Ius Novum
2/2016

COMMUNICATIONS INTERCEPTION AND OBTAINING TELECOMMUNICATIONS BILLINGS BY AUTHORISED ENTITIES WITHIN THEIR OPERATIONAL AND INTELLIGENCE ACTIVITIES IN POLAND

MACIEJ ROGALSKI

INTRODUCTION

The article focuses on the issue of communications interception and obtaining telecommunications billings by authorised entities, e.g. the Police, within their operational and surveillance activities. The regulations concerning communications interception and obtaining billings are laid down in a few statutes in Poland. Communications interception and obtaining billings for the needs of the criminal proceeding are regulated in Articles 218–218b CPC and Article 241 CPC. Apart from that, communications interception and obtaining billings are also admissible for the needs of the so-called authorised entities' operational and surveillance activities based on special acts. At present, there are eight such entities: Policja [the Police][1], Straż Graniczna [the Border Guard][2], the Fiscal Intelligence[3], Żandarmeria Wojskowa [the Military Police][4], Służba Kontrwywiadu Wojskowego [the Military Counterintelligence Service][5], Agencja Bez-

[1] Act of 6 April 1990 on the Police, Journal of Laws of 2015, item 355 with amendments that followed (Act on the Police) and Act of 10.

[2] Act on the Border Guard of 12 October 1990, Journal of Laws of 2014, item 1402 with amendments that followed (BG).

[3] Act of 28 September 1991 on fiscal control, Journal of Laws of 2015, item 553 with amendments that followed (FC).

[4] Act of 24 August 2001 on the Military Police and other military order organs, Journal of Laws of 2013, item 568 with amendments that followed (MP).

[5] Act of 9 June 2006 on the Military Counterintelligence Service and on the Military Intelligence Service of 10 January 2014, Journal of Laws of 2014, item 253 with amendments that followed (MCS and MIS).

pieczeństwa Wewnętrznego [the Internal Security Agency][6], Centralne Centralne Biuro Antykorupcyjne [Central Anticorruption Bureau][7] and the Customs Service[8]. The article does not thoroughly discuss the issue of recording telephone communication, i.e. the so-called tapping, and video and audio recording of persons in rooms, vehicles or places other than public ones[9].

OPERATIONAL AND SURVEILLANCE ACTIVITIES AND OPERATIONAL CONTROL

1. The concept of operational and surveillance activities first occurred in the Polish legislation in Act of 14 July 1983 on the Ministry of the Interior and the scope of operations of its organs[10]. In jurisprudence, operational and surveillance activities are described as a separate system of (authorised entities') low-key or secret activities conducted beyond the criminal process in order to prevent or combat crime and other legally determined negative social phenomena[11].

It is necessary to distinguish operational control within operational and surveillance activities, which is one of the forms of operational and surveillance activities. Operational control is secret and may be conducted by the eight above-mentioned authorised entities. Until recently, the Acts envisaged three types of operational control that each of the eight entities could perform. It could concern the control of the correspondence contents, the control of communications contents and the use of technical devices in order to

---

[6] Act of 24 May 2002 on the Internal Security Agency and on the Intelligence Agency of 22 October 2015, Journal of Laws of 2015, item 1929 with amendments that followed (ISA and IA).

[7] Act of 9 June 2006 on the Central Anticorruption Bureau, of 4 September 2014, Journal of Laws of 2014, item 1411 with amendments that followed (CAB).

[8] Act of 27 August 2009 on the Customs Service, Journal of Laws of 2009, no. 168, item 1323 with amendments that followed (CS).

[9] See J. Bratoszewski, L. Gardocki, Z. Gostyński, S. Przyjemski, R. Stefański, S. Zabłocki, *Kodeks postępowania karnego. Komentarz [Criminal Procedure Code]*, vol. I, Warszawa 2003, pp. 1017–1018; K. Marszał, Podsłuch w polskim procesie karnym de lege lata i de lege ferenda [Tapping in the Polish criminal process *de lege lata* and *de lege ferenda*], [in:] Problemy nauk penalnych. Prace ofiarowane Pani Profesor Oktawii Górniok [Penal science problems. Papers presented to Professor Oktawia Górniok], *Prace Naukowe Uniwersytetu Śląskiego*, Katowice 1996, no. 150, p. 343; T. Grzegorczyk, *Kodeks postępowania karnego. Komentarz [Criminal Procedure Code: Commentary]*, Zakamycze 2005, p. 590.

[10] Journal of Laws No. 38, item 172 with amendments. See A. Taracha, *Czynności operacyjno-rozpoznawcze. Aspekty kryminalistyczne i prawnopodatkowe [Operational and surveillance actions. Forensic science and tax law aspects]*, Lublin 2006, p. 12.

[11] See T. Hanausek, *Kryminalistyka. Zarys wykładu [Forensic science: lecture outline]*, Kraków 1996, p. 96; P. Chrzczonowicz, Społeczeństwo inwigilowane w państwie prawa [Society under surveillance in the rule of law state], [in:] P. Chrzczonowicz, V. Kwiatkowska-Darul, K. Skowroński (ed.), *Materiały z konferencji naukowej [Scientific conference papers]*, Toruń 2003, pp. 153–154. Also see W. Kozielewicz, Postępowanie w przedmiocie zarządzenia kontroli operacyjnej [Proceeding connected with ordering operational monitoring], [in:] L. Paprzycki, Z. Rau, *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu. Nowoczesne technologie i praca operacyjna [Practical elements of combating organised crime and terrorism. Modern technologies and operational work]*, Warszawa 2009, pp. 509–510; A. Sakowicz, *Opinia o projekcie ustawy o czynnościach operacyjno-rozpoznawczych [Opinion on the bill on operational and surveillance actions]*, the Sejm paper No. 353, www.sejm.gov.pl; D. Zalewski, A. Melezini, *Ustawa o kontroli skarbowej. Komentarz praktyczny [Act on anti-fraud control: Practical commentary]*, Warszawa 2015, Legalis, commentary on Article 36.

obtain information and evidence and record them, especially the contents of telephone conversations and other information transferred with the use of telecommunications networks. Act of 15 January 2016 amending Act on the Police and some other acts (Act of 15 January 2016)[12] extended the scope of control adding a new type in the form of "obtaining data contained in data storage devices, telecommunications network terminal equipment and IT and telecommunications systems".

2. There is an opinion in literature that operational control consisting in the use of technical devices is different from the control of the contents of correspondence. It is assumed that the control of correspondence includes only the interception of letters, postcards or other forms of information transfer with the use of traditional forms of communication[13]. However, it is necessary to adopt the broad concept of control of the contents of correspondence, i.e. covering not only interception of correspondence in the form of letters, postcards or other forms of transmitting information with the use of traditional forms of communication but also the control conducted with the use of technical measures[14]. It is not important in what form the contents are transferred, i.e. whether it is done on paper or in an electronic form. The way in which the control is performed is, in fact, of secondary importance from the technical point of view. As a result, it must be admitted that the "control of the contents of correspondence" as well as the "operational control of correspondence" means practically the same. In jurisprudence, a concept of an electronic document is used and it means a logically coherent piece of information processed in a computer system, or more broadly an IT system, i.e. for example a text, graphic or music file[15]. In the same way the scope is understood in Article 218 § 1 CPC. It is assumed that the provision is also applicable to the interception of correspondence sent by electronic mail[16].

---

[12] Journal of Laws of 2016, item 147.

[13] Compare J. Kudła, Wybrana problematyka czynności operacyjno-rozpoznawczych na tle uwag de lege ferenda projektu ustawy o czynnościach operacyjno-rozpoznawczych [Selected issues of operational and surveillance activities in the light of *de lege ferenda* bill on operational and surveillance activities], [in:] L. Paprzycki, Z. Rau (ed.), *Praktyczne elementy... [Practical elements...]*, *op. cit.*, p. 533; D. Szumiło-Kulczycka, *Czynności operacyjno-rozpoznawcze i ich relacje do procesu karnego [Operational and surveillance actions and their relation to the criminal process]*, Warszawa 2012, p. 162.

[14] See S. Dubisz (ed.), *Uniwersalny słownik języka polskiego [Universal dictionary of the Polish language]*, vol. 2, Warszawa 2003, p. 453; E. Sobol (ed.), *Słownik wyrazów obcych [Dictionary of foreign words]*, Warszawa 2002, p. 601. Also see I. Dobosz, *Tajemnica korespondencji jako dobro osobiste oraz jej ochrona w prawie cywilnym [Privacy of communication as publicity right and its protection in civil law]*, Kraków 1989, p. 17; T. Taras, O dopuszczalności i legalności podsłuchu telefonicznego [On admissibility and lawfulness of telephone tapping], *Annales UMCS*, section G, Lublin 1960, p. 51; K. Dudka, Zatrzymanie korespondencji w projekcie kodeksu postępowania karnego z 1995 r. na tle przepisów obowiązujących [Postal interception in the bill on criminal proceeding of 1995 in the light of binding regulations], *Prokuratura i Prawo* 1996, no. 4; K. Dudka, *Kontrola korespondencji i podsłuch w polskim procesie karnym [Interception of communication in the Polish criminal process]*, Lublin 1998, p. 10.

[15] See P. Ochman, Spór o pojęcie dokumentu w prawie karnym [Dispute over a concept of a document in criminal law], *Prokuratura i Prawo* 2009, no. 1, p. 33.

[16] See P. Hofmański, E. Sadzik, K. Zgryzek, *Kodeks postępowania karnego. Komentarz [Criminal Procedure Code: Commentary]*, vol. I, Warszawa 2011, pp. 1231–1232.

The Act of 15 January 2016 removes the former doubts in the discussed scope because it specifies operational control consisting in "obtaining and recording the contents of correspondence, including correspondence conducted with the use of electronic communication means" (see, for example, Article 19 (6.3) of Act on the Police amended by Act of 15 January 2016). Thus, the provision defines that it does not apply to correspondence in the paper form but also with the use of electronic communication means. Formerly, Article 19 (6.1) of Act on the Police referred to operational control in the form of "control of correspondence" but did not indicate the form of correspondence, which could raise doubts described above.

RULING OF THE CONSTITUTIONAL TRIBUNAL OF 30 JULY 2014, FILE NO. K 23/11

1. The practice of operational and surveillance activities that have been in use so far demonstrates numerous problems, including constitutional ones[17]. The Constitutional Tribunal issued many rulings concerning them. The key one is the ruling of 30 July 2014, K 23/11[18], in which the Constitutional Tribunal defines, inter alia, the conditions for admissibility of operational and surveillance activities. Taking into account the former judgements of the Constitutional Tribunal and the European Court of Human Rights as well as the Court of Justice of the European Union (ECJ) concerning provisions regulating secret ways of obtaining information about individuals by public authorities in a democratic state ruled by law, the Constitutional Tribunal determined in its ruling the minimum requirements that regulations limiting constitutional freedoms and rights must fulfil. The Constitutional Tribunal indicated, inter alia, that

– the collection, retention and processing of personal data, especially data concerning private matters, is admissible only based on a clear and precise statutory provision;
– it is absolutely necessary to precisely determine in an act which state organs are authorised to collect and process data on individuals, including the right to use operational and surveillance activities;
– an act must determine the conditions for secret obtaining information on persons that are only detection of serious crimes and preventing them; an act should indicate the types of such crimes;
– an act must determine categories of persons who may be subject to operational and surveillance activities;
– operational and surveillance activities should be a subsidiary means of obtaining information or evidence against individuals when it is not possible to obtain them in a different, less bothersome way;

---

[17] Compare the ruling of the Constitutional Tribunal of 12 December 2005, K 32/04, *Orzecznictwo Trybunału Konstytucyjnego – A* 2005, No. 11, item 132; Z. Rau, Czynności operacyjno-rozpoznawcze w polskim systemie prawa – działania w kierunku uniwersalnej ustawy [Operational and surveillance actions in the Polish legal system – steps towards a universal statute], [in:] L. Paprzycki, Z. Rau, *Praktyczne elementy... [Practical elements...]*, *op. cit*., p. 720.

[18] Journal of Laws of 2014, item 1055.

– an act should determine the maximum period of applying operational and surveillance methods towards an individual that cannot exceed the framework necessary in a democratic state ruled by law;
– it is absolutely necessary to precisely normalise in an act the procedure of taking a decision to launch operational and surveillance activities, especially including the requirement of obtaining an independent organ's consent to use secret methods of collecting information;
– it is necessary to determine in an act precise rules of dealing with the material collected in the course of operational and surveillance activities, especially the rules of using it and disposing of unnecessary and inadmissible data;
– it is necessary to inform individuals about a secret procedure of obtaining information on them, in a reasonable time after the end of the procedure and, on the interested person's motion, asking a court to examine and assess whether the activities were legal[19].

2. Checking the provisions regulating operational and surveillance activities and taking into account recommendations in the ruling of 30 July 2014, K 23/11, the Constitutional Tribunal stated, inter alia, discrepancies in the following provisions regulating operational and surveillance activities:
1) Article 27 (1) in connection with Article 5 (1.2.b) ISA and IA and Article 2, Article 47 and Article 49 in connection with Article 31 (3) of the Constitution;
2) Article 20c (1) of Act on the Police; Article 10b (1) BG; Article 36b (1.1) FC; Article 30 (1) MP; Article 28 (1. 1) ISA and IA; Article 32 (1.1) MCS and MIS; Article 18 (1.1) CAB; Article 75d (1) CS – because they do not envisage independent supervision of the provision of telecommunications data specified in Article 180c and Article 180d of Act of 16 July 2004 – Telecommunications law (TL)[20], are inconsistent with Article 47 and Article 49 in connection with Article 31 (3) of the Constitution;
3) Article 19 of Act on the Police; Article 9e BG; Article 36c FC; Article 31 MP; Article 27 ISA and IA; Article 31 MCS and MIS; Article 17 CAB – in the scope in which they do not envisage a guarantee of immediate, supervised by a commission and recorded disposal of materials containing information banned to be used as evidence, the secrecy of which has not been waived by a court or a waiver of which was not admissible, are in contradiction to Article 42 (2), Article 47, Article 49, Article 51 (2) and Article 54 (1) in connection with Article 31 (3) of the Constitution;
4) Article 28 ISA and IA; Article 32 MCS and MIS; Article 18 CAB – in the scope in which they do not envisage disposal of data that are of no significance for the proceeding, are in contradiction to Article 51 (2) in connection with Article 31 (3) of the Constitution;

---

[19] Ruling of the Constitutional Tribunal of 30 July 2014, K 23/11, Journal of Laws of 2014, item 1055; http://trybunal.gov.pl; *Legalis* no. 994752, part. III. 5.

[20] Journal of Laws of 2004, No. 171, item 1800 with amendments that followed.

5) Article 75d (5) CS in the scope in which it allows for the retention of the material other than the one containing information important for the proceeding in fraudulent misdemeanours or crimes specified in Chapter 9 of the Act of 10 September 1999 – Penal Fiscal Code (PFC)[21], is in contradiction to Article 51 (4) of the Constitution.

Re. 1. The provision of Article 27 (1) of Act on ISA and IA referred to Article 5 (1.2) of Act on ISA and IA. On the other hand, the provision of Article 5 (1.2.b) of Act on ISA and IA indicated crimes against the economic foundations of the state. The ruling of the Constitutional Tribunal of 30 July 2014, K 23/11, stated Article 27 (1) in connection with Article 5 (1.2.b) of Act on ISA and IA was in contradiction to Article 2, Article 47 and Article 49 in connection with Article 31 (3) of the Constitution of the Republic of Poland. In the reasons for the ruling, the Constitutional Tribunal indicated that neither the Criminal Code nor any other act uses a term "crimes against the economic foundations of the state", when referring to the names of particular forbidden acts, their defining elements or the titles of chapters on particular types of crimes. Due to the legislator's use of an unclear term, referring to undefined "crimes against the economic foundations of the state", real limits to secret interference into human freedoms and rights are not specified clearly enough and are determined by organs responsible for law application. In the Constitutional Tribunal's opinion, this state of things in is conflict with the constitutional principle of the specificity of legal provisions in the law-making process (Article 2 of the Constitution) and the principle of statutory forms of the limitation upon the exercise of constitutional freedoms and rights (Article 31 (3) of the Constitution)[22].

Implementing the ruling, the legislator gave Article 27 (1.2) of Act on the ISA and IA the following wording: "A court, on a written motion filed by the Head of the ISA, after having obtained the consent of the Attorney General in writing, may take a decision on ordering operational control – provided other measures proved to be inefficient or will be useless – in the course of performing operational and surveillance activities undertaken by the ISA in order to recognise, prevent and detect crimes specified in Chapters XXXV–XXXVII of the Criminal Code and Chapters 6 and 7 of the Penal Fiscal Code – if they are against the economic foundations of the state – and in order to obtain and record evidence of these crimes and pursue their perpetrators." The new wording of the provision eliminates previous reservations. Firstly, what the Constitutional Tribunal questioned, it does not refer to "crimes against the economic foundations of the state" in general but refers to specific decisions of the Criminal Code and Penal Fiscal Code. Secondly, it orders the application of the principle of subsidiarity. Operational control may be ordered only when other measures prove to be inefficient or are useless. "Other measures" should be understood as other forms of operational and surveillance activities that are not classified as operational control. "Inefficiency" means lack of expected results and "uselessness" – lack of possibility of obtaining expected results with the use of a particular measure. In literature, it is assumed that filing a motion to order operational control, an adequate organ must

[21] Journal of Laws of 2013, item 186, with amendments that followed.
[22] Journal of Laws of 2014, item 1055; http://trybunal.gov.pl; *Legalis* no. 994752, Part III.5.

prove inefficiency of former activities or present arguments for high probability of uselessness of traditional methods of criminal analysis[23]. Thirdly, it clearly indicates the aim of operational and surveillance activities undertaken by the ISA, i.e. recognition, prevention and detection of crime.

The adopted solutions are in accordance with the judgement of 8 April 2014 of the Court of Justice of the European Union, which in joined cases C293/12 and C594/12 (judgement of 8 April 2014 ECJ)[24] ruled Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC was invalid (Directive 2006/24/EC)[25]. Directive 2006/24/EC was implemented in the Polish law with the amendment of Telecommunications law of 24 April 2009[26]. The amendment imposed an obligation on telecommunications companies of retention and then – on request of authorised organs – provision of communications data laid down in Article 180c and Article 180d TL. Thus, it created legal framework for the authorised entities of access to these data. In the judgement of 8 April 2014, the ECJ indicated that Directive 2006/24/EC was limited to a general reference in Article 1 (1) to a concept of "serious crime" as defined by each Member State in its national law. The lack of a definition of "serious crime" in Directive 2006/24 causes that there is a clear borderline in which cases telecommunications data may be subject to retention and use.

Re. 2. According to the ruling of the Constitutional Tribunal of 30 July 2014, K 23/11, the provisions of Article 20c (1) of Act on the Police, Article 10b (1) BG; Article 36b (1.1) FC; Article 30 (1) MP; Article 28 (1.1) ISA and IA; Article 32 (1.1) MCS and MIS; Article 18 (1.1) CAB; Article 75d (1) CS – because they do not envisage independent supervision of communications data provision laid down in Article180c and Article 180d TL, were ruled to be in contradiction to Article 47 and Article 49 in connection with Article 31 (3) of the Constitution. In the reasons for this part of the ruling, the Constitutional Tribunal indicated that one of the requirements that statutory provisions entitling specified organs to obtain telecommunications data must meet is the creation of mechanisms of independent supervision. Since the collection of the data is secret, with no knowledge or will of the parties about which information is retained and with a limited social supervision, the lack of independent supervision of the state organs over the process poses a risk of misuse. It not only may contribute to unjustified interference into human freedoms and rights but also constitute threat for democratic mechanisms of power exercise. The obligation of statutory provision of procedural mechanisms preventing arbitrariness in obtaining telecommunications data is even

---

[23] See W. Kozielewicz, Postępowanie w przedmiocie zarządzenia kontroli operacyjnej [Proceeding connected with ordering operational monitoring], [in:] L. Paprzycki, Z. Rau, *Praktyczne elementy... [Practical elements...]*, *op. cit*., p. 511; ruling of the Constitutional Tribunal of 30 July 2014, K 23/11, Journal of Laws of 2014, item 1055; http://trybunal.gov.pl; *Legalis* no. 994752, Part III.6.

[24] Journal of Laws of 2014, L 105, p. 54.

[25] L 105/54 PL, Official Journal of the European Union of 13 April 2006.

[26] Act of 24 April 2009 amending the Act – Telecommunications law and some other acts, Journal of Laws of 2009, item 1445.

stronger because no provision has imposed an obligation to obtain a court's consent (or a consent of another organ independent of organs demanding the provision of these data or organs superior to them) to provide the authorised organs with the data specified in Article 180c and Article 180d TL. The procedure did not even require obtaining a public prosecutor's consent. The legislator did not also envisage major elements of control *ex post* legitimising undertaken activities. Thus, obtaining telecommunications data by the Police was under no control independent of the organ obtaining data[27].

Act of 15 January 2016 introduced a lot of changes in the acts regulating activities of entities authorised in the area. For example, Article 20c of Act on the Police questioned in the ruling of the Constitutional Tribunal was given new wording. But what is of key importance for the implementation of the ruling of the Constitutional Tribunal of 30 July 2014, K 23/11, are the provisions of Article 20ca of Act on the Police added after Article 20c: "Article 20ca (1) A regional court having jurisdiction over the area where the Police unit is based supervises telecommunications, postal or Internet data obtained by that Police unit. (2) The Police unit mentioned in (1), in compliance with the provisions on the protection of classified information, provides a court mentioned in (1) in half-year periods reports on:

1) the number of cases of obtaining telecommunications, postal and Internet data in the period covered by the report and the type of the data;
2) legal classification of forbidden acts in connection with which an organ requested telecommunications, postal or Internet data or information on obtaining data in order to save life or health of a person or back up search or rescue operations.
3) Within the supervision mentioned in (1), a regional court may get acquainted with the material giving grounds for the provision of telecommunications, postal or Internet data to the Police.
4) A regional court informs the Police unit about the outcome of the examination within 30 days after its completion.
5) Supervision mentioned in (1) is not applicable to obtaining data under Article 20cb (1)".

Thus, the provision of Article 20ca of Act on the Police introduces subsequent supervision that is an admissible solution from the point of view of constitutional norms. It should ensure the implementation of the constitutional principle of supervising public institutions' operations. The created mechanism should make it possible for services responsible for the state security and public order to efficiently combat threats. On the other hand, it created a system of supervision of obtaining communications, postal or Internet data by the Police. A regional court having jurisdiction over the area where the Police unit obtaining data is based was made responsible for the supervision. Court supervision meets the requirement of the supervisory organ's independence from the government. Police officers obtaining data are also not in direct or indirect subordination relation with that organ.

The adopted solution in the subsequent form, as it has already been indicated, is admissible from the point of view of the norms of the Constitution. The solution gives preference to activities of services responsible for the state security and public order.

[27] Journal of Laws of 2014, item 1055; http://trybunal.gov.pl; *Legalis* no. 994752, Part III.10.4.

However, a question is raised whether it would not be better, from the point of view of the protection of citizens' freedoms and rights but also taking into account the interests of the services, to adopt a solution ensuring prior supervision by a court. Subsequent supervision might be applied in cases when the Police or other services' activities were necessary without delay. Prior supervision would contribute to the improvement of appropriateness of the Police and other organs' motions as well as their number.

Secondly, a question is raised about the efficiency of the adopted solution in practice. In other words, to what extent will a court's supervision be real and not only nominal? It must be pointed out that data will be submitted to a court relatively rarely, in half-year periods. A regional court may, within its powers, get acquainted with the material justifying provision of telecommunications, postal and Internet data to the Police and as a result inform the Police about the examination outcome. After that, the activeness of a court in the process of verifying the appropriateness of data provision ends. There is no established procedure in case a court finds out that the provision of data violated binding regulations.

Thirdly, the introduction of the model of a court's prior supervision of potential access to telecommunications data would be conducive to real implementation of the principle of subsidiarity in obtaining data. The condition for access to data would be the exhaustion by the Police or other services of other legal measures that do not influence privacy or secrecy of communications.

The critical comments presented above find grounds in the judgement of 8 April 2014 of the ECJ. The Court stated that obtaining access to data by adequate state organs is not subject to prior supervision by a court or another independent administrative organ. A court or an independent administrative organ should supervise the provision and use of data so that it is limited to cases when it is absolutely necessary to meet a given objective[28]. Thus, the ECJ clearly speaks of prior supervision by an independent organ.

Re. 3. The Constitutional Tribunal, in its ruling of 30 July 2014, K 23/11, also stated that Article 19 of Act on the Police; Article 9e BG; Article 36c FC; Article 31 MP; Article 27 ISA and IA; Article 31 MCS and MIS; Article 17 CAB – in the scope of which they do not envisage ensuring immediate, supervised by a commission and recorded disposal of material containing information banned to be used as evidence, the secrecy of which has not been waived by a court or a waiver of which was not admissible – were in contradiction to Article 42 (2), Article 47, Article 49, Article 51 (2) and Article 54 (1) in connection with Article 31 (3) of the Constitution.

In the reasons for this part of the ruling, the Constitutional Tribunal indicated the lack of sufficient procedural guarantees of the protection of confidentiality of information passed to entities that are trusted because of their professional secrecy privilege. The regulations in question do not envisage – in a way that does not raise interpretational doubts – obligation of a court's prior supervision of data being collected or a possible waiver of professional secrecy privilege in a given case. The discussed

[28] Theses 60–62 of the judgement of 8 April 2014 of the Court of Justice of the European Union, Journal of Laws of 2014, L 105.

acts do not guarantee that in case of a justified suspicion that collected material contains information protected by the professional secrecy privilege, a court will perform additional verification of the material and possibly waive professional secrecy before the material is transferred to officers of the services or a public prosecutor. The questioned provisions do not also envisage a procedure of disposing of the information collected in the course of operational control that constitutes professional secrecy. In the Constitutional Tribunal's opinion, there is no interpretational doubt that these grounds cannot be derived from, inter alia, appropriately used Article 238 § 3–5 and Article 239 CPC. The Constitutional Tribunal presented especially negative assessment of the lack of adequate solutions concerning professional secrecy that, due to its significance for the materialisation of such values as the right to defence and the freedom of press, should be especially protected against disclosure of its contents to services making use of operational control[29].

Act of 15 January 2016 introduced necessary changes in acts the provisions of which were negated in the discussed scope. The provisions of Act on the Police may be an example. In accordance with the Bill, an addition of items 15f–15j was made after item 15e in Article 19.

Due to the contents of the ruling of the Constitutional Tribunal, the provisions of Article 15j of Act on the Police are important as they envisage an obligation to immediately and under the supervision of a commission dispose of the material the use of which is inadmissible in the criminal proceeding and record it. The Police unit was obliged to immediately inform a public prosecutor about the disposal of this material. In accordance with Article 19 (15j) of Act on the Police in the version after the amendment of 15 January 2016: "The Police unit is obliged to implement a court order on disposing of the material specified in Article 19 (15h) and to immediately, under the supervision of a commission dispose of the material the use of which is inadmissible in the criminal proceeding and record it. The Police unit immediately informs a public prosecutor specified in (15g) about the disposal of the material."

The solutions adopted in the Act of 15 January 2016 did not eliminate discrepancies in the norms regulating obtaining information in the course of operational and surveillance activities, *de lege lata* allowing for recording such communications that cannot be used as evidence in the criminal proceeding. The binding norms having guarantee features that are envisaged in the provisions of the CPC with regard to professional secrecy are becoming seeming ones because, despite the ban on introducing material being professional secrecy to the criminal proceeding, the legislator – although indirectly, through ambiguous statutory regulation – allows for its collection and retention by services authorised to apply operational control. It is especially visible in the area of the protection of the professional secrecy privilege of defence attorneys and journalists, which – under the CPC – are subject to unconditional legal protection and evidentiary ban that cannot be waived[30].

The presented issue was also noticed in the judgement of 8 April 2014 of the ECJ. The Court stated that Directive 2006/24/EC applies to all persons using electronic

---

[29] Journal of Laws of 2014, item 1055; http://trybunal.gov.pl; *Legalis* no. 994752, Part III.11.8.
[30] *Ibid*.

communications services whose data are retained. It refers even to those persons towards whom there are no grounds whatsoever, factual or legal, to initiate the criminal proceeding. The Directive does not envisage any exceptions. This means that it is also applied to persons whose communications and information obtained during these communications are subject to professional secrecy privilege under national law[31].

Re. 4. The ruling of the Constitutional Tribunal of 30 July 2014, K 23/11, states that the provisions of Article 32 MCS and MIS, and Article 18 CAB – in the scope in which they envisage disposal of the data that are insignificant for the conducted proceeding – were in contradiction to Article 51 (2) in connection with Article 31 (3) of the Constitution. In the formerly binding provisions, there were no procedures for verification and disposal of insignificant data, i.e. useless for further proceeding. In accordance with Article 51 (2) of the Constitution, public authorities shall not acquire, retain and make accessible information on citizens other than that which is necessary in a democratic state ruled by law. The assessment of necessity should be conducted taking into account the principle of proportionality resulting from Article 31 (3) of the Constitution. In its judgements, the Constitutional Tribunal explained the concept of "data necessary in a democratic state", indicating that "in a democratic state ruled by law it is not necessary to retain information on citizens obtained in the course of operational activities because of potential usefulness of this information. It can be applied only in connection with a given proceeding conducted based on a statute allowing for limitation of freedoms because of security of the state and public order". The condition for secret acquisition of information on individuals, including their telecommunications data, is establishment of a procedure of immediate selection and disposal of unnecessary and inadmissible material. This solution prevents unauthorised use of legally collected information by the state organs and its retention just in case it is useful for other purposes in the future[32].

Act of 15 January 2016, implementing the ruling of the Constitutional Tribunal, introduced adequate changes to the provisions of acts that were negated in the discussed scope. The provision of Article 28 (7) ISA and IA is an example. In accordance with the provision, data that are insignificant for the criminal proceeding or are not significant for security of the state must be immediately, under the supervision of a commission disposed of and the disposal must be recorded.

Re. 5. The ruling of the Constitutional Tribunal of 30 July 2014, K 23/11, stated that the provision of Article 75d (5) CS in the scope in which it allows for retention of material other than that containing information significant for a proceeding in fiscal misdemeanours or crimes specified in Chapter 9 of Act of 10 September 1999 – Penal Fiscal Code (FCC)[33] was in contradiction to Article 51 (4) of the Constitution.

The questioned provision read as follows: "Material obtained in the course of activities undertaken based on Article 75d (2) CS that do not contain information significant for a proceeding connected with fiscal misdemeanours or crimes must be

---

[31] Theses 57–58 of the judgement of 8 April 2014 of the Court of Justice of the European Union, Journal of Laws of 2014, L 105.

[32] Journal of Laws of 2014, item 1055; http://trybunal.gov.pl; *Legalis* no. 994752, Part III.12.2.

[33] Journal of Laws of 2013, item 186, with amendments.

immediately and under the supervision of a commission disposed of and the disposal must be recorded." In the reasons for the ruling, the Constitutional Tribunal indicated that although the provision of Article 75d (5) CS obliges the Customs Service to dispose of telecommunications data that are insignificant for a proceeding conducted by the Customs Service, it specifies the conditions for retention of the material in a too broad way. Material that is subject to disposal is only the one that does not contain information significant for a proceeding in fiscal misdemeanours or crimes[34].

Act of 15 January 2016 in Article 75d (6) stipulates that "telecommunications or Internet data that are insignificant for criminal or penal fiscal proceeding shall be immediately, under the supervision of a commission disposed of and the disposal must be recorded". The provision of Article 75d (6) of the Bill, compared to the former Article 75d (5) CS, from the point of view of the issue of the scope of collected data, has not been substantially changed. The Constitutional Tribunal pointed out in the reasons for its ruling that correct interpretation of Article 75d (5) CS, from constitutional perspective, does not give grounds for giving it such a broad content as the legislator did. The provision regulating conditions for collecting data (5) is contained in the same editorial unit as the provision regulating the aim of their collection (1). Thus, both provisions should be interpreted collectively. Then, the understanding of the questioned provision will be limited only to fiscal misdemeanours and crimes laid down in Chapter 9 PFC to which Article 75d (1) CS refers[35].

3. Act of 15 January 2016 not only introduced changes resulting from the ruling of 30 July 2014, K 23/11, but in addition it broadened the competence of entities authorised to conduct operational control. Article 19 (6) of Act on the Police can be an example. In accordance with the former wording of the provision, operational control included:

1) controlling correspondence contents;
2) controlling communications contents;
3) using technical means making it possible to acquire information and evidence in a secret way and record them, especially the contents of telephone conversations and other information transferred with the use of telecommunications networks.

In accordance with the new wording of Article 19 (4) of Act on the Police, operational control may also consist in "acquiring and recording data contained in data storage devices, telecommunications network terminal equipment, IT systems as well as information and communications technology systems". Article 19 (6.2) of Act on the Police clearly indicates that operational control also includes "acquiring and video and audio recording of persons in rooms, vehicles and places other than public ones". It is worth drawing attention to broadening operational control by adding acquiring and recording data contained in "telecommunications network terminal equipment". In accordance with Article 2 (43) TL, telecommunications network terminal equipment means "telecommunications equipment for direct or indirect connection to the end

[34] Journal of Laws of 2014, item 1055; http://trybunal.gov.pl; *Legalis* no. 994752, Part III.12.4.
[35] *Ibid*.

of the network". In other words, it is simply a telephone. Taking into account how technologically sophisticated they are, especially mobile handsets, and how many functions they have, operational control will mean access to an enormous amount of information (emails, short messages, personal data, files etc.).

4. It can be observed that there is a big difference between the provisions of the CPC and the provisions of special acts with regard to collecting and making data accessible. In case of the CPC, there are two basic groups of provisions regulating the issues: controlling and recording conversations (Article 237 and the following CPC) and provision of correspondence, communications and billings (Article 218–218b CPC). For example, the construction of operational control laid down in Article 19 (6.4) of Act on the Police adopted in Act of 15 January 2016 blurs these differences. Access to telephones means the ability of controlling a conversation conducted e.g. with the use of the short messaging system. Another example of different provisions of the CPC and special acts may be the provisions regulating the time limit for operational control and tapping. For example, in the former Article 19 (9) of Act on the Police, there was a possibility of prolonging the total length of control to a total of six months (Article 19 (8) of Act on the Police) but with no indication of a maximum period for which operational control can be prolonged next time. In the new Article 19 (9) of Act on the Police, it is specified that the decision on prolonging operational control may be issued for the subsequent periods that can total no longer than 12 months. Thus, the 12-month period of operational control is inconsistent with Article 238 § 1 CPC, which envisages controlling and recording telephone communications for a period of three months and its possible extension for the maximum of another three months, i.e. a total of six months.

CONCLUSIONS

Act of 15 January 2016 substantially amended acts regulating operation of entities authorised to conduct operational and surveillance activities. The changes were mainly the implementation of the ruling of the Constitutional Tribunal of 30 July 2014, K 23/11. In this scope, the changes should be assessed positively. However, not all the amendments implement postulations suggested earlier. A court's subsequent supervision of acquired data can be an example. The adoption of the principle of subsequent supervision as well as the lack of detailed regulations of the procedure in case of violation of law may cause that the supervision will become seeming. There was no attempt to develop solutions envisaging subsequent supervision in urgent situations and prior supervision as a rule.

It must be also highlighted that Act of 15 January 2016 introducing changes extended the powers of services in the field of acquiring new data and information. The extension of operational control by adding access to data in telephones is an example of that.

Act of 15 January 2016 did not introduce at least partial or differentiated, depending on the size of entity obliged to provide data, charges for the entities providing data. Introduction of even symbolic fees would certainly increase the level of conscientiousness in paying attention to the quantity of requested data and their types. In Poland, a big number of data demanded by authorised entities is still a serious problem.

The changes introduced to special acts deepen the differences between these regulations and analogous solutions in the CPC. The examples of that may be the scope of operational control that, apart from provision of correspondence, communications and telephone billings, envisages acquiring and recording data contained in data storage devices and telecommunications networks terminal equipment, IT as well as information and communications technology systems, or a period of control and recording conversations laid down in the CPC and operational control laid down in special acts.

BIBLIOGRAPHY

Bratoszewski J., Gardocki L., Gostyński Z., Przyjemski S., Stefański R., Zabłocki S., *Kodeks postępowania karnego. Komentarz [Criminal Procedure Code: Commentray]*, vol. I, Warszawa 2003.

Chrzczonowicz P., Społeczeństwo inwigilowane w państwie prawa [Society under surveillance in the rule of law state], [in:] Chrzczonowicz P., Kwiatkowska-Darul V., Skowroński K. (ed.), *Materiały z konferencji naukowej [Scientific conference papers]*, Toruń 2003.

Dobosz I., *Tajemnica korespondencji jako dobro osobiste oraz jej ochrona w prawie cywilnym [Privacy of communication as publicity right and its protection in civil law]*, Kraków 1989.

Dubisz S. red. *Uniwersalny słownik języka polskiego [Universal dictionary of the Polish language]*, vol. 2, Warszawa 2003.

Dudka K., Zatrzymanie korespondencji w projekcie kodeksu postępowania karnego z 1995 r. na tle przepisów obowiązujących [Postal interception in the bill on criminal proceeding of 1995 in the light of binding regulations], *Prokuratura i Prawo* 1996, no. 4.

Dudka K., *Kontrola korespondencji i podsłuch w polskim procesie karnym [Interception of communication in the Polish criminal process]*, Lublin 1998.

Grzegorczyk T., *Kodeks postępowania karnego. Komentarz [Criminal Procedure Code: Commentary]*, Zakamycze 2005.

Hanausek T., *Kryminalistyka. Zarys wykładu [Forensic science: lecture outline]*, Kraków 1996.

Hofmański P., Sadzik E., Zgryzek K., *Kodeks postępowania karnego. Komentarz [Criminal Procedure Code: Commentary]*, vol. I, Warszawa 2011.

Kozielewicz W., Postępowanie w przedmiocie zarządzenia kontroli operacyjnej [Proceeding connected with ordering operational monitoring], [in:] Paprzycki L., Rau Z., *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu. Nowoczesne technologie i praca operacyjna [Practical elements of the fight against organised crime and terrorism: modern technologies and operational methods]*, Warszawa 2009.

Kudła J., Wybrana problematyka czynności operacyjno-rozpoznawczych na tle uwag de lege ferenda projektu ustawy o czynnościach operacyjno-rozpoznawczych [Selected issues of operational and surveillance activities in the light of *de lege ferenda* bill on operational and surveillance activities], [in:] *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu. Nowoczesne technologie i praca operacyjna [Practical elements of the fight against organised crime and terrorism: modern technologies and operational methods]*, (ed.) Paprzycki L., Rau Z., Warszawa 2009.

Marszał K.: Podsłuch w polskim procesie karnym *de lege lata* i *de lege ferenda* [Tapping in the Polish criminal process *de lege lata* and *de lege ferenda*], [in:] Problemy nauk penalnych. Prace ofiarowane Pani Profesor Oktawii Górniok [Penal science problems. Papers presented

to Professor Oktawia Górniok], *Prace Naukowe Uniwersytetu Śląskiego*, Katowice 1996, no. 150.

Ochman P., Spór o pojęcie dokumentu w prawie karnym [Dispute over a concept of a document in criminal law], *Prokuratura i Prawo* 2009, no. 1.

Rau Z., Czynności operacyjno-rozpoznawcze w polskim systemie prawa – działania w kierunku uniwersalnej ustawy [Operational and surveillance actions in the Polish legal system – steps towards a universal statute], [in:] Paprzycki L., Rau Z., *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu. Nowoczesne technologie i praca operacyjna [Practical elements of combating organised crime and terrorism. Modern technologies and operational work]*, Warszawa 2009.

Sakowicz A., *Opinia o projekcie ustawy o czynnościach operacyjno-rozpoznawczych [Opinion on the bill on operational and surveillance actions]*, the Sejm paper No. 353, www.sejm.gov.pl.

Sobol E. (ed.), *Słownik wyrazów obcych [Dictionary of foreign words]*, Warszawa 2002.

Szumiło-Kulczycka D., *Czynności operacyjno-rozpoznawcze i ich relacje do procesu karnego [Operational and surveillance actions and their relation to the criminal process]*, Warszawa 2012.

Taracha A., *Czynności operacyjno-rozpoznawcze. Aspekty kryminalistyczne i prawnopodatkowe [Operational and surveillance actions. Forensic science and tax law aspects]*, Lublin 2006.

Taras T., *O dopuszczalności i legalności podsłuchu telefonicznego [On admissibility and lawfulness of telephone tapping]*, Annales UMCS, section G, Lublin 1960.

Zalewski D., Melezini A., *Ustawa o kontroli skarbowej. Komentarz praktyczny [Act on fiscal control]*, Warszawa 2015, Legalis, a commentary on Article 36.

COMMUNICATIONS INTERCEPTION AND OBTAINING TELECOMMUNICATIONS BILLINGS BY AUTHORISED ENTITIES WITHIN THEIR OPERATIONAL AND INTELLIGENCE ACTIVITIES IN POLAND

Summary

The article focuses on the issue of communications interception and obtaining telecommunications billings by authorised entities, e.g. the Police, within their operational and surveillance activities. In Poland, apart from courts and the prosecution service, these entities are authorised to collect this information. Their entitlements are laid down in statutes regulating their functioning. The Constitutional Tribunal of the Republic of Poland in its ruling of 30 July 2014, K 23/11, stated that a series of provisions regulating operational and surveillance activities are in contradiction to the Constitution. The amendments to these acts take into account the ruling of the Constitutional Tribunal. The article discusses the changes and presents the new solutions.

Key words: *operational and surveillance activities*, *operational control*, *authorised entities*, *correspondence*, *communications*, *telecommunications billings*

POZYSKIWANIE KORESPONDENCJI, PRZESYŁEK I WYKAZU POŁĄCZEŃ W RAMACH CZYNNOŚCI OPERACYJNO-ROZPOZNAWCZYCH UPRAWNIONYCH PODMIOTÓW W POLSCE

Streszczenie

Przedmiotem artykułu jest problematyka pozyskiwania przez tzw. uprawnione podmioty, np. Policję, w ramach czynności operacyjno-rozpoznawczych, korespondencji, przesyłek i wykazu połączeń. W Polsce, poza sądami i prokuraturą, podmioty te są uprawnione do pozyskiwania tego rodzaju informacji. Uprawnienia wskazanych podmiotów są przewidziane w ustawach szczególnych, które regulują ich działalność. W wyroku z dnia 30 lipca 2014 r., sygn. K 23/11, polski Trybunał Konstytucyjny stwierdził niezgodność szeregu przepisów regulujących czynności operacyjno-rozpoznawcze z postanowieniami polskiej Konstytucji. Nowela ustaw regulujących te uprawnienia uwzględnia wyrok Trybunału Konstytucyjnego. Artykuł omawia zmiany i przedstawia nowe uregulowania w tym zakresie.

Słowa kluczowe: *czynności operacyjno-rozpoznawcze*, *kontrola operacyjna*, *uprawnione podmioty*, *korespondencja*, *przesyłki*, *wykaz połączeń telekomunikacyjnych*