ACTA IURIDICA RESOVIENSIA Nr 2(45)/2024
ISSN 2720-0574 DOI: 10.15584/actaires.2024.2.3

Krzysztof Chmielarz

Akademia Tarnowska
ORCID: 0000-0002-1088-8133

Patryk Chmielarz

Uniwersytet Komisji Edukacji Narodowej w Krakowie
ORCID: 0000-0003-0286-741X

PROCEDURAL USE OF WIRETAPPING AND INTERCEPTION OF COMMUNICATIONS IN THE REPUBLIC OF POLAND IN THE CONTEXT OF THE RIGHT TO PRIVACY

Introduction

The ubiquitous technological development and mass computerisation inevitably affect not only the daily lives of citizens, but also the availability of new surveillance techniques[1]. Despite the restrictions on citizens' rights and freedoms connected with ensuring state security, it becomes necessary to analyse the issue of violations of the realm of the individual's privacy by public authorities using surveillance methods[2].

Current Polish law stipulates two types of wiretapping, i.e. procedural wiretapping and interception of communications. Procedural wiretapping must be conducted in accordance with the provisions of the Act of 6 June 1997 – Code of Criminal Procedure. The interception of communications, however, is applied on the basis of specific laws, which indicate which entities (bodies and services) have the authority to conduct operational control, which includes, i. a. interception of communications. Procedural wiretapping is regulated in Chapter 19 entitled "Evidence" of the Code of Criminal Procedure (Art. 168a of the Code of Criminal Procedure and Art. 168b of the Code of Criminal Procedure) and in Chapter 26 of the Code of Criminal Procedure entitled "Surveillance and Telephone Tapping" (Art. 237–242

[1] K. Brylak-Hudyma, *Konstytucyjne prawa i wolności w obliczu nowych systemów inwigilacji*, "Prawo Mediów Elektronicznych" 2020, No. 2, p. 12.

[2] K. Chmielarz, *Prawo do prywatności a bezpieczeństwo wewnętrzne państwa. Kontrola operacyjna i dane telekomunikacyjne w kontekście inwigilacji społeczeństwa*, Warszawa 2020, p. 7.

of the Code of Criminal Procedure). Interception of communications is not included in the criminal procedure (Code of Criminal Procedure), but it is defined as part of the operational control carried out by authorised entities, which include: 1) state authorities of a police nature, including the Police, the Military Gendarmerie and the Border Guard; 2) the Intelligence Agency, as the Internal Security Agency and the Foreign Intelligence Agency, the Central Anti-Corruption Bureau, the Military Counterintelligence Service and the Military Intelligence Service; and 3) security and protection institutions, which include the State Protection Service, the National Tax Administration and the Internal Supervision Bureau of the Ministry of the Interior and Administration.

This study analyses the scope of the right to privacy according to the provisions of the Constitution of the Republic of Poland and the treaty rules of the European Union, without losing the field of research of the Strasburg case-law, the constitutional jurisprudence of the Republic of Poland or the law courts' decisions of the Republic of Poland.

Legal conditions of the right to privacy

When discussing the right to privacy, it should be noted that this right is one of those human rights and freedoms which are essential in a democratic state governed by the rule of law and at the same time serve as a kind of measure of the development of democracy, and the awareness of respect for privacy is also one of the determinants of a sense of security[3]. The right to protection of privacy in accordance with Art. 47 of the Constitution of the Republic of Poland of 2 April 1997, guarantee everyone the right to protection of private life, family life, honour and good name, as well as the right to decide on one's personal life.

Similarly, Art. 53(7) of the Constitution of the Republic of Poland indicates that no one can be obliged by public authorities to disclose their worldview, religious beliefs or religion. In the literature on the subject, it is also stated that the broadly understood right to privacy also includes the right of parents to bring up their children in accordance with their own convictions (Art. 48 of the Constitution of the Republic of Poland) and to provide their children with moral and religious upbringing and teaching in accordance with their own convictions (Art. 53(3) of the Constitution of the Republic of Poland)[4].

It should be noted that a manifestation of the right to privacy is also the inviolability of the dwelling, as defined in Art. 50 of the Constitution of the Republic

[3] J. Łebkowska, *Bezpieczeństwo – teoretyczny wymiar ponadczasowej wartości*, "Przegląd Strategiczny" 2011, No. 1, p. 37.

[4] K. Chałubińska-Jentkiewicz, M. Nowikowska, *Bezpieczeństwo, tożsamość, prywatność – aspekty prawne*, Warszawa 2020, p. 32.

of Poland, and admissibility of searches only in cases and as specified in the Act, and the secrecy of correspondence, as provided for in Art. 49 of the Constitution of the Republic of Poland, including all types of interpersonal contacts. Protection of the secrecy of correspondence also extends to modern means of conveying information such as telephone, telex, radiotelephone, audiotape, teleprinter, fax, smartphone, computer and other electronic media.

Distinguishing between the freedom of communication and the right to privacy, the doctrine indicates that the freedom of communication concerns primarily communication by means of a certain medium and not direct conversation between persons in a certain place, as this is rather an expression of the right to privacy[5].

The disposition of Art. 47 of the Constitution of the Republic of Poland indicates that alongside the legal protection of private and family life, the legislator included the right to decide about one's personal life, which also constitutes a manifestation of privacy in the broad sense[6]. In the doctrine of the subject, it is noted that the right to decide about one's personal life indicated in Art. 47 *in fine* means the possibility to choose one's profession, place of work and residence, marital status, lifestyle, aesthetic views. These can be matters related to collegial relations, the way of spending time, style of clothing, interests[7]. It should be noted that the constitutional provisions establishing the principle of protection of the sphere of private life are of general nature. However, this is a correct approach, as an attempt to precisely define the scope of the right to privacy and its content would create the risk of leaving important factual circumstances outside the scope of regulation. There is, in fact, a constant development of threats and means of protection of the right to privacy[8].

In Polish judicature, the right to privacy is defined as informational autonomy[9], understood as guaranteeing each person the right to decide for themselves to what extent they wish to remain anonymous and to what extent they consent to the sharing of their information with third parties[10]. It is the person themselves who determines the scope, the sphere of events in their life which may be disclosed to third parties[11].

In order to explain the concept of the right to privacy, it is necessary to analyse the construction of this right and its understanding on the basis of acts of international law, with particular regard to the acts of the Council of Europe,

[5] P. Sarnacki, *Prawo do ochrony prywatności* [in:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, ed. L. Garlicki, Warszawa 2007, p. 3.

[6] A. Mednis, *Prawo do prywatności a interes publiczny*, Warszawa 2006, p. 113.

[7] K. Chałubińska-Jentkiewicz, M. Nowikowska, *Bezpieczeństwo, tożsamość*…, p. 33.

[8] *Ibidem.*

[9] See: wyrok SA w Białymstoku z dnia 20 września 2018 r., sygn. I ACa 379/18.

[10] See: wyrok SA w Poznaniu z dnia 13 listopada 2001 r., sygn. I ACa 1140/01.

[11] See: wyrok SA w Warszawie z dnia 29 lipca 2014 r., sygn. VI ACa 1657/13.

including the European Convention on Human Rights[12]. Therefore, it seems necessary to discuss this issue on the basis of the ECHR. The European Convention on Human Rights in Art. 8 (1) states that everyone has the right to respect for their private and family life, their residence and their correspondence. Neither on the basis of the European Convention on Human Rights nor Polish legislation there is a legal definition of the right to privacy. Privacy is a broad term, analysed *ad casum*, which refers to the human psyche and feelings[13].

It should be emphasised that the ECHR does not contain a definition of private life. The Strasbourg Court in the case of *Niemietz vs. Germany* stated that the scope of the right to privacy includes the so-called *inner circle* in which an individual can live as they choose[14]. The right to respect for private life means the right to live as a person wishes, protected from the public. In the case of *Botta vs. Italy*, the ECHR indicated that this concept also includes the right to establish and develop relationships with other people in order to develop and fulfil one's own personality[15]. In the case of *Karhuvaara and Iltalehti vs. Finland*, the Court emphasised that the protection of personal data concerning a person's private information is crucial for the exercise of the right to respect for private life[16]. The concept of private life also extends to elements of an individual's identity, which include: name[17], surname[18], image[19], manner of clothing[20]. Family life includes marital relations and those arising from ties of kinship and affinity. It involves the right to obtain information on the adoptive family[21], paternity[22].

In the case of *Szabo and Vissy vs. Hungary*, the Court decided that legislation giving the State the right to monitor the conversations and correspondence of citizens is permissible, but it must satisfy guarantees that there will be no abuse on the part of the authorities, in particular, that that right will apply only in connection with a specific category of serious offences, will apply only to persons whose behaviour gives rise to such suspicion, that there are appropriate safeguards and limits on the duration of such measures, and that there is a procedure for obtaining and subsequently storing and destroying the materials thus obtained[23].

---

[12] The European Convention on Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and 14 supplemented by Protocols No. 1, 4, 6, 7, 12, 13 and 16.

[13] J. Braciak, *Prawo do prywatności*, Warszawa 2004, p. 21.

[14] See: Judgment ECHR of 16 December 1992, *Niemietz vs. Germany*, No. 13710/88.

[15] See: Judgment ECHR of 24 February 1998, *Botta vs. Italy*, No. 21439/93.

[16] See: Judgment ECHR of 25 February 1997, *Z. vs. Finland*, No. 22009/93.

[17] T. Jasudowicz, *Orzecznictwo strasburskie*, Warszawa 1998, pp. 570–572.

[18] See: Judgment ECHR of 22 February 1994, *Burghartz vs. Switzerland*, No. 16213/90.

[19] See: Judgment ECHR of 24 June 2004, *Von Hannover vs. Germany*, No. 59320/00.

[20] See: Judgment ECHR of 15 May 1980, *McFeeley vs. United Kingdom*, No. 8317/78.

[21] See: Judgment ECHR of 7 July 1989, *Gaskin vs. United Kingdom*, No. 10454/83.

[22] See: Judgment ECHR of 28 December 1984, *Rasmussen vs. Denmark*, No. 8777/79.

[23] See: Judgment ECHR of 12 January 2016, *Szabo and Vissy vs. Hungary*, No. 37138/14.

When it comes to the protection of state security, the state may exercise a certain freedom to use secret methods which have the effect of violating the right to privacy[24]. Therefore, there must be a legal basis allowing for the identification *in abstracto* of the subjective and material conditions for interference[25], and such measures may be applied only where necessary in a democratic state and only for a limited period of time, necessary for the achievement of the aim pursued[26]. In addition, there must be effective control exercised by an independent body over access to and subsequent use of communications[27].

It should be stressed that the disposition of Art. 8 ECHR does not guarantee the right to private life, but the right to respect for private life. The State must ensure that third parties do not interfere in the private life of individuals[28].

The protection of private life does not extend to information that is "of a public nature", but even public information may fall within the protection of Art. 8 ECHR also if it is systematically collected and stored by the authorities[29]. It should be noted that the recording of private (telephone) conversations by the opposing party and the private use of such recordings do not constitute a violation of Art. 8 of the Convention if they have been made by private means, but by its very nature, such a situation must be distinguished from the case of secret monitoring and recording of conversations between private persons in the context and for the purpose of official proceedings, criminal or otherwise, and with the consent and technical assistance of the official investigating authorities[30].

The European Court of Human Rights, in the case of *Klass and others vs. Germany*, has indicated that private life, as referred to in Art. 8(1) of the European Charter of Human Rights, cannot be reduced to the strictly personal and inner affairs of an individual, but must be understood, also in social terms, as the opportunity to develop contacts with others and to interact with the outside world[31]. After all, the European Court of Human Rights did not deny the admissibility of secret obtaining of information about individuals by public authorities, but even pointed to its indispensability, as a tool to effectively guarantee security and protect institutions of a democratic state against sophisticated forms of threats, especially espionage or

[24] See: Judgment ECHR of 24 April 1990, *Huvig vs. France*, No. 11105/84; Judgment ECHR of 16 February 2000, *Amann vs. Switzerland*, No. 27798/95; Judgment ECHR of 26 March 1987, *Leander vs. Sweden*, No. 9248/81; Judgment ECHR of 30 July 1998, *Valenzuela Contreras vs. Spain*, No. 27671/95.

[25] See: Judgment ECHR of 20 February 2009, *Iordachi and others vs. Moldova*, No. 25198/02.

[26] See: Judgment ECHR of 6 September 1978, *Klassand others vs. Germany*, No. 5029/71.

[27] See: Judgment ECHR of 2 August 1984, *Malone vs. United Kingdom*, No. 8691/79.

[28] K. Chałubińska-Jentkiewicz, M. Nowikowska, *Bezpieczeństwo, tożsamość*…, p. 50.

[29] See: Judgment ECHR of 7 June 2006, *Segerstedt-Wiberg and others vs. Sweden*, No. 62332/00; Judgment ECHR of 18 November 2008, *Canli vs. Turkey*, No. 22427/04.

[30] See: Judgment ECHR of 25 October 2007, *van Vondel vs. Netherlands*, No. 38258/03.

[31] See: Judgment ECHR of 6 September 1978, *Klass and others vs. Germany*, No. 5029/71.

terrorism. The case-law of the ECHR clearly indicates that state interference in the sphere of individual privacy must always be precisely defined in the applicable law, and even more so in the case of the regulation of wiretapping[32].

The importance of EU law in interpreting and determining the scope of the right to privacy plays a significant role. Essential to this is the Charter of Fundamental Rights of the European Union[33], in which, according to Art. 7, everyone has the right to respect for private and family life, home and communication. The freedom and secrecy of communications and the right to privacy are not absolute and are subject to limitations related to the necessity of the performance of tasks by the State authorities responsible for security, defence and public order. The provisions of Art. 13 of Directive 95/46/EC of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data provide that a Member State may adopt legislative measures to restrict the scope of the rights and obligations provided for in Art. 6(1), Art. 10, 11(1) and Art. 12 and 21 of that Directive when such a restriction constitutes a measure necessary to safeguard national security, defence and public security[34].

Article 5(1) of Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 imposes an obligation on Member States to preserve the confidentiality of communications and prohibits the listening, recording, storing or otherwise intercepting or monitoring of communications and related traffic data by persons other than users, without the consent of the users concerned, except as authorised under Art. 15(1) of that Directive, which allows for restrictions on the confidentiality of communications in exceptional situations[35]. According to the Court of Justice of the European Union[36] these specific situations include measures which are necessary, appropriate and proportionate within a democratic society to safeguard

[32] See: Judgment ECHR of 29 June 2006, *Weber and Saravia vs. Germany*, No. 54934/00; Judgment ECHR of 4 December 2015, *Zakharov vs. Russia*, No. 47413/06; Judgment ECHR of 4 May 2000, *Rotaru vs. Romania*, No. 28341/95; Judgment ECHR of 2 September 2010, *Uzun vs. Germany*, No. 35623/05; Judgment ECHR of 6 September 1978, *Klass and others vs. Germany*, No. 5029/71; Judgment ECHR of 6 October 2015, *Maximillian Schrems vs. Data Protection Commissioner* with the participation of *Digital Rights Ireland Ltd*, No. C-362/14.

[33] See: Charter of Fundamental Rights of the European Union.

[34] See: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995), p. 31; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016).

[35] See: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (*OJ L 201, 31.7.2002)*, p. 37.

[36] See: Judgment ECHR of 29 January, *Productores de Música de España (Promusicae) vs. Telefónica de España SAU*, No. C-275/06.

national security (state security), defence, public security and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system[37].

The analysis of the Court of Justice of the European Union case law indicates certain lines of interpretation of Art. 7 of the Charter of Fundamental Rights of the European Union. In the judgment in joined cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications and others, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others*, the Court of Justice assessed infringement by the provisions of Directive No. 2006/24/EC of the European Parliament and the Council expressed in Art. 7 of the right to privacy[38]. Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC imposed an obligation on Member States to ensure that providers of publicly available electronic communications services retain and store for a period of two years data generated by the use of those services, including address, billing and location data generated by users of electronic communications[39]. Similarly, in the cases of *Secretary of State for the Home Department and Tele2 Sverige AB*, the Court of Justice recognised a threat to the right to privacy posed by the national provisions of Sweden and the United Kingdom[40]. In both cases, national acts imposed an obligation on providers of electronic communications services to store data generated in the course of providing those services. The Court pointed out that the overall data generated by network traffic provided accurate data on the private lives of users. Such information and its collection could give the impression of constant observation of users' private lives. For this reason, according to the CJEU, the mere storage of such data constitutes a profound interference with the right to privacy of the individual and the right to informational autonomy[41].

In particular, in recent years, the CJEU's judgment on *Google Spain SL, Google Inc. vs. Agencia Espanola de Protección de Datos (AEPD) and Mario Costeja González*, on the basis of Directive 95/46/EC of the European Parliament and the Council, where the Court addressed the requirements relating to the processing of personal

[37] M. Rogalski, *Podsłuch procesowy i pozaprocesowy. Kontrola i utrwalanie rozmów na podstawie k.p.k. oraz ustaw szczególnych*, Warszawa 2016, p. 35.

[38] See: Judgment ECHR of 8 April 2014, *Digital Rights Ireland Ltd vs. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and Attorney General*, No. C-293/12; *Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others*, No. C-594/12.

[39] K. Chałubińska-Jentkiewicz, M. Nowikowska, *Bezpieczeństwo, tożsamość*…, p. 51.

[40] See: Judgment ECHR of 21 December 2016, *Tele2 Sverige AB vs. Post- och telestyrelsen*, No. C-203/15; *Secretary of State for the Home Department vs. Tom Watson, Peter Brice, Geoffrey Lewis*, No. C-698/15.

[41] K. Chałubińska-Jentkiewicz, M. Nowikowska, *Bezpieczeństwo, tożsamość*…, p. 52.

data of automated indexing carried out by search engines, imposing an obligation on search engine operators to remove, at the request of the individual, links to websites published by third parties containing information about the individual. The Court has ruled that an individual's rights in that regard are, in principle, overridden not only by the economic interest of the operator of an internet search engine but also by the interest which the potential recipients may have in finding that information through a search carried out on the person's full name[42].

Notwithstanding the above, Art. 8 ECHR remains a valuable source of inspiration when interpreting Art. 47 of the Constitution of the Republic of Poland, since the considerations made on the basis of Art. 8 ECHR may also in most cases, due to the similarity of the analysed conflicts of values, remain under the Polish constitutional order[43].

Legal aspects of procedural wiretapping

Wiretapping is the secret obtaining and recording of the content of conversations carried out with the use of means of communication by any technical devices. Wiretapping also involves the monitoring of conversations carried out outside of a communication system, provided that the person performing the monitoring is not a participant in this conversation[44].

In the doctrine and case law of the courts, wiretapping is not a uniform concept, since two types are distinguished: procedural wiretapping and interception of communications. The theory also distinguishes passive wiretapping, which violates the confidentiality of the transmitted information without changing its content, and active wiretapping, which, like passive wiretapping, violates confidentiality and additionally modifies the content, causing a disturbance to the authenticity or integrity of the information[45].

The procedural and out-of-court activity of the authorities authorised to apply and conduct wiretapping occurs only and exclusively in the form of passive wiretapping, since active wiretapping is inadmissible under Polish law[46].

The wiretapping discussed relates exclusively to wiretapping conducted in the course of ongoing criminal proceedings, and the ordering or approval of its legality by a Polish court does not apply to wiretapping conducted by the authorities

[42] See: Judgment ECHR of 13 May 2014, *Google Spain SL, Google Inc. vs. Agencia Espanola de Protección de Datos (AEPD), Mario Costes González*, No. C-131/12.

[43] *Konstytucja RP. Komentarz*, Vol. I–II, eds. M. Safjan, L. Bosek, Warszawa 2016, p. 32.

[44] K. Dudka, *Podsłuch prywatny i dziennikarski a proces karny* [in:] *Problemy stosowania prawa sądowego. Księga ofiarowana Profesorowi Edwardowi Skrętowiczowi*, ed. I. Nowikowski, Lublin 2007, p. 106.

[45] M. Rogalski, *Podsłuch procesowy*…, p. 52.

[46] K. Dudka, *Kontrola korespondencji i podsłuch w polskim procesie karnym*, Lublin 1998, p. 60.

of another state. The legality of wiretapping conducted by the authorities of a foreign state in the course of proceedings pending there should be assessed in accordance with the provisions in force in the state in which the activity is carried out. Pursuant to Art. 237 § 1 of the Code of Criminal Procedure, the monitoring and recording of telephone conversations (wiretapping) may be ordered by the court at the prosecutor's request after initiation in order to detect and obtain evidence for the ongoing proceedings or to prevent the commission of a new offence.

Monitoring and recording of conversations is admissible during the proceedings, i.e. after the initiation of preparatory proceedings and already in the *ad rem* phase (identification of a suspect). Therefore, the monitoring and recording of conversations is inadmissible in the case when the proceedings are not pending (have not been initiated) or have already been completed. The application of wiretapping should aim at preventing the perpetrator of the act subject to proceedings or other person connected with the perpetrator or their act from committing a new offence[47].

The prosecutor in accordance with Art. 119 § 1 of the Code of Criminal Procedure in the justification of the request for the ordering of wiretapping, indicates the advisability and necessity (evidential, preventive), and in particular the adequacy (proportionality) of conducting the monitoring and recording of telephone conversations. Polish regulations does not introduce the principle of subsidiarity in connection with procedural wiretapping, but this does not mean that the monitoring and recording of conversations may be ordered by the court in every case, and not only when it is necessary. This is because the constitutional principles of subsidiarity and proportionality of interference with personal freedom and rights apply. Wiretapping must be necessary (essential) for the detection and obtaining of evidence for ongoing proceedings or for the prevention of offences.

The court's decision on approval of the request of the prosecutor to monitor and record the content of telephone conversations requires the form of a decision. The court on the basis of Art. 237 § 2 of the Code of Criminal Procedure decides in a session without the participation of the parties. The court's decision is issued only at the request of the prosecutor, and the police in the preparatory proceedings do not have powers in this respect. Pursuant to Art. 237 § 2 of the Code of Criminal Procedure, in urgent cases the prosecutor may order monitoring and recording of telephone conversations, but they are obliged to apply to the court for approval of the decision within 3 days. The court issues a decision on the request within 5 days in a session without the participation of the parties. The court's consent is of a consequential nature, unlike the consent given by the court pursuant to Art. 237 § 1 of the Code of Criminal Procedure, which has the nature of a prior consent. If the prosecutor's decision is not approved, the court in the decision issued on the request orders to destroy all the recorded materials. Appealing against the court's decision concerning the prosecutor's request on the

[47] M. Rogalski, *Podsłuch procesowy*…, p. 54.

basis of Art. 237 § 2 of the Code of Criminal Procedure withholds its execution, which means that it is absolutely suspensive. It also withholds the destroying of all recordings from wiretapping, which should be destroyed only after the court decision becomes final.

The court's decision pursuant to Art. 237 § 2 of the Code of Criminal Procedure on the approval of the prosecutor's decision legalises the telephone tapping ordered by the prosecutor. In turn, the prosecutor's failure to apply for wiretapping approval within the time limit indicated in this provision has the same effect as non-approval of the monitoring and recording of telephone conversations ordered by them (Art. 238 § 3 of the Code of Criminal Procedure). Such wiretapping becomes illegal and must be stopped immediately, and consequently, evidence from such wiretapping, as obtained in a manner contrary to the act, is subject to removal from the penal process and cannot be the basis for factual findings. If at the hearing the evidence obtained until the prosecutor's decision was not approved was provided, the court should reject this evidence, as the acceptance of this evidence would constitute a violation of the provisions of the criminal procedure.

Only the telephone numbers indicated in the request, namely those used by persons indicated in Art. 237 § 4 of the Code of Criminal Procedure, i.e. the suspect, the defendant and in relation to the victim or any other person with whom the defendant may come into contact or who may be associated with the perpetrator or with a threat of a crime, are subject to wiretapping ordered in the course of proceedings.

Pursuant to Art. 237 § 3 of the Code of Criminal Procedure, the monitoring and recording of the content of telephone conversations is admissible only if the pending proceedings or a justified fear of a new offence concerns: 1) murder; 2) exposure to public danger or causing a catastrophe; 3) human trafficking; 4) abduction of a person; 5) racketeering; 6) unlawful seizure of aircraft or ships; 7) robbery, aggravated theft or racketeering and extortion; 8) an attempt on the sovereignty or integrity of the state; 9) an attempt on the constitutional state system or its main bodies, or on a unit of the Armed Forces of the Republic of Poland; 10) espionage or disclosure of classified information with the security classification "secret" or "top secret"; 11) collection of weapons, explosives or radioactive materials; 12) forgery and trading in counterfeit money, means or instruments of payment or negotiable documents entitling to the receipt of a sum of money, goods, cargo or in-kind winnings, or containing an obligation to pay capital, interest, share in profits or a declaration of participation in a company; 12a) counterfeiting or falsification of invoices, or the use of counterfeit or falsified invoices in the scope of factual circumstances which may be relevant to the determination of the amount of a public payment or its refund, or to the refund of another payment of a tax nature, as well as the issue and use of invoices attesting untruth in relation to

factual circumstances which may be relevant to the determination of the amount of a public payment or its refund or to the refund of another payment of a tax nature; 13) manufacturing, processing, marketing and smuggling of drugs, precursors, substitutes or psychotropic substances; 14) organised criminal group; 15) property of significant value; 16) use of violence or unlawful threat in connection with criminal proceedings; 16a) giving false testimony and presenting a false opinion, expertise or translation by an expert, assessor or translator; 16b) falsely accusing another person of committing an offence, a fiscal offence or a fiscal transgression 16c) creation of false evidence or other deceitful acts, directing a prosecution against another person for an offence, a fiscal offence or a fiscal transgression, or undertaking such acts in the course of proceedings; 16d) withholding evidence of innocence of a person suspected of committing an offence, a fiscal offence or a fiscal transgression; 16e) notifying a body appointed for prosecution of an offence or a fiscal transgression that has not been committed; 16f) aiding and abetting; 16g) failure to report an offence; 17) bribery and influence peddling; 18) procurement, facilitation of prostitution and pandering; 19) offences specified in Chapter XVI of the Act of 6 June 1997 – Criminal Code and in Art. 5–8 of the Rome Statute of the International Criminal Court, drafted in Rome on 17 July 1998. Monitoring and recording of the content of telephone conversations is also admissible for the purpose of disclosing property threatened with forfeiture, referred to in Art. 45 § 2 of the Criminal Code or Art. 33 § 2 of the Act of 10 September 1999 – Penal Fiscal Code and in Art. 5–8 of the Rome Statute of the International Criminal Court.

The doctrine emphasises that the monitoring of conversations cannot be of an abstract nature (without specifying the category of offence). It is therefore inadmissible to order wiretapping if the proceedings are conducted in the matter of revealing property other than that threatened with forfeiture referred to in Art. 45 § 2 of the Criminal Code or Art. 33 § 2 of the Penal Fiscal Code. It should be noted that the catalogue of offences characterised by a high degree of social noxiousness of an act and high gravity of an offence is closed, therefore as a rule, the use of wiretapping is not admissible if it concerns offences not listed in Art. 237 § 3 of the Code of Criminal Procedure. If, however, the legal classification of the act for which proceedings are pending both *in rem* (in the case) and *in personam* (against a specific person) is changed, in the course of wiretapping, to an offence not listed in Art. 237 § 3 of the Code of Criminal Procedure, it will be necessary to discontinue the evidential act of wiretapping[48].

Procedural wiretapping may be conducted for a maximum of 3 months with the possibility of extension, in a particularly justified case, for a maximum of a further 3 months. In total, the monitoring and recording of telephone conversations

[48] *Ibidem*, p. 76.

in the course of one proceeding may last a maximum of 6 months, and in the event of the expiration of this period, it is not possible to extend the wiretapping even if justified and necessary. The wiretapping shall be discontinued immediately after the termination of the reasons listed in Art. 237 § 1–3 of the Code of Criminal Procedure, but at the latest upon the expiry of the period for which Art. 238 § 2 of the Code of Criminal Procedure was introduced.

Pursuant to Art. 238 § 3 of the Code of Criminal Procedure the prosecutor, upon the termination of the monitoring, requests the court to order the destruction of all recordings if all of them are irrelevant for the purpose of criminal proceedings. This refers to a situation, when during wiretapping no information of importance for the conducted criminal proceedings was recorded, which could be used as evidence in these proceedings. The court decides on the request immediately in a session without the participation of the parties, determining which recordings of the conversations are no longer relevant to the proceedings and should be destroyed, and which may be used in the criminal proceedings. Destruction means the physical removal of the recordings of telephone conversations from the media on which they were recorded. A transcript, if made, should also be destroyed[49].

Similarly, after the preparatory proceedings on the basis of Art. 238 § 4 of the Code of Criminal Procedure the prosecutor requests the court to order the destruction of recordings in the part in which they are not important for the criminal proceedings and do not constitute evidence. The court decides on the request submitted by the prosecutor at a session, in which the parties may participate. Also a person referred to in Art. 237 § 4 of the Code of Criminal Procedure may submit a request for ordering the destruction of recordings, not earlier than after the preparatory proceedings have been completed. The court decides on the request at a session in which the parties and the applicant may participate.

Legal aspects of interception of communications

Interception of communications is conducted in the mode of operational surveillance, which is a part of operational and investigative activities. Detailed regulations for operational and investigative activities are determined by departmental ordinances and instructions, which are secret and bear appropriate confidentiality clauses. Operational and investigative activities are carried out by Polish services within the framework of the so-called operational work by means of various forms and methods, which are precisely defined in ordinances of respective Heads of

[49] B. Kurzępa, *Kontrola i utrwalanie rozmów telefonicznych według kodeksu postępowania karnego*, "Prokuratura i Prawo" 1999, No. 13, p. 77.

Service, covered by a confidentiality clause. These activities are conducted mainly in order to obtain information on the perpetrator of an offence and the act itself, on events, persons and environments that are of interest to law enforcement agencies, as well as in order to verify findings already made by services in a specific case.

As already mentioned, operational surveillance is part of an out-of-court type of monitoring and recording of the content of telephone conversations, referred to as interception of communications. That is, interception of communications occurs outside the Polish criminal trial. Eleven Polish law enforcement agencies are appointed to use it: 1) the Police; 2) the Internal Security Agency; 3) the Foreign Intelligence Agency; 4) the Central Anti-Corruption Bureau; 5) the Border Guard; 6) the Military Counterintelligence Service; 7) the Military Intelligence Service; 8) the Military Gendarmerie; 9) the National Tax Administration (Customs and Fiscal Service); 10) the State Protection Service and 11) the Internal Supervision Bureau of the Ministry of the Interior and Administration.

The analysis of materials collected during operational surveillance enables obtaining materials of great significance, allowing for precise penetration into criminal groups and mutual connections between communicating persons, which allows for quick detection of perpetrators of crimes. Consequently, it is possible to obtain knowledge which has not been available to law enforcement agencies so far[50].

Operational surveillance is conducted secretly and includes: 1) obtaining and recording the content of conversations conducted with the use of technical means, including via telecommunication networks; 2) obtaining and recording the image or sound of persons from premises, means of transport or places other than public places; 3) obtaining and recording the content of correspondence, including correspondence conducted with the use of means of electronic communication; 4) obtaining and recording data contained in computer data carriers, telecommunication terminal equipment, IT and ICT systems; 5) accessing and controlling the content of parcels.

Operational surveillance is conducted notwithstanding the provisions of the Code of Criminal Procedure, as it has different aims and objectives. Interception of communications, which is a part of operational surveillance, may be conducted in preparatory proceedings both *in rem* and *in personam*, as well as in jurisdictional proceedings parallel to conducted procedural actions. The use of interception of communications is allowed also before the initiation of proceedings, in the course of proceedings even when a procedural wiretapping is already in use. Operational surveillance by state law enforcement bodies is of a subsidiary nature, meaning that it may be ordered only if other measures used so far have proved to be ineffective or the investigative methods used are of no use[51].

[50] J. Słoński, *Kontrola operacyjna*, "Kwartalnik Prawno-Kryminalistyczny Szkoły Policji w Pile" 2011, No. 3–4, p. 26.

[51] M. Rogalski, *Podsłuch procesowy*…, p. 179.

In accordance with the judgment of the Supreme Court, the provisions governing procedural wiretapping and interception of communications are considered a circumstance excluding unlawfulness of wiretapping, they are an important indication when assessing the exclusion of unlawfulness in other cases of wiretapping, because they prove in which situations the legislator themselves allows the possibility of limiting the secrecy of communications[52].

The powers in the field of conducting operational surveillance are vested in the Internal Security Agency, pursuant to Art. 27(1) of the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency. On the basis of Art. 5(1) of the Act on the Internal Security Agency and the Foreign Intelligence Agency, the tasks of the Internal Security Agency include in particular: 1) the recognition, prevention and combating of threats against the internal security of the state and its constitutional order, and in particular against the sovereignty and international position, independence and inviolability of its territory, as well as national defence; 2) the recognition, prevention and detection of offences of espionage, terrorism, the unlawful disclosure or use of classified information and other offences against the security of the state 3) obtaining, analysing, processing and transmitting to competent authorities information which may be of significant importance for the protection of the internal security of the state and its constitutional order; 4) undertaking other activities specified in separate laws and international agreements.

Also, pursuant to Art. 6(3) of the Act on the Internal Security Agency and the Foreign Intelligence Agency, the powers vested in the Foreign Intelligence Agency to conduct operational surveillance, in the territory of Poland, are vested in the Agency only in connection with its activities outside the borders of the state and only through the Head of the Internal Security Agency.

The tasks of the Foreign Intelligence Agency, which are carried out primarily outside the borders of the Republic of Poland, generally include: 1) obtaining, analysing, processing and transmitting to competent authorities information which may be of significant importance to the security and international position of the Republic of Poland as well as its economic and defence potential; 2) recognising and counteracting external threats against the security, defence, independence and inviolability of the territory of the Republic of Poland 3) protecting diplomatic missions of the Republic of Poland and their employees against activities of foreign special services and other activities that may be detrimental to the interests of the Republic of Poland; 4) ensuring cryptographic protection of communications with Polish diplomatic and consular missions and providing courier service; 5) identifying international terrorism, extremism and international organised crime groups; 6) conducting electronic intelligence; 7) undertaking other activities specified in separate laws and international agreements.

[52] See: wyrok SN z dnia 13 listopada 2002 r., sygn. I CKN 1150/00.

The purpose of carrying out operational surveillance by the Internal Security Agency and the Foreign Intelligence Agency, and therefore also the use of interception of communications, is to recognise, prevent and detect offences indicated in Art. 27(1) of the Act on the Internal Security Agency and the Foreign Intelligence Agency, as well as to obtain and preserve evidence of such offences, disclose property threatened with forfeiture in connection with such offences and prosecute their perpetrators.

Interception of communications used by the Internal Security Agency and the Foreign Intelligence Agency may last only as long as it has been ordered, i.e. for a specified period of time, and should be terminated immediately after the reasons for ordering it cease to exist. The Head of the Internal Security Agency is obliged to execute the court's order to destroy the materials and the immediate, witnessed and recorded destruction of materials whose use in criminal proceedings is inadmissible. Furthermore, the Public Prosecutor General orders the destruction of materials obtained as a result of wiretapping which do not contain evidence of criminal offences or are not important for state security.

The Military Counterintelligence Service, on the basis of Art. 31(1) of the Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service, is authorised to use operational surveillance. The main tasks of the Military Counterintelligence Service include: 1) recognition, prevention and detection of offences committed by soldiers in active military service, officers of the Military Counterintelligence Service and the Military Intelligence Service and employees of the Armed Forces of the Republic of Poland and other organisational units of the Ministry of National Defence: against peace, humanity and war crimes defined in the Polish Criminal Code, as well as other acts and international agreements; 2) recognition, prevention and detection of incidents and offences of terrorism against the security of the defence potential of the state, the Armed Forces of the Republic of Poland and organisational units of the Ministry of National Defence; 3) conducting radioelectronic counterintelligence and undertakings in the field of cryptographic protection and cryptanalysis; 4) participation in planning and conducting inspections of the implementation of international agreements on disarmament; 5) protecting the security of military units, other organisational units of the Ministry of National Defence and soldiers performing official tasks outside the borders of the state.

Military Intelligence Service on the basis of Art. 6(3) of the Act on the Military Counterintelligence Service and the Military Intelligence Service is authorised to use operational surveillance only on the territory of the Republic of Poland and can be conducted only in connection with its activities abroad and only through the Military Counterintelligence Service or the Internal Security Agency, according to their respective competences.

The main tasks of the Military Intelligence Service include: 1) obtaining, collecting, analysing, processing and transmitting to competent authorities information which may be of significant importance to the security of the defence

potential of the Republic of Poland and the safety and combat capability of the Armed Forces of the Republic of Poland; 2) recognition of international trade in weapons, munition and explosives, as well as goods, technologies and services of strategic importance to the state security, and recognition of international trade in weapons of mass destruction and threats related to the proliferation of these weapons and their means of delivery; 3) recognition, counteraction and prevention of terrorist incidents against personnel and property of the Armed Forces of the Republic of Poland outside the state borders and combating the effects of such incidents; 4) recognising and analysing threats occurring in regions of tension, conflicts and international crises, affecting the state defence and the combat capability of the Armed Forces of the Republic of Poland, as well as undertaking actions aimed at eliminating those threats.

The aim of conducting operational surveillance by the Military Counterintelligence Service, and therefore the use of interception of communications, is to recognise and detect offences against specific legally protected goods: peace, humanity and war crimes, as well as to prevent such offences.

Officers of the Central Anti-Corruption Bureau, on the basis of the delegation contained in Art. 17(1) of the Act of 9 June 2006 on the Central Anti-Corruption Bureau, are authorised to conduct operational surveillance, which is conducted in secret, like all wiretapping of this type.

The main tasks of the Central Anti-Corruption Bureau include: 1) recognising, preventing and detecting offences against the activities of state and local government institutions, referred to in Art. 228–231 of the Criminal Code, against the administration of justice referred to in Art. 232 of the Criminal Code, Art. 233 of the Criminal Code, Art. 234 of the Criminal Code Art. 235 of the Criminal Code, Art. 236 § 1 of the Criminal Code and Art. 239 § 1 of the Criminal Code, and against financing of political parties, specified in Art. 49d and 49f of the Act of 27 June 1997 on political parties (Dz.U. of 2018, Item 580), if they remain in connection with corruption; 2) disclosure of cases of failure to comply with the procedures specified by law for taking and implementing decisions on: privatisation and commercialisation, financial support, public procurement, disposal of property of entities or entrepreneurs, and granting of concessions, permits, subjective and subjective VAT exemptions, concessions, preferences, quotas, plafonds, sureties and credit guarantees; 3) control of the correctness of implementation of contracts on public-private partnership; 4) control of the correctness and authenticity of declarations of financial interests or declarations on conducting business activities by persons performing public functions referred to in Art. 115 § 19 of the Criminal Code.

The purpose of conducting operational surveillance by the Central Anti-Corruption Bureau is to recognise, prevent and detect offences indicated in Art. 17 (1) and (4) of the Act on the Central Anti-Corruption Bureau and to obtain and record evidences of offences, as well as to disclose property threatened with forfeiture in connection with offences.

It is difficult to imagine that interception of communications could not be carried out by the Police, which i.a. prevent, detect and identify perpetrators of offences. The provisions of Art. 19 (1) of the Act of 6 April 1990 on the Police contain a closed catalogue of offences which may be subject to wiretapping. The legislator provided for the possibility of ordering wiretapping by the Police in order to: 1) prevention, detection and identification of perpetrators; 2) obtaining and recording of evidence of offences prosecuted by public indictment; 3) intentional crimes prosecuted under international agreements ratified with prior consent expressed in a law, as defined in the Polish Criminal Law.

Pursuant to Art. 1(2) of the Act on the Police, the main tasks of the Police include: 1) protection of life and health of people and of property against unlawful attacks violating these goods; 2) protection of public security and order, including ensuring peace in public places as well as in means of public transport and public communication, in road traffic and on waters intended for public use; 3) conducting counter-terrorist activities; 5) detection of crimes and offences and prosecution of the perpetrators; 4) processing of criminal information, including personal data; 5) keeping of data collections containing information collected by authorised bodies on fingerprints of persons, unidentified fingerprints from crime scenes and the results of deoxyribonucleic acid (DNA) analysis; 6) implementation of tasks resulting from the provisions of the European Union law and international agreements on the principles and in the scope specified therein.

In the Act of 24 August 2001 on the Military Gendarmerie and military law enforcement the performance of operational surveillance, including the interception of communications, is regulated in Art. 31(1) of the Act, which states that the Military Gendarmerie, within the limits of its tasks, may in order to prevent, detect, identify perpetrators and obtain and record evidence of intentional crimes prosecuted by public indictment, when other measures have proved ineffective or will be of no use, a military district court, at the written request of the Chief Commander of the Military Gendarmerie, submitted after obtaining the written consent of the Public Prosecutor General, or at the written request of the Commander of the Military Gendarmerie unit, submitted after obtaining the consent of the Chief Commander of the Military Gendarmerie and the written consent of the competent deputy district attorney for military affairs, may by issuing a decision to order the interception of communications.

Pursuant to Art. 4(4) of the Act on the Military Gendarmerie, the tasks of the Military Gendarmerie are: 1) ensuring observance of military discipline; 2) protection of public order in the areas and facilities of military units as well as in public places; 3) protection of life and health of people and of military property against attacks infringing these goods; 4) conducting activities on the areas or in the facilities belonging to the units and organisational units subordinate to the Minister of National Defence or supervised by him or administered by these

units and organisational units 5) protection of diplomatic missions of the Republic of Poland located in the place of stationing of Polish Military Contingents and protection of diplomatic and consular personnel of these posts; 6) cooperation with Polish and foreign authorities and services competent in matters of public security and order as well as with military police.

The provisions of Art. 9e of the Act of 12 October 1990 on the Border Guard provide for the possibility of conducting the interception of communications. Pursuant to the above-mentioned disposition, when performing operational and investigative activities undertaken by the Border Guard in order to prevent, detect, identify perpetrators and obtain and record evidence of an intentional crime prosecuted by public indictment, listed in the Act, when other measures have proved to be ineffective or will be of no use, the court at the written request of the General Commander of the Border Guard or the Commander of the Border Guard Internal Affairs Bureau, after obtaining a written consent of the Public Prosecutor General, or at the written request of the Commander of the Border Guard unit, after obtaining a written consent of the competent district attorney, may by issuing a decision to order the interception of communications.

On the basis of Art. 1(2) of the Act on the Border Guard, the tasks of the Border Guard include: 1) protecting the state border on land and sea; 2) organising and controlling border traffic; 3) preventing and counteracting illegal migration; 4) issuing permits for crossing the state border, including visas; 5) recognising, preventing and detecting offences and prosecuting their perpetrators, within the competence of the Border Guard, 6) carrying out security checks in means of transport at international road, rail, sea and river border crossing points, 7) ensuring security on board aircraft carrying passengers by air; 8) protection of the state border in the airspace of the Republic of Poland by conducting observations of aircraft and flying objects flying across the state border at low altitudes and informing about these flights the appropriate units of the Air Force of the Armed Forces of the Republic of Poland.

On the basis of Art. 42(1)–(2) of the Act of 9 June 2006 on the State Protection Service, in order to recognise, prevent and detect intentional offences prosecuted by public indictment and specified in the Act, when other measures have proved ineffective or will be of no use, the District Court in Warsaw may, by issuing a decision, order an operational surveillance upon a written request of the Commander of the State Protection Service submitted after obtaining the written consent of the Public Prosecutor General. The request is presented together with materials justifying the need to apply an operational surveillance.

Pursuant to Art. 3 of the Act on the State Protection Service, the main tasks of the State Protection Service include: 1) the protection of the President of the Republic of Poland, the Marshal of the Sejm, the Marshal of the Senate, the President of the Council of Ministers, the Deputy Prime Minister, the minister

responsible for internal affairs and the minister responsible for foreign affairs as well as former presidents of the Republic of Poland 2) the recognition and prevention of offences against the Republic of Poland, offences against life or health, offences against public security, offences against safety in communications, offences against freedom, offences against honour and personal inviolability, offences against public order, attacks and active assaults directed against protected persons.

Pursuant to Art. 118(1) of the Act of 16 November 2016 on the National Tax Administration within the framework of operational and investigative activities undertaken by officers carrying out operational and investigative activities in order to detect, determine perpetrators and obtain and record evidence of offences: 1) fiscal offences, if the value of the object of the offence or depletion of the public law liabilities exceeds, on the date the offence was committed, fifty times the minimum remuneration for work; 2) fiscal offences referred to in Art. 107 § 1 of the Penal Fiscal Code; 3) against economic transactions, causing material damage, if the amount of the damage exceeds, on the date the offence was committed, fifty times the minimum remuneration for work; 4) defined in Art. 270a § 1 and 2 of the Criminal Code, Art. 271a § 1 and 2 of the Criminal Code and Art. 277a § 1 of the Criminal Code; 5) against property, if the value of the property exceeds on the date of committing the offence fifty times the amount of the minimum remuneration for work; 6) specified in Art. 258 of the Criminal Code, Art. 270 of the Criminal Code, Art. 271 of the Criminal Code or Art. 273 of the Criminal Code, in connection with which there has been a depletion or exposure to a depletion of public law liabilities exceeding fifty times the amount of the minimum remuneration for work; 7) defined in Art. 228–231 of the Criminal Code, committed by persons employed in organisational units of the National Tax Administration or by officers, in connection with the performance of official activities; 8) defined in Art. 229 of the Criminal Code, committed by persons not employed in organisational units of the National Tax Administration or who are not officers, in connection with the performance of official activities by persons referred to in the Act; 9) prosecuted under international agreements ratified with prior consent expressed in a law, specified in the Polish Criminal Law; 10) specified in points 1–8 or in Art. 33 § 2 of the Fiscal Penal Code – in order to disclose property threatened with forfeiture – if other measures have proved ineffective or will be of no use, the District Court in Warsaw, at a written request of the Head of the National Fiscal Administration submitted after obtaining a written consent of the Public Prosecutor General, may, by issuing a decision, order an operational surveillance.

Pursuant to Art. 2(1) of the Act on the National Tax Administration, the main tasks of the National Tax Administration in particular involve: 1) realisation of tax revenues, fees and non-tax receivables of the budget, as well as other

receivables, on the basis of separate regulations, with the exception of taxes and receivables of the budget for which other authorities are competent; 2) realisation of revenues from customs duties and other fees related to the import and export of goods; 3) realisation of customs policy resulting from membership in the customs union of the European Union; 4) recognition, detection and combating of fiscal offences and fiscal misdemeanours, prevention of these offences and prosecution of their perpetrators; 5) recognition, detection and combating of offences and misdemeanours related to the infringement of provisions on goods whose trade is subject to prohibitions or restrictions under provisions of Polish law, provisions of European Union law or international agreements, prevention of these offences and prosecution of their perpetrators, if they have been disclosed by the Customs and Fiscal Service; 6) disclosure and recovery of property threatened with forfeiture in connection with offences, or Art. 33 § 2 of the Fiscal Penal Code.

The Internal Supervision Bureau, headed by the Internal Supervision Inspector, was established by the Act of 9 November 2017 on amending the Act on certain rights of employees of the office serving the minister responsible for internal affairs as well as officers and employees of offices supervised by that minister and certain other acts, which amended the Act of 21 June 1996 on certain rights of employees of the office serving the minister responsible for internal affairs and officers and employees of offices supervised by that minister.

Pursuant to Art. 11a (1–3) (1) of the Act in question, the Internal Supervision Inspector is a body with the help of which the minister responsible for internal affairs supervises the services subordinate to him or supervised by him, over Police officers, Border Guard officers, State Protection Service officers and State Fire Service firefighters, as well as over the employees working in these services. The Internal Supervision Inspector is subordinate to the minister responsible for internal affairs.

The tasks of the Internal Supervision Inspector involve in particular: 1) support the minister responsible for internal affairs in activities related to the enforcement of actions in compliance with the law and principles of ethics in the Police, the Border Guard, the State Protection Service and the State Fire Service, in connection with the necessity to ensure the observance of human and civil rights and freedoms, as well as the disclosure of irregularities in this respect; 2) disclosure and monitoring of behaviours violating the principles of professional ethics of officers of the Police, the Border Guard and the State Protection Service as well as firefighters of the State Fire Service; 3) revealing and analysing irregularities occurring in connection with the conducted explanatory activities and disciplinary proceedings in the Police, the Border Guard, the State Protection Service and the State Fire Service; 4) analysing information on infringements of the law by supervised entities; 5) analysing and evaluating operational and

investigative activities conducted in the Police and the Border Guard and revealing irregularities in this area to the extent that this does not violate the competences of the prosecutor's office and the court; 6) recognition, prevention and detection of intentional offences and fiscal offences, prosecuted by public indictment, committed by officers of the Police, the Border Guard and the State Protection Service as well as firefighters of the State Fire Service, and also employees employed in these services.

In the course of performing operational and investigative activities undertaken by the Bureau in relation to Police officers, Border Guard and State Protection Service officers as well as State Fire Service firefighters and also employees of these services, in order to prevent, detect, determine perpetrators as well as obtain and record evidence of offences prosecuted by public indictment, intentional offences defined in the Art. 228 § 1 and 3-5 of the Criminal Code, Art. 229 § 1 and 3-5 of the Criminal Code, Art. 230 § 1 of the Criminal Code, Art. 230a § 1 of the Criminal Code, Art. 231 § 2 of the Criminal Code, Art. 245 of the Criminal Code, Art. 246 of the Criminal Code, Art. 258 of the Criminal Code, Art. 269 of the Criminal Code and Art. 299 § 1, 2, 5 and 6 of the Criminal Code, when other measures have proved to be ineffective or will be of no use, the District Court in Warsaw may, by issuing a decision, order an operational surveillance at a written request of the Internal Supervision Inspector submitted after obtaining the written consent of the Public Prosecutor General. The request is presented together with materials justifying the need to apply an operational surveillance.

The operational surveillance should be terminated immediately after the reasons for ordering it cease to exist, but at the latest at the end of the period for which it was introduced. The Internal Supervision Inspector informs the Public Prosecutor General on the results of the operational surveillance after its completion, and upon their request also on the course of the surveillance. In the event of obtaining evidence which makes it possible to initiate criminal proceedings or which is significant for the ongoing criminal proceedings, the Internal Supervision Inspector provides the Public Prosecutor General with all materials collected during the operational surveillance. The Internal Supervision Inspector is obliged to execute the order of the District Court in Warsaw to destroy materials, and to immediate, witnessed and recorded destruction of materials whose use in criminal proceedings is inadmissible. The Internal Supervision Inspector immediately notifies the Public Prosecutor General of the destruction of such materials. A person with regard to whom an operational surveillance was used, is not provided with access to materials collected during the operational surveillance.

In urgent cases, if this could result in the loss of information or the obliteration or destruction of evidence of an offence, all authorised services may order, after obtaining the written consent of the Public Prosecutor General, an operational surveillance, at the same time applying to the District Court for a decision in this matter.

If the court does not grant consent within 5 days from the date of ordering the operational surveillance, authorised bodies suspend the operational surveillance and carry out a recorded, witnessed destruction of materials collected during its application.

All entitled authorities should submit the request for ordering an operational surveillance together with materials (documentation of service activity and results obtained in the conducted case) justifying the need to apply an operational surveillance. The court may order the interception of communications for a period not longer than 3 months. However, the court at a written request of the authorised service filed after the written consent of the prosecutor may issue a decision to extend the operational surveillance for another 3 months. If, in justified cases, during the application of operational surveillance, new circumstances emerge that are important for the prevention or detection of an offence, or for the determination of perpetrators and obtaining evidence of an offence, the court, at a written request of an authorised law enforcement body submitted after written consent of the prosecutor, may again issue a decision on the extension of the operational surveillance for consecutive periods, none of which may last longer than 12 months.

The request for the court to order an operational surveillance should be drawn up by an authorised law enforcement authority, which should include in particular: 1) the case number and its code name, if it has been assigned; 2) a description of the offence with its legal qualification, if possible; 3) the circumstances justifying the need to apply operational surveillance, including the stated ineffectiveness or unsuitability of other measures; 4) details of the person or other details which allow to clearly determine the subject or object with regard to which the operational surveillance will be used, indicating the place or manner of its use; 5) the purpose, time and type of the operational surveillance conducted. Before issuing a decision, the court familiarises itself with the materials justifying the application, in particular with the materials collected during the operational surveillance ordered in this case.

The materials collected during the operational surveillance which do not contain evidence that allow to initiate criminal proceedings or evidence significant for the ongoing criminal proceedings will be subjected to immediate, recorded and witnessed destruction by the authorised law enforcement authority which requested for the ordering of the operational surveillance, of which it will immediately inform the prosecutor.

Conclusion

As an important means of gathering and detecting evidence and as an important means of preventing and combating crime, the use of wiretapping is indeed justified by the restrictions on freedom of communication and is in the public

interest[53]. The Constitutional Tribunal noted that with the growing importance of new technologies, the risk of their use to commit crimes and violate the law is also increasing, therefore entrusting specialised public authorities, such as special services and the police, with adequate powers will allow to prevent and detect crimes, prosecute their perpetrators, as well as provide information on threats to legally protected goods[54].

Evidence from wiretapping or operational surveillance is collected for use in criminal proceedings as a basis for establishing factual findings[55]. The basic condition for the admissibility of the use of evidence from recordings in criminal proceedings is that it must be obtained lawfully, which is a guarantee nature of compromise between the constitutionally protected secrecy of communications and the establishment of the truth in a criminal trial[56].

Procedural wiretapping and interception of communications are legal provided that they relate to the catalogue of offences listed therein and also in a situation in which the district court, under certain conditions and in compliance with certain procedures by the law enforcement authorities, consents to them[57]. The limits specified by the legislator defining the conditions of admissibility of ordering wiretapping exclude any derogation from this rule of law. Even the public interest cannot justify the violation of provisions regulating the search for and obtaining of evidence from telephone tapping, as this would nullify the constitutional protection of civil rights. In the Lublin Court of Appeal judgment it was held that declaring wiretapping illegal results in the fact that this evidence is no longer given and may not be used in proceedings, i.e. taken into consideration when sentencing, even despite the fact that during the trial the media containing the recording of the conversations conducted was played[58]. The Poznań Court of Appeal ruled similarly on the issue of evidence from wiretapping in civil cases. Secret recording of a private conversation violates the constitutional principle of freedom and protection of communication. Evidence of this kind obtained in an unlawful manner, even if its use is justified by reasons of national security, should not, as a rule, be admissible in proceedings[59].

---

[53] J. Machlańska, *Dowód z podsłuchu procesowego a ochrona tajemnicy obrończej*, "Palestra" 2016, No. 1–2, p. 17.

[54] See: wyrok TK z dnia 30 lipca 2014 r., sygn. K 23/11.

[55] A. Taracha, *Wykorzystanie informacji uzyskanych w wyniku czynności operacyjno-rozpoznawczych w procesie karnym* [in:] *Nowy kodeks postępowania karnego. Zagadnienia węzłowe*, ed. E. Skrętowicz, Kraków 1998, p. 180.

[56] Z. Kwiatkowski, *Zakazy dowodowe w procesie karnym*, Kraków 2005, p. 58.

[57] See: postanowienie SA w Krakowie z dnia 6 listopada 2007 r., sygn. II AKz 528/07; postanowienie SN (7) z dnia 26 kwietnia 2006 r., sygn. I KZP 6/07; wyrok SN z dnia 19 września 2000 r., sygn. V KKN 331/00; wyrok SN z dnia 3 grudnia 2008 r., sygn. V KK 195/08.

[58] See: wyrok SA w Lublinie z dnia 18 maja 2009 r., sygn. II AKa 122/08.

[59] See: wyrok SA w Poznaniu z dnia 10 stycznia 2008 r., sygn. I ACa 1057/07.

Analysing the scale of wiretapping used in Poland in the period from 2013 to 2022, it follows that courts ordered the monitoring and recording of conversations or operational surveillance against total of 58 487 persons and refused to order wiretapping against 223 persons. In addition, the courts in the period in question did not consent to operational surveillance against 1,518 persons. Since the beginning of its existence, the State Protection Service and the Internal Supervision Inspector have not yet submitted any request for ordering an operational surveillance[60].

Bibliography

Braciak J., *Prawo do prywatności*, Warszawa 2004.

Brylak-Hudyma K., *Konstytucyjne prawa i wolności w obliczu nowych systemów inwigilacji*, "Prawo Mediów Elektronicznych" 2020, No. 2.

Chałubińska-Jentkiewicz K., Nowikowska M., *Bezpieczeństwo, tożsamość, prywatność – aspekty prawne*, Warszawa 2020.

Chmielarz K., *Prawo do prywatności a bezpieczeństwo wewnętrzne państwa. Kontrola operacyjna i dane telekomunikacyjne w kontekście inwigilacji społeczeństwa*, Warszawa 2020.

Dudka K., *Kontrola korespondencji i podsłuch w polskim procesie karnym*, Lublin 1998.

Dudka K., *Podsłuch prywatny i dziennikarski a proces karny* [in:] *Problemy stosowania prawa sądowego. Księga ofiarowana Profesorowi Edwardowi Skrętowiczowi*, ed. I. Nowikowski, Lublin 2007.

Jasudowicz T., *Orzecznictwo strasburskie*, Warszawa 1998.

Konstytucja RP. Komentarz, Vol. I–II, eds. M. Safjan, L. Bosek, Warszawa 2016.

Kurzępa B., *Kontrola i utrwalanie rozmów telefonicznych według kodeksu postępowania karnego*, "Prokuratura i Prawo" 1999, No. 13.

Kwiatkowski Z., *Zakazy dowodowe w procesie karnym*, Kraków 2005.

Łebkowska J., *Bezpieczeństwo – teoretyczny wymiar ponadczasowej wartości*, "Przegląd Strategiczny" 2011, No. 1.

Machlańska J., *Dowód z podsłuchu procesowego a ochrona tajemnicy obrończej*, "Palestra" 2016, No. 1–2.

Mednis A., *Prawo do prywatności a interes publiczny*, Warszawa 2006.

Rogalski M., *Podsłuch procesowy i pozaprocesowy. Kontrola i utrwalanie rozmów na podstawie k.p.k. oraz ustaw szczególnych*, Warszawa 2016.

Sarnacki P., *Prawo do ochrony prywatności* [in:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, ed. L. Garlicki, Warszawa 2007.

Słoński J., *Kontrola operacyjna*, "Kwartalnik Prawno-Kryminalistyczny Szkoły Policji w Pile" 2011, No. 3–4.

Taracha A., *Wykorzystanie informacji uzyskanych w wyniku czynności operacyjno-rozpoznawczych w procesie karnym* [in:] *Nowy kodeks postępowania karnego. Zagadnienia węzłowe*, ed. E. Skrętowicz, Kraków 1998.

[60] See: open information sent from the Prosecutor General of the Republic of Poland to the Senate of the Republic of Poland.

Summary

The study presents an analysis the current legal regulations in the field of the procedural use of wiretapping and interception of communications by law enforcement agencies, which should respect the constitutional standards of the right to privacy, both the regulations contained in the Constitution of the Republic of Poland and the treaty rules of the European Union. The source of the study was the published and unpublished information obtained from government services and bodies, including the scale of the use of monitoring and recording of conversations, as well as the analysis of current legal regulations.

Keywords: procedural wiretapping, interception of communications, right to privacy

PODSŁUCH PROCESOWY I OPERACYJNY STOSOWANY W RZECZYPOSPOLITEJ POLSKIEJ W KONTEKŚCIE PRAWA DO PRYWATNOŚCI

Streszczenie

Opracowanie przedstawia analizę uregulowań prawnych w zakresie stosowania podsłuchu procesowego i podsłuchu operacyjnego przez organy ścigania, które winny przestrzegać zasad konstytucyjnych standardów prawa do prywatności, zawartych zarówno w Konstytucji Rzeczypospolitej Polskiej, jak i przepisach traktatowych Unii Europejskiej. Źródłem badań były uzyskane publikowane i niepublikowane informacje od służb i organów państwowych, zawierające skalę stosowania kontroli i utrwalenia rozmów, jak również analiza aktualnych przepisów prawa.

Słowa kluczowe: podsłuch procesowy, podsłuch operacyjny, prawo do prywatności