgladacie.html, (access: 15.12.2020).

40. *Służby masowo inwigilują. Pobierają dane od operatorów*, https://wyborcza.pl/7,156282,25225521,sluzby-masowo-inwigiluja-pobieraja-dane-od-operatorow.html, (access: 17.12.2020).
41. *Ustawa inwigilacyjna i antyterrorystyczna. Sprawdzamy jak działają*, https://panoptykon.org/wiadomosc/ustawa-inwigilacyjna-i-antyterrorystyczna-sprawdzamy-jak-dzialaja, (access: 17.12.2020).
42. *Ustawa ograniczy podsłuchy i bilingi*, http://wiadomosci.onet.pl/kraj/ustawa-ograniczy-podsluchy-ibilingi,1,4012797,wiadomosc.html, (access: 20.12.2020).