https://doi.org/10.31268/ZPBAS.2023.14 nr 1(77) 2023 ■ s. 254–260 ZESZYTY PRAWNICZE BAS Biura Analiz Sejmowych Kancelarii Sejmu

Szymon Kondej

Legal solutions regarding wiretapping (ECPRD Request No. 5334)[1]

Rozwiązania prawne dotyczące stosowania podsłuchu (wniosek ECPRD nr 5334)

The author analyses the provisions which regulate the use of wiretapping in the Polish legal order. He describes the legal solutions concerning the authorization of operational control, the methods of carrying it out and the limits of such control, as well as the legal usability of evidence obtained through wiretapping. The author also discusses the regulations on the methods of storage and subsequent destruction of evidence obtained in this form of operational control.

Keywords: wiretapping, operational control

Autor analizuje przepisy regulujące stosowanie podsłuchu w polskim porządku prawnym. Opisuje rozwiązania prawne dotyczące autoryzacji kontroli operacyjnej, metody jej przeprowadzenia oraz limity kontroli, a także prawne możliwości wykorzystania zdobytych w drodze podsłuchu dowodów. Autor omawia również regulacje dotyczące metod przechowywania i późniejszego zniszczenia dowodów zdobytych w tej formie kontroli operacyjnej.

Słowa kluczowe: podsłuch, kontrola operacyjna

Student ■
Uniwersytet Warszawski, Wydział Prawa i Administracji, WARSZAWA, POLSKA ■
s.kondej@student.uw.edu.pl ■ https://orcid.org/0009-0000-9317-527X

In response to ECPRD Request No. 5334 regarding "Request for information concerning wiretapping" the Bureau of Research provides the following information.

1. Is wiretapping a means of obtaining evidence?

Yes. According to the Article 168b of the Act of 6th June 1997 – Code of Criminal Procedure, the prosecutor should decide on the use of the evidence obtained as a result of operational control ordered at the request of an authorized body under special provisions. Also the Article 237 of the abovementioned Act states that after the initiation of proceedings, the court, at the request of the prosecutor, may order the inspection and recording of the contents of telephone conversations in

[1] *Request for information concerning wiretapping (ECPRD Request No. 5334)* prepared on February 17, 2023 as part of cooperation in The European Centre for Parliamentary Research and Documentation (Europejskie Centrum Badań Parlamentarnych i Dokumentacji); BAS-WAP-323/23.

order to detect and obtain evidence for ongoing proceedings or to prevent the commission of new crimes

It is more vague when the wiretapping is not conducted by the authorized body. The Article 168a stated that evidence cannot be declared inadmissible solely on the grounds that it was obtained in violation of the rules of procedure or by means of a criminal act unless the evidence was obtained in connection with the performance of official duties by a public official, as a result of: murder, wilful commission of a grievous bodily injury or deprivation of freedom. However evidence from illegal wiretapping conducted by normal citizens is not regulated. According to the judgement of the Supreme Court of 22nd April 2016[2], with such types of evidence, it is necessary to carry out an assessment: does the evidence violate the right to privacy and if it does, is it necessary to ensure another person's right to a fair trial.

2. How many types of wiretapping are provided for?

3. Which laws regulate wiretapping for the purposes of justice? (Please, indicate the legal references)

The wiretapping may be carried out as a part of operational and investigative activities or under covert operational control. Whenever I refer to operational control it also includes wiretapping. The operational control is conducted in secret and may consist in:

1) obtaining and recording the content of conversations conducted by technical means, including by means of telecommunications 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 by means of electronic communication,
4) obtaining and recording data contained in computer data carriers, telecommunication terminal equipment, information and data communication systems,
5) accessing and inspecting the contents of mail.

There is no single act regulating the wiretapping or operational control. The relevant regulations are scattered across a number of laws. They can be found in:

- Articles 168b, 218-218b and 237-242 of the Act of 6th June 1997 Code of Criminal Procedure[3],
- Articles 6, 21–22b and 27–29 of the Act of 24th May 2002 on the Internal Security Agency and the Foreign Intelligence Agency[4],

---

[2] Ii csk 478-15-1.pdf (sn.pl) (judgement in Polish) [available: 17.020.2023]. All references to online sources have the same access date.

[3] Https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19970890555 (legislation in Polish).

[4] Https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20020740676 (legislation in Polish).

- Articles 5, 6, 25–28, 29 and 31–32b of the Act of 9th June 2006 on the Military Counterintelligence Service and the Military Intelligence Agency[5],
- Article 9 of the Act of 10th June 2016 on anti-terrorist activities[6],
- Articles 14, 15 and 19 of the Act of 6th April 1990 on the Police[7],
- Articles 13, 14 and 17 of the Act of 9th June 2006 on the Central Anticorruption Bureau[8],
- Articles 4, 17 and 31 of the Act of 24th August 2001 on the Military Gendarmerie and military ordnance authorities[9],
- Articles 9 and 9e of the Act of 12th October 1990 on the Border Guard[10],
- Article 23p of the Act of 9th April 2010 on Prison Service[11] (this this provision has not yet entered into force, this will happen on 14th December 2022),
- Article 118 of the Act of 16th November 2016 on the National Revenue Administration[12],
- Article 19 of the Act of 8th December 2017 on the State Protection Service[13],
- Articles 11j, 11m, 11n, 11l. 11w of the Act of 21st June 1996 on Special Forms of Supervision by the Minister Responsible for Interior[14]

4. What are the conditions for interceptions and any limits to their usability? Can they be used in all criminal proceedings or only in proceedings relating to certain offences?

Please see answers to Question 1 and Question 12.

---

5 Https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20061040709 (legislation in Polish).

6 Https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20160000904 (legislation in Polish).

7 Https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19900300179 (legislation in Polish).

8 Https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20061040708 (legislation in Polish).

9 Https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20210001214 (legislation in Polish).

10 Https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19900780462 (legislation in Polish).

11 Https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20100790523 (legislation in Polish).

12 Https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20160001947 (legislation in Polish).

13 Https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180000138 (legislation in Polish).

14 Https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19961060491 (legislation in Polish).

5. Who authorises wiretapping? Who carries them out (the police? Private companies?)?

Operational control can be performed by Internal Security Agency, Foreign Intelligence Agency, Military Intelligence Agency, Military Counterintelligence Service, Central Anticorruption Bureau, Central Investigative Bureau of the Police, State Protection Service, Military Gendarmerie, Border Guard, Prison Guard, National Revenue Administration, Internal Oversight Office and the Police.

All these services may carry out operational control only when other measures have proved to be ineffective or useless and after obtaining the consent of the General Prosecutor (or the public prosecutor competent for the district when carrying out control by the police) and the relevant decision of the competent district court. The subject-matter scope of the control conducted also varies depending on the type of service conducting the control. In cases of urgency, a control may be initiated without the permission of the court, with a simultaneous application, and in the event that it would not be granted, the service shall suspend the control.

6. Is there a maximum duration for eavesdropping operations?

Yes. Article 238 § 1 of the Code of Criminal Procedure imposes a time limit and states that surveillance and telephone tapping may be imposed for a maximum period of three months, which may be extended in particularly justified cases for an additional period not exceeding three months. According to relevant acts, some services (Internal Security Agency, Central Anticorruption Bureau, Military Counterintelligence Service and Border Guard) can prolong the control for maximum 12 months with the approval of the General Prosecutor.

7. How is the material obtained through wiretapping stored? Is there an archive of wiretapped material? If yes, by whom is the archive managed? Who is responsible for the intercepted material stored in the archive?

8. How is the confidentiality of eavesdropping activities guaranteed? What instruments are envisaged to avoid "leaks"?

If materials collected during operational control allow to initiate criminal proceedings or are significant for the criminal proceedings, they are handed over to the prosecutor or the General Prosecutor. They should pass the evidence to the court, which shall rule on its admissibility.

The Article 238 § 3–5 of the Code of Criminal Proceeding states that the prosecutor shall request an application for the destruction of all records in whole or in part where they are not relevant to the proceedings. The court shall rule on the application at a sitting.

According to the Article 19 para 17 of the Act on the Police, materials collected during the operational control which do not contain evidence allowing for the initiation of criminal proceedings or evidence significant for the criminal

proceedings in progress shall be destroyed without delay, by means of a protocol and by a commission. Destruction of materials shall be ordered by the Police authority which applied for ordering operational control. Also the Article 19 para 15f–15h of the abovementioned Act states that materials containing information obtained through violation of attorney-client privilege, the secrecy of confession or professional secrecy have to be destroyed, unless using them is necessary for the good of justice and using other proofs is not possible.

Other state services that can perform operational control are also obligated to destroy without delay, by means of a protocol and by a commission, materials collected during the operational control which do not contain evidence allowing for the initiation of criminal proceedings or evidence significant for the criminal proceedings in progress. Destruction of materials shall be ordered by the authority which applied for the order of operational control. An exception is made by the Article 15f of the Act on the Internal Security Agency and the Foreign Intelligence Agency, which stipulates that in the case of operational control conducted by Internal Security Agency, the district court in Warsaw may decide, on the written motion of Head of the Internal Security Agency, to preserve operational control materials that are important for state security.

Detailed rules on the conduct of operational control, including the storing of the materials, are contained primarily in the Regulation of the Minister of Justice of 24th June 2003 on the Manner of Technical Preparation of Information Transfer Networks, for the Control of Information Transfers and the Manner of Making, Recording, Storing, Reproducing and Destroying Records of Controlled Transfers[15], and in the Regulation of the Minister of Interior and Administration of 8th July 2022 on Operational Control Conducted by the Police[16].

The storage and transmission of applications, orders and materials obtained during the application of controls, as well as the processing and destruction of these materials shall be carried out in such a way as to ensure that the information contained in the documents and materials is kept confidential and that unauthorized access to them is prevented.

9. Is the dissemination of footage, recordings or material obtained through wiretapping and not relevant to court proceedings punished?

According to the Article 267 of the Criminal Code[17], whoever, for the purpose of obtaining information to which he is not entitled, installs or uses an eavesdrop-

[15] Https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20031101052 (legislation in Polish).

[16] Https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20220001458 (legislation in Polish).

[17] Https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19970880553 (legislation in Polish).

ping, visual or other device or software, is subject to a fine, restriction of liberty or imprisonment for up to 2 years. The offence is prosecuted on application. Also in the event of dissemination of footage, recordings or material, civil action can be brought for violation of personal rights.

10. With regard to the use phase, who is responsible for the selection of the relevant recordings? What are the rules governing the use of material obtained through wiretapping and deemed irrelevant for trial purposes?

Please see answers to Question 1 and 8.

11. Is the use of computer capturing allowed? If yes, are specific rules provided for?

Yes. According to the Chapter 25 of the Code of Criminal Procedure, items (that includes computers) that may constitute evidence in the case should be handed over at the request of the court or prosecutor, and in urgent cases – also at the request of the Police or other authorized body.

12. Is the usability of wiretaps limited to the proceedings in which they are ordered? Or can they be used in other proceedings for the investigation of crimes?

Evidence obtained by means of operational control may relate to:

- offence committed by a person against whom the operational control was applied;
- other offense than the one covered by the operational control order;
- offense committed by a person other than the one covered by the operational control order;

The prosecutor shall decide on the use of this evidence in criminal proceedings.

Bibliography

Legal Acts

Ustawa z 6 kwietnia 1990 r. o Policji, t.j. Dz.U. 2023, poz. 171.

Ustawa z 12 października 1990 r. o Straży Granicznej, t.j. Dz.U. 2022, poz. 1061.

Ustawa z 21 czerwca 1996 r. o szczególnych formach sprawowania nadzoru przez ministra właściwego do spraw wewnętrznych, t.j. Dz.U. 2022, poz. 2487.

Ustawa z 6 czerwca 1997 r. – Kodeks karny, t.j. Dz.U. 2022, poz. 1138, ze zm.

Ustawa z 6 czerwca 1997 r. – Kodeks postępowania karnego, t.j. Dz.U. 2022, poz. 1375, ze zm.

Ustawa z 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych, t.j. Dz.U. 2021, poz. 1214.

Ustawa z 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, t.j. Dz.U. 2022, poz. 557.
Ustawa z 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym, t.j. Dz.U. 2022, poz. 1900.
Ustawa z 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, t.j. Dz.U. 2023, poz. 81.
Ustawa z 9 kwietnia 2010 r. o Służbie Więziennej, t.j. Dz.U. 2022, poz. 2470.
Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych, t.j. Dz.U. 2022, poz. 2632.
Ustawa z 16 listopada 2016 r. o Krajowej Administracji Skarbowej, t.j. Dz.U. 2023, poz. 615.
Ustawa z 8 grudnia 2017 r. o Służbie Ochrony Państwa, t.j. Dz.U. 2023, poz. 66.
Rozporządzenie Ministra Sprawiedliwości z 24 czerwca 2003 r. w sprawie sposobu technicznego przygotowania sieci służących do przekazywania informacji, do kontroli przekazów informacji oraz sposobu dokonywania, rejestracji, przechowywania, odtwarzania i niszczenia zapisów z kontrolowanych przekazów, Dz.U. nr 110, poz. 1052.
Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 8 lipca 2022 r. w sprawie kontroli operacyjnej prowadzonej przez Policję, Dz.U. poz. 1458.

Judicial Decisions

Wyrok Sądu Najwyższego z 22 kwietna 2016, sygn. akt II CSK 478/15.