Law Review ● vol. VI, issue 2, July-December 2016, p. 3-21

STUDIES, DISCUSSIONS, COMMENTS

LEGAL REGULATIONS FOR THE COLLECTION AND SHARING OF DATA TELECOMMUNICATIONS IN POLAND

Maciej ROGALSKI[*]
Associate Professor
Łazarski University in Warsaw, Poland

Abstract

The article is an analysis of the legal provisions of the Code of Criminal Procedure, special Acts and the Telecommunications Law regulates the collection and sharing of telecommunication data in Poland. Analysis of regulations is carried out taking into account the judgment of the Polish Constitutional Court ("TK") of 30 July 2014., Ref. K 23/11 and the judgment of the Court of Justice of the European Union ("CJEU") of 8 April 2014. The enforcement of Constitutional Court's judgment of 30 July 2014 led to the adoption of the Law of 15 January 2016 amending the Acts governing the activities of authorized entities. These studies are related to the project, whose founder is the National Science Centre in Poland, in the competition Opus (registration number of the project 2015/17/B/HS5/00472).

Keywords: *collecting and providing telecommunications data; operational activities; telecommunication connections; a list of connections; transfer of information.*

Introduction

1. The article is about of gathering and sharing of telecommunications data. Polish law issues related to the collection and sharing of the calls are regulated in several legal acts. Issue the call for the purpose of criminal proceedings is governed by articles 218-218b Code of Criminal Procedure ("k.p.k.") and art. 241 k.p.k. Apart from issuing the calls for the purpose of criminal proceedings, under Polish law, a list of connections can also be made available under the so-called operational activities carried out under special laws by the so-called "eligible entities". Currently

[*] *E-mail:* maciej@rogalski.waw.pl.

in Poland there are eight such bodies: Police[1], Border Guard[2], the tax intelligence[3], Military Police[4], Military Counter-intelligence Service[5], the Internal Security Agency[6], Central Anti-Corruption Bureau[7] and the Customs Service[8]. Finally, the provisions of the Telecommunications Law determine the type and scope of data shared telecommunications (art. 180c and 180d of the Act of 16 July 2004. - Telecommunications Law ("P. T.") [9]) and the obligations of telecommunication companies in this area (art. 179 et seq P. T.). Due to the size of the development, the study will not be implementing acts to the Telecommunications Law, regulating the issues discussed: decree of the Council of Ministers dated 20 January 2012 on the technical and operational requirements for interfaces to perform the tasks and responsibilities of the national defense, state security and public safety and order[10] and regulation of Minister of Infrastructure dated 28 December 2009 on the detailed list of data types and operators of public telecommunications networks or providers of public telecommunications services obliged to their retention and storage[11].

1. The rules of the Code of Criminal Procedure - data acquisition by the courts and the prosecutor's office

1.1. Previous use regulations in Poland regarding the collection and sharing of telecommunications data revealed a number of problems. The first will be presented the most important issues related to the application of the provisions k.p.k. and relevant regulations provided in special acts and in telecommunications law.

According to the art. 218 § 1 of the Code of Criminal Procedure, offices, institutions and entities operating in the field of mail or telecommunications business, customs offices and institutions and transport companies are obliged to

[1] The Act of 6 April 1990 Police, Official Gazette ("Dz. U.") of 2015, item 355, as amended ("the Police Act").

[2] The Act on the Border Guard on 12 October 1990, Dz. U. of 2014, item 1402, as amended ("SG").

[3] The Act of 28 September 1991 on fiscal control, consolidated text ("tj.") Dz. U. of 2015, item 553, as amended ("KS").

[4] The Act of 24 August 2001 on Military Police and military law enforcement bodies, tj. Dz. U. of 2013, item 568, as amended ("ŻW").

[5] The Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service, tj. 10 January 2014, Dz. U. of 2014, item 253, as amended ("SKW and SWW").

[6] The Act of 24 May 2002 on the Agency of Internal Security and Intelligence Agency, tj. 22 October 2015, Dz. U. of 2015, item 1929, as amended ("ABW and AW").

[7] The Act of 9 June 2006 on the Central Anti-Corruption Bureau, tj. 4 September 2014, Dz. U. of 2014, item 1411, as amended ("CBA").

[8] The Act of 27 August 2009 Customs Service, Dz. U. of 2009., No. 168, item 1323, as amended, ("SC").

[9] Dz. U. of 2004, item 1800 as amended

[10] Dz. U. of 2012, item 200.

[11] Dz. U. of 2009, No. 226, item 1828.

give the court or the prosecutor, at the request contained in the order, correspondence and parcels and the data referred to in article 180c and 180d P. T., if relevant for the proceedings. Only the court or the prosecutor are entitled to them or to open them. According whereas art. 218 § 2-3 k.p.k. indicated decision, delivered to the addressees correspondence and telephone subscriber or broadcaster, whose list of calls or other communications information was released. Delivering a decision may be postponed for a period of time, which is necessary for the good things, but not later than until the final completion of the proceedings. Devoid of significance for criminal proceedings correspondence and parcels must be returned immediately to the competent authorities, institutions or the aforementioned companies.

The provision of art. 218 § 1 k.p.k. therefore imposes on operators of telecommunications activities required to deliver to the court or the prosecutor, at the request contained in the order data, referred to in art. 180c and 180d P.T., if they are relevant for the proceedings. In practice, the basis for a decision requiring them to be issued in the fact that telecommunications data may be relevant to the proceedings[12]. The provision of art. 180d P. T. itself does not specify the directory data to be available. It refers to other provisions of article 159 para. 1 point 1 and 3-5, art. 161 and art. 179 paragraph 9 P. T. The legislator has applied so here reference design consisting of second degree as static. This kind of legislative structure should be used with extreme caution in the event that regulates the interference of public authorities in the legal status of the individual.

Acquiring the list of telecommunication connections or other communications information, including correspondence sent by electronic mail in the ground in the criminal process, thus defines art. 218 k.p.k. While the obtained data contained in the information systems and media, including correspondence sent by e-mail provided by art. 236a k.p.k.[13]

1.2. The provisions of k.p.k. for the availability of telecommunications data (art. 218 § 1 k.p.k.), do not provide for the principle of subsidiarity. As part of the so conducted criminal proceedings – both in the *in rem* and in phase *in personam* – entities conducting appropriate activities, in particular telecommunications activities are obliged to give the court or the prosecutor, at the request contained in the order, correspondence and parcels and data referred to in art. 180c and art. 180d P.T., if such data are relevant for the proceedings (art. 218 § 1 k.p.k.). These entities are required in each case for the implementation of the obligation to provide the information as soon as it is requested by authorized entities, and not only when it is necessary. This effectively leads to a very large number of requests submitted. Meanwhile, the secret gathering of information about individuals in the course of action should be the center of the subsidiary, which is used when other

[12] P. Hofmański, E. Sadzik, K. Zgryzek, *Kodeks postępowania karnego. Komentarz*, Volume I, Warszawa 2011, p. 1233.

[13] T. Grzegorczyk, *Kodeks postępowania karnego. Komentarz*, Zakamycze 2005, p. 590.

solutions are unsuitable or ineffective. Implicit interference with the freedom and rights, is to be the *ultima ratio*[14]. It should be noted that in the case of operational control of the force, however, the principle of subsidiarity. Operational control can be ordered only when other measures have proved ineffective or are unsuitable[15].

1.3. An important issue is the protection of professional secrecy in the collection and sharing of data communications. In terms of the mystery of his own defense, the Supreme Court ("SN") formed the view that the defender remains outside the circle of entities to which is permitted to control and consolidate the talks[16]. According to this view, it is unacceptable to use – as evidence in criminal proceedings – secret information in his own defense, because it would circumvent the unconditional prohibition of evidence included in art. 178 point 1 k.p.k. This position has been formulated on the basis of regulations k.p.k. regulating the so-called eavesdropping process[17]. This view is valid in relation to other trade secrets. Rightly points out, however, that the current normalization of a guarantee, which provide rules k.p.k. in relation to professional secrecy, may prove to be illusory. Despite the fact the general ban on the introduction of content is a professional secret to a criminal trial as evidence in the case, the legislator permits – even indirectly, by the ambiguous statutory regulation – to the collection and storage by the departments authorized to use operational control[18].

In the jurisprudence of the Constitutional Court and the European Court of Human Rights ("ECHR") has repeatedly pointed out that for effective use of the assistance of a lawyer is necessary to preserve the confidentiality of messages transmitted by the defenders of the accused (suspect) [19]. No possibility of the confidential communication of the accused with his protector, also via telecommunication technology, means that legal aid loses much of its effectiveness[20]. Aptly pointed out also that ensuring the confidentiality of the discussions with counsel of the accused is necessary not only at the stage of court proceedings, but at any stage of the proceedings, even by a body extrajudicial (the

[14] See TK judgment of 30 July 2014., Ref. K 23/11, Orzecznictwo Trybunału Konstytucyjnego Zbiór Urzędowy ("OTK ZU") 2014, No. 7, pos. 180.

[15] See W. Kozielewicz, *Postępowanie w przedmiocie zarządzenia kontroli operacyjnej*, [in] L. Paprzycki, Z. Rau, *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu. Nowoczesne technologie i praca operacyjna*, Warszawa 2009, p. 511; Constitutional Court's judgment of 30 July 2014, Ref. K 23/11, Dz. U. of 2014, item 1055; http://trybunal.gov.pl; Legalis No. 994752, part III, point 6.

[16] See Supreme Court ruling of 26 October 2011., Ref. I KZP 12/11, Orzecznictwo Sądu Najwyższego Izba Karna i Wojskowa („OSNKW") 2011, No. 10, item 90.

[17] See Constitutional Court's judgment of 22 November 2004, Ref. SK 64/03, OTK ZU 2004, No 10/A, item 107, part III, point 3.

[18] See Constitutional Court's judgment of 30 July 2014, Ref. K 23/11, OTK ZU 2014, No. 7, item 180.

[19] See Constitutional Court's judgment of 11 December 2012, Ref. K 37/11, OTK ZU 2012, No. 11/A, item 133, part III, point 3, and case-law cited TK and the ECHR.

[20] Constitutional Court's judgment of 30 July 2014, Ref. K 23/11, OTK ZU 2014, No. 7, item 180.

prosecutor, the police, state security service) [21]. These views remain valid not only for traditional telephone contact, but also with the use of modern means of communication at a distance, in particular by e-mail and so-called. SMS.

1.4. Pay attention finally to be very frequent and numerous requests to provide telecommunication data for the purpose of criminal proceedings. This situation is explained by, among others, the necessity of a kind of double occurrence of the same data – the first time for the purposes of operational intelligence, and the second time when pending for criminal proceedings - as evidence. This practice is due to the lack of sufficient legal basis which would allow for the use of gathered during the preliminary investigation materials in a criminal trial as evidence. Among the purpose of collecting and processing data communications by police and state protection, it was not evidence indicated target. It was pointed out only that these data can be made available to services for the prevention or detection, as well as perform statutorily defined tasks of services of an analytical and planning character. Re-occurrence of telecommunications data for evidence purposes, after a request such data for operational intelligence, may affect the actual scale data acquisition telecommunications in Poland, overstating statistics[22]. This problem should no longer occur due formulated by the Law of 15 January 2016 amending the Police Act and some other laws ("Law of 15 January 2016.") [23], remit of operational activities. An example would be art. 19 paragraph 1 of the Police Act, the first sentence: "In carrying out operational activities undertaken by the police to prevent, detect, determine the perpetrators, as well as obtain and record evidence, prosecuted by indictment, intentional crime (...)". This provision clearly so already indicates the purpose of operational activities, which is to obtain and preserve evidence.

2. The rules of special acts – data acquisition by authorized entities

2.1. Getting the call by authorized entities also takes place within the framework of the so-called operational activities. The Polish doctrine acts of operational reconnaissance characterized as a separate system of confidential or secret activities (authorized bodies), outside the process of the criminal, but usually aimed at current or future goals of this process and performed for preventing and combating crime and other legally certain negative social phenomena[24]. As part of

[21] See P. Hofmański, A. Wróbel [in] *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. Komentarz do artykułów 1-18,* Volume 1, editing L. Garlicki, Warszawa 2010, p. 407.

[22] See D. Szumiło-Kulczycka, *Czynności operacyjno-rozpoznawcze i ich relacje do procesu karnego*, Warszawa 2012, pp. 270-271; Dz. U. of 2014, item 1055; http://trybunal.gov.pl; Legalis No. 994752, part III, point 6.

[23] Dz. U. of 2016, item 147.

[24] See A. Taracha, *Czynności operacyjno-rozpoznawcze. Aspekty kryminalistyczne i prawnopodatkowe*, Lublin 2006, p. 12; T. Hanausek, *Kryminalistyka. Zarys wykładu*, Kraków 1996, p. 96; P. Chrzczonowicz, *Społeczeństwo inwigilowane w państwie prawa*, [in] P. Chrzczonowicz, V. Kwiatkowska-Darul,

the operational activities stands out operational control, which is one of the forms of operational activities. Operational control is implicit and can be performed by eight indicated previously authorized entities. Operational control can involve, among others, the use of technical means enabling to secretly obtain information and evidence and their recording, and in particular the content of telephone conversations and other information transmitted via telecommunications networks.

2.2. On 7 February 2016 entered into force the Law of 15 January 2016 amending the Police Act and some other laws. This Act was performing the Constitutional Court's judgment of 30 July 2014., Ref. K 23/11. The Act expanded the existing powers of authorized entities in the field of operational control. An example would be art. 19 paragraph 6 of the Police Act. According to the current wording of the provision of operational control include in particular the use of technical means enabling to secretly obtain information and evidence and their recording, and in particular the content of telephone conversations and other information transmitted via telecommunications networks. According whereas the new wording of art. 19 paragraph 6 section 4 of the Police Act, operational control may also rely on "achieving and consolidating the data contained in data media, telecommunications terminal equipment, information systems and telecommunications." According to the art. 2 section 43 P.T., telecommunications terminal equipment indicates "communication device designed to connect directly or indirectly to the termination of the network." In other words, it is simply about telephones. Considering how much in terms of technology are developed, in particular mobile devices, and how to perform many functions, operational control in this area will mean access to a huge amount of information (emails, SMS-sy, personal data files etc.).

2.3. The current practice of operational intelligence revealed numerous problems, including those of a constitutional nature[25]. In this regard were made numerous judgments of the Polish Constitutional Court, of which the key is the Constitutional Court's judgment of 30 July 2014., Ref. K 23/11[26], in which the Tribunal determined, among others, conditions of admissibility of operational activities. Taking into account existing arrangements TK and the European Court

K. Skowroński red., *Materiały z konferencji naukowej*, Toruń 2003, pp. 153-154. See also W. Kozielewicz, *Postępowanie w przedmiocie zarządzenia kontroli operacyjnej*, [in] L. Paprzycki, Z. Rau, *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu. Nowoczesne technologie i praca operacyjna*, Warszawa 2009, pp. 509-510; A. Sakowicz, *Opinia o projekcie ustawy o czynnościach operacyjno-rozpoznawczych*, Sejm Paper No. 353, www.sejm.gov.pl; D. Zalewski, A. Melezini, *Ustawa o kontroli skarbowej. Komentarz praktyczny*, Warszawa 2015, Legalis, commentary to art. 36.

[25] See Constitutional Court's judgment of 12 December 2005, K 32/04, OTK-A 2005, No. 11, item. 132; Z. Rau, *Czynności operacyjno-rozpoznawcze w polskim systemie prawa - działania w kierunku uniwersalnej ustawy*, [in] L. Paprzycki, Z. Rau, *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu. Nowoczesne technologie i praca operacyjna*, Warszawa 2009, p. 720.

[26] Dz. U. of 2014, item 1055.

of Human Rights and the Court of Justice of the European Union on the rules governing the secret acquisition by public authorities in a democratic state of law information units. TK indicated in the judgment described the minimum requirements to be satisfied jointly provisions limiting constitutional rights and freedoms[27].

TK carrying out checks on the rules governing the operational activities, taking into account the guidelines indicated in the judgment of 30 July 2014., Ref. K 23/11, stated the incompatibility of many regulations governing operational activities, including, as has already been indicated, the steps for the collection and sharing of data communications. It is necessary to analyze the deficiencies found by the Tribunal, as were the cause of changes in the laws governing the activities of authorized entities, based on which are currently collected data communications.

2.4. The provision of art. 27 paragraph 1 of the ABW and AW, regulating the conditions for conducting operational activities, referred to the art. 5 paragraph 1 point 2 of the ABW and AW. Moreover, ar. 5 paragraph 1 point 2 b of the Law on ABW and AW pointed to crimes threatening the economic foundations of the state, as offenses for which can be carried out operational activities. TK judgment of 30 July 2014 K 23/11, art. 27 paragraph 1 in connection with art. 5 paragraph 1 point 2 b of the Law on ABW and AW was declared incompatible with art. 2, art. 47 and art. 49 in conjunction with 31 paragraph 3 of the Polish Constitution ("RP"). In support of that judgment, the Constitutional Tribunal pointed out that the Penal Code or other laws do not use the expression "criminal offenses affecting the economic base of the state", both when it comes to generic names of individual offenses, components definition, or the titles of the chapters of criminal law, which are collected a particular type of crime. Due to the use of a legislator blurred expression, referring to unspecified "crimes affecting the economic base of the state", the actual boundaries of covert interference in the freedom and human rights are not defined in a sufficiently determined by the legislature and determine these bodies applying the law[28].

The Act of 15 January 2016 following the Constitutional Court's judgment, he gave the provision of art. 27 paragraph 1 point 2 of the ABW and AW as follows: "The court, upon the written request of the Head of the Internal Security Agency, made after obtaining the written consent of the Attorney General may, by order, order that operational control - when other measures have proved ineffective or are not useful - the performance operational activities undertaken by the Internal Security Agency in order to identify, prevent and detect offenses referred to in sections XXXV-XXXVII of the penal Code and sections 6 and 7 of the Criminal Code of the Tax - if they threaten the economic base of the state - and in order to obtain and record evidence these crimes and prosecute the perpetrators." The new

[27] Constitutional Court's judgment of 30 July 2014, Ref. K 23/11, Dz. U. of 2014, item 1055; http://trybunal.gov.pl; Legalis No. 994752, part III, point 5.

[28] Dz. U. of 2014, poz. 1055; http://trybunal.gov.pl; Legalis nr 994752, part III, point 5.

wording of this provision removes existing reservations. Firstly, what is negated in the Tribunal's judgment, no longer points to the overall "crime detrimental to the economic base of the state" but refers to specific provisions of the Criminal Code and the Criminal Code of the Tax. Secondly, it tells observe the principle of subsidiarity. Operational control can therefore be ordered only when other measures have proved ineffective or are unsuitable. The term "other means" should be understood as other forms of operational activities, which are not operational control. "Ineffective" means but not to bring the expected results, while "unfit" – the inability to achieve the intended results, using specific means. In the literature it is assumed that bringing about the management of operational control, the competent authority must demonstrate the ineffectiveness of existing activities or lend credence to the inadequacy of traditional methods of criminal analysis[29]. Thirdly it is indicated clearly the aim undertaken by ABW operational intelligence, which is the identification, prevention and detection of crime.

The solutions are in line with the judgment of 8 April 2014 Court of Justice of the European Union, which in Joined Cases C 293/12 and C 594/12 ("the judgment of 8 April 2014 ECJ"[30]) annulled 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 ("Directive 2006/24/EC")[31]. Directive 2006/24 / EC was implemented into Polish law an amendment to the telecommunications law of 24 April 2009[32]. The amendment is imposed on telecommunications companies the obligation to retain and store, and then – at the request of certain authorities – the sharing of telecommunications data, referred to in art. 180c and 180d P.T. It also created the legal framework for access to such data by authorized bodies. In its judgment of 8 April 2014 CJEU pointed out that Directive 2006/24 is limited to a general reference in art. 1 paragraph 1 to the term "serious crimes" as defined in the laws of each Member State. No in Directive 2006/24 the definition of "serious crimes" means that there is a clear limit the cases in which telecommunications data retention and can be used.

2.5. TK judgment of 30 July 2014, K 23/11, the provisions of art. 20c paragraph 1 of the Police Act; art. 10b paragraph 1 SG; art. 36b paragraph 1 point 1 KS; art. 30 paragraph 1 ŻW; art. 28 paragraph 1 point 1 of ABW and AW; art. 32 paragraph 1

[29] See W. Kozielewicz, *Postępowanie w przedmiocie zarządzenia kontroli operacyjnej* [in] L. Paprzycki, Z. Rau, *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu. Nowoczesne technologie i praca operacyjna*, Warszawa 2009, p. 511; Constitutional Court's judgment of 30 July 2014., Ref. K 23/11, Dz. U. of 2014, item 1055; http://trybunal.gov.pl; Legalis No. 994752, part III, point 6.

[30] Dz. U. of 2014 r., item 105, p. 54.

[31] L 105/54 EN Official Journal of the European Union of 13 April 2006.

[32] The Act of 24 April 2009 amending the Act - Telecommunications Law and some other acts, Dz. U. of 2009, item 1445.

point 1 of the SKW and SWW; art. 18 paragraph 1 point 1 of the CBA; art. 75d paragraph 1 SC – in that it does not provide for an independent control data sharing telecommunications referred to in art. 180c and art. 180d P.T., were found to be incompatible with art. 47 and art. 49 in conjunction with 31 paragraph 3 of the Constitution. In support of this part of the judgment the Constitutional Tribunal pointed out that one of the requirements to be satisfied by laws authorizing the designated entities to obtain telecommunications data, is to create an independent control mechanism. Since the acquisition of these data is done implicitly, without the knowledge and the will of the entities whose information is collected by these entities, and also the limited control of society, the lack of independent control of state authorities over this process creates a risk of abuse. The requirement of normalization in the law of procedural mechanisms to counter the arbitrariness of the acquisition of telecommunications data is the stronger, because no provision did not impose the obligation to obtain the consent of the court (or another body that would be independent from the authorities demanding the release of the data or bodies over them superior) to make available to authorized entities data referred to in art. 180c and art. 180d P.T. This procedure does not even require the consent of the prosecutor. The legislator did not provide for a framework of *ex post* controls legalizing actions taken[33].

The Act of 15 January 2016 has made significant changes in the laws governing the activities of authorized entities in this area. Examples include the provisions of art. 20ca of the Act on the Police added after art. 20c in the following wording: "Art. 20ca 1. Control over your data by the police telecommunications, postal or online exercises district court competent for the authority of the Police, which made available the data. 2. The Police referred to in paragraph 1, shall, subject to the provisions on the protection of classified information, the provincial court referred to in paragraph 1, a semi-annual basis, a report including:

1) the number of cases in the reporting period to obtain data telecommunications, postal or internet and the nature of the data;

2) qualified legal acts in connection with the occurrence of which a data telecommunications, postal or online, or information on obtaining data in order to save human life or health, or support of search or rescue.

3. The audit referred to in paragraph 1, the district court may refer to the materials supporting the provision of police data telecommunications, postal or online. 4. The district court shall inform the Police of the audit within 30 days of its completion. 5. Control referred to in paragraph 1, is not subject to obtaining data on the basis of art. 20cb paragraph. 1 ".

The provision of Art. 20ca of the Police Act introduces the subsequent control. Control entrusted to the provincial court competent for the seat of the Police authority, which was made available the data. The control exercised by the court

[33] Dz. U. of 2014, item 1055; http://trybunal.gov.pl; Legalis nr 994752, part III, point 10.4.

satisfies the requirement of independence of the supervisory authority of the government. This solution favors performance of departments responsible for national security and public order. But the question arises whether or not a better solution for the protection of civil rights and freedoms, but also takes into account the interests of staff, would be a solution, which in principle provides for the inspection prior court. Follow-up audit would be used in demanding the Police and other services urgent cases. Prior examination of the court would contribute both to increase the correctness prepared by the authorities of the Police and other service requests, as well as their numbers.

Secondly, the question arises about the effectiveness of the solution adopted in practice. In other words, if the control exercised by the court will be real and not just apparent control. Due to the current already very heavy burden on the courts, no additional posts and have expertise people to exercise real control will be very difficult. It is worth noting that after the changes introduced by the Act of 15 January 2016, entitled parties will be able to use the data and set the IP address, connect and login times. In these cases, the consent of the court is not required. Judicial control will be exercised while post factum, which indicated the restrictions will be ineffective solution. One should also note that the data will be transferred quite rare, i.e. every six months. Exercising control of the district court may, in the framework of its powers refer to the materials supporting the provision of police telecommunications data, the effect of which will be the results of checks provided by the court police authority. After the transfer of inspection results will be completed in principle activity of the court in the process of verifying the correctness of data sharing. They are defined in terms of procedural further court action if we find that a disclosure in breach of the regulations in force. The solution to this problem could be either appropriate to strengthen human resources and competence relevant units of courts, judges providing substantive support or establish a separate institution dealing with the control of the quantity, scope and compliance procedures for data acquisition telecommunications.

Thirdly, the introduction of the model ex-ante control of the court in terms of access to telecommunications data would facilitate the actual implementation of the principle of subsidiarity data acquisition. Condition for access to the data would be exhausted by the police and other services of the other remedies which less impact on the privacy and secret communication.

The criticisms find their support in the judgment of 8 April 2014 CJEU. The Court noted that the acquisition by the competent national authorities to access the data is not subject to the prior scrutiny of a court or an independent administrative authority. The court or independent administrative authority should check that the sharing and use of data was limited to cases where it is strictly necessary to attain the objective pursued[34]. ECJ says explicitly of prior control by an independent authority.

[34] Theses 60-62 judgment of 8 April 2014, Court of Justice of the European, Dz. U. of 2014, L 105.

2.6. TK judgment of 30 July 2014, K 23/11, also considered art. 19 of the Police Act; art. 9e SG; art. 36c KS; art. 31 Military Police; art. 27 ABW and AW; art. 31 SKW and SWW; art. 17 CBA – the extent to which it does not provide a guarantee of prompt, commission and destruction protocol materials containing banned evidence on which the court has not quashed or set aside professional secrecy was inadmissible as incompatible with art. 42 paragraph 2, art. 47, art. 49, art. 51 paragraph 2 and art. 54 paragraph 1 in connection with art. 31 paragraph 3 of the Constitution. TK in support of this part of the judgment pointed to the absence in the contested provisions of sufficient procedural guarantees to ensure the protection of the confidentiality of information provided to entities providing professions of public trust. They provide – without any doubt of interpretation – or obligation to prior judicial review of the data collected, or possible exemption (repeal) of professional secrecy in the particular case. It is not guaranteed in these laws that, in the reasonable suspicion that the collected materials contain information covered by professional secrecy and therefore require special protection, there will be additional verification of these materials by the court and the possible exemption from professional secrecy, before being transferred to officers or the prosecutor. The challenged provisions do not provide for the destruction procedures collected in the course of operational control information constituting professional secrets[35].

The bill introduced the necessary changes in legislation, the provisions of which have been negated in this area. Examples include the provisions of the Police Act. According to the Draft Law in art. 19 paragraph 15e paragraphs have been added 15f-15j. Due to the content of the ruling TK are crucial to the provisions of art. 15j of the Police Act providing for duty immediately, commission and protocol of destruction of materials to be used in criminal proceedings is unacceptable. Body of Police was obliged to immediately inform the prosecutor of the destruction of these materials.

Presented problem was also observed in the judgment of 8 April 2014 CJEU. The Court noted that Directive 2006/24/EC covers in a comprehensive manner all the use of electronic communications services, data retained. This applies even to those persons in respect of whom lack any basis, both actual and legal persons to criminal prosecution. The Directive does not provide for any exceptions to those people. This means that it is also applied to people whose contact and the message obtained during this contact, on the basis of national law is covered by professional secrecy[36].

2.7. The judgment of the Constitutional Tribunal dated 30 July 2014, K 23/11, the provisions of art. 28 ABW and AW; art. 32 SKW and SWW; art. 18 CBA - the extent to which it does not provide for the destruction of data irrelevant to the

[35] Dz. U. of 2014, item 1055; http://trybunal.gov.pl; Legalis No. 994752, part III, point 11.8.

[36] Theses 57-58 judgment of 8 April 2014, Court of Justice of the European Union, Dz. U. of 2014, L 105.

proceedings were considered incompatible with art. 51 paragraph 2 in conjunction with 31 paragraph 3 of the Constitution. The previously existing legislation, there was no procedure for verification and destruction of data irrelevant, which is unnecessary for further proceedings. According to the art. 51 paragraph 2 of the Constitution the public authorities shall not acquire, collect and share information on citizens other than necessary in a democratic state ruled by law. In its case law TK he explained the concept of "the data necessary in a democratic country," pointing out that "in a democratic state ruled by law is not necessary to store information on citizens obtained in the course of operational activities due to the potential usefulness of this information. This can be used only in connection with a particular procedure, conducted under the Act authorizing the restriction of freedom due to national security and public order." Implicit condition for obtaining information about individuals, including those related to their telecommunications data, to establish procedures for immediate selection and material destruction unnecessary and unacceptable. This solution prevents unauthorized use by State authorities legally collected information and its storage in case, if in the future proved to be useful for other purposes[37].

The bill implementing the Constitutional Court's judgment has made the appropriate changes in the provisions of laws, the provisions of which have been negated in this area. An example is the provision of art. 28, paragraph 7 of the ABW and AW. Under this provision, the data which are not relevant to the criminal proceedings or are not relevant to the security of the state, shall have immediate destroyed.

2.8. Act of 15 January 2016 not only eliminated the numbers indicated in the Tribunal's judgment, contrary to the Polish Constitution rule, but introduced new provisions that raise doubts. The new legislation does not directly concern the collection and provides telecommunications data, but because of the solutions adopted worth quoting their content. An example might be a new sound, given the law of 15 January 2016, the provision of art. 20c of the Police Act. According to the art. 20c paragraph 1 of the Police Act, in order to prevent or detect crime or to save human life or health, or support exploration activities or emergency, police can obtain data constituting a content respectively, of telecommunications, postal delivery or transfer of the service provided by electronic means as defined in: 1) art. 180c and art. 180d P.T., hereinafter referred to as "telecommunications data"; 2) art. 82 paragraph 1 point 1 of the Act of 23 November 2012 r. - Postal Law[38], hereinafter referred to as "mail data"; 3) art. 18 paragraph. 1-5 of the Act of 18 July 2002 on electronic services[39], hereinafter referred to as "data web" - and can be processed without the knowledge and consent of the person concerned. Sharing these data policeman can be done, among others, through a telecommunications

[37] Dz. U. of 2014, item 1055; http://trybunal.gov.pl; Legalis No. 994752, part III, point 12.2.

[38] Dz. U. item 1529 and 2015 item 1830.

[39] Dz. U. 2013, item 1422 and 2015, item 844.

network (art. 20c paragraph 2 of the Police Act). In this case, the sharing of data takes place without the participation of employees of a telecommunications provider or when necessary their participation, if such a possibility is provided for in an agreement between the Commander in Chief of the Police and the entity. The Act of 15 January 2016 introduced so access to the data on line – the so-called a secure Internet connection. For obtaining such data will not be needed prior consent of the court, as is the case for example. So chat, which substantially limit the court's control over the acquisition of such data. Although the provision of art. 20c paragraph 5 of the Police Act provides that the Chief Commander of Police, Commander of the Central Bureau of Investigation and the commander of the provincial police keep records of instances to obtain data telecommunications, postal and Internet containing information identifying the organizational unit of the Police and the police officer who receives the data, their type, the purpose of the acquisition and the time in which they were obtained, but certainly not balance this lack of prior control by an independent authority. The collected data, which are relevant for criminal proceedings, the Chief Commander of Police, Commander CBŚP or commander of Provincial Police shall provide competent prosecutor locally or in kind. The prosecutor decides on the scope of use of the communicated data. Data that are not relevant to the criminal proceedings, shall without delay destructed (art. 20c paragraph 6-7 of the Police Act).

3. The provisions of telecommunications law in the collection and sharing of data communications

3.1. The provisions of art. 180c and 180d P.T. determine directly and by reference to other provisions of the Telecommunications Law, the data that telecommunications companies are obliged to make available to courts, prosecutors and authorized entities. According to the art. 180c paragraph 1 P.T., a list that included data necessary to:

1) determine the completion of the network, telecommunications terminal equipment, the end user: a) initiating the connection, b) to whom the call is;

2) to determine: a) the date and time of the call and its duration, b) type of connection, c) the location of the telecommunications terminal equipment.

Based on the art. 180c paragraph. 2 P.T. was issued Regulation of the Minister of Infrastructure of 28 December 2009 on the detailed list of data types and operators of public telecommunications networks or providers of public telecommunications services obliged to their retention and storage[40]. This regulation defines:

1) a detailed list of the necessary data: a) establish the network termination, telecommunications terminal equipment, the end user initiating the connection,

[40] Dz. U. No. 226, item 1828.

b) determine the network termination, telecommunications terminal equipment, the end user to which the call is connected, c) the date and time of the call and its duration, d) identify the type of call, e) determine the location of the telecommunications terminal equipment;

2) types of public telecommunications network operators and providers of public telecommunications services obliged to retain data referred to in paragraph 1.

However, pursuant to art. 180d P.T., telecommunications companies are obliged to ensure the conditions for access to and preservation and to provide qualified entities and the Customs Service, the court and the prosecutor, at his own expense, processed their data, referred to in art. 159 para. 1 point 1 and 3-5 P.T., in art. 161 P.T. and in art. 179 paragraph 9 P.T., connected with the service telecommunications, on the principles and maintaining the procedures set out in separate regulations.

3.2. The telecommunications law is regulated the issue of the bearing and sharing of telecommunications data. The provision of art. 180d P.T. states that telecommunications companies are obliged to ensure the conditions for access to and preservation and to provide qualified entities and the Customs Service, the court and the prosecutor, at his own expense, processed their data. Directly to the issue of the cost of collection and provides telecommunications data refers to art. 180a P.T. According to the first paragraph of art. 180a P.T., subject to Art. 180c paragraph 2, point 2 P.T., public telecommunications network operator and provider of publicly available telecommunications services are obliged at their own expense:

1) stop and store the data referred to in Article. 180c P.T., generated in telecommunications networks or by them processed on Polish territory for a period of 12 months from the date of the merger or failed connection attempts, and the expiry of this period, the data destroyed, except those that have been protected in accordance with the separate regulations;

2) provide the data referred to in point 1, to authorized entities and the Customs Service, the court and the prosecutor, on the principles and procedures set forth in separate regulations;

3) protect the data referred to in paragraph 1 against accidental or unlawful destruction, loss or alteration, unauthorized or unlawful storage, processing, access or disclosure, in accordance with art. 159-175 and art. 175c. 180e P.T.

The problem of cost of collecting and sharing data communications also dealt with the Supreme Court. In its decision of 25 March 2010, I KZP 37/09, pointed out that the provision of art. 180a paragraph 1 point 2 P.T. imposes on operators of public telecommunications networks and providers of publicly available telecommunications service obligation to provide, it is a search, developing relevant statements and transmission via telecommunications networks to authorized entities, including the court and the prosecutor of the data referred to in art. 180c paragraph 1 P.T. So understood the costs of sharing the burden of data

provider or supplier, and can not form part of the legal costs and therefore do not constitute expenditure referred to in art. 618 k.p.k., or expenses incurred by the State Treasury in the course of criminal proceedings[41].

In practice, however, they created doubt as to who bears the costs associated with the transfer of e-mail service. In its resolution of 30 September 2014, I KZP 18/14, the Supreme Court explained that art. 180d P.T. applies to data related to the transmission of e-mail service by telecommunications companies. There is no use to give the service provider the state authorities for the needs of their investigations of data on a specific art. 18 paragraph 6 of the Act of 18 July 2002 on electronic services[42], and on the same service provided electronically. The cost of developing these data apply art. 619 § 1 k.p.k. in conjunction art. 618 § 1 k.p.k.[43] Taken by the Supreme Court resolution was a response to the question addressed to the Supreme Court, or the provision of art. 180d P.T apply to information in the field of e-mail services, the basis for granting information is art. 18 paragraph 6 of the Act of 18 July 2002 on electronic services. This provision states that the service provides free information referred to in art. 18 paragraph 1-5 of the Act on electronic services, state authorities authorized pursuant to separate regulations for the purpose of their investigations.

The position of the Supreme Court is based on the distinction of two types of services: mail forwarding services and electronic mail[44]. The doctrine also indicates that the e-mail service is a hybrid service. Mail transport is a telecommunications service, and resource-mail, its storage and sharing is a service of the information society. According to Directive 2002/21/ EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks[45], e-mail service is not a telecommunications service[46]. The main elements of e-mail services are sharing personal email account, providing the possibility of receiving mail directed to this e-mail account, providing the ability to send mail from your mail account, ensure storing e-mail, not the business of a wholly or mainly in the conveyance of signals electronic communications network. In this connection, the e-mail service is not a telecommunications service as defined in the Telecommunications Act, the

---

[41] Biuletyn SN 2010 No. 3; www.sn.pl; OSNKW 2010, No. 5, item 43, p. 42, Krakowskie Zeszyty Sądowe ("KZS") 2010, No. 5, item 19.

[42] Tj. Dz. U. of 2013, item 1422.

[43] OSNKW 2014, No. 12, item 86; Prokuratura I Prawo 2015, No. 1-2, item 28, KZS 2014, No. 10, item 10; Biuletyn SN 2014, No. 9; www.sn.pl.

[44] Similarly: A. Krasuski, *Prawo telekomunikacyjne. Komentarz*, Warszawa 2010, pp. 91-92; M. Rogalski, *Prawo telekomunikacyjne. Komentarz*, Warszawa 2010, pp. 85-86; S. Piątek, *Prawo telekomunikacyjne. Komentarz*, Warszawa 2013, pp. 103-105.

[45] Dz. U. UE. L. 2002/208.33.

[46] M. Jurkiewicz, *Definicje legalne w prawie nowych technologii*, Przegląd Legislacyjny 2011, No. 1, pp. 112-114; M. Łopaciński, *Poczta elektroniczna w prawie telekomunikacyjnym*, http://prawo.vagla.pl/node/7152.

information from its scope can not have, therefore, the application of art. P.T. 180d, which in turn imposes on telecommunications undertakings to provide at their expense the conditions for access and preservation of and access to authorized entities and the Customs Service, courts and prosecutor, processed their data associated with the service forwarding e-mail. The Supreme Court considered that since the legislature in art. 18 paragraph 6 of the Act on electronic services, differently than it did in the Act - Telecommunications Law, has not hindered the service costs of execution imposed on it in those activities, there are no arguments that these costs are treated differently than the remuneration payable to the institution and reimbursement of costs incurred. In light of the Supreme Court found that the cost of making the data related to the e-mail service is the expense of the Treasury in criminal proceedings and the Treasury temporarily taught, pursuant to art. 619 § 1 k.p.k. Since the height and the rules for determining such charges have not been regulated in the regulations referred to in art. 618 § 2 k.p.k., the amount of the expenditure concerned to decide the amount awarded by the court, prosecutor or other body conducting the proceedings (art. 618 § 3 k.p.k.)[47].

So both doctrine and judicial decisions assume that the cost of collecting and sharing data telecommunications bear telecommunications companies, and not the courts and prosecutor's offices or authorized entities. The Act of 15 January 2016 also did not introduce any partial or varied, depending on the size of the entity obliged to provide data, payment for the entities obliged to provide data. Meanwhile in Poland, still a major problem is the very large amount of data requested by authorized entities. The introduction of at least a partial payment, even of a symbolic nature, will affect positively, i.e. a reduction in the number of inquiries, through carefully formulated question and taking into account the cost of search queries in the budgets of authorized entities, courts and prosecutor's offices.

3.3. In practice, the controversy also raises demand by entities authorized to provide telecommunications data for the period beyond that provided for by law the time of their detention, which is now 12 months (art. 180a paragraph 1 point 1 P.T.). The basis for such a request is often a factual circumstance in the form of ownership of the data subject is obliged to issue them. Such a situation is possible in practice, since some provisions of the telecommunications law provide for a longer retention periods, e.g. provision of art. 168 paragraph 2 P.T., provides for more than 12 months period necessary to consider the complaint. Nevertheless it should be noted that more than 12 months retention period is possible only in the cases expressly provided for by the provisions of the Telecommunications Law and what is essential only for the purpose specified in these regulations. In contrast, for the purposes of criminal proceedings, at the request of the court or

[47] OSNKW 2014, No. 12, item 86; Prokuratura i Prawo 2015, No 1-2, item 28, KZS 2014, No. 10, item 10; Biuletyn SN 2014, No. 9; www.sn.pl.

prosecutor, telecommunications data may be stored in accordance with art. 180a paragraph 1 point 1 P.T., for a period not longer than one year. If so, the authorized entity requesting access to the data after 12 months of their registration telecommunications provider should refuse to provide such data. Note, however, that this view is not universal. Presented are also the position that if the entrepreneur has data telecommunications, although already 12 months after, these data should be made available at the request of authorized entities.

Summary

1. Existing regulation k.p.k. and special laws, including changes introduced by the Act of 15 January 2016 after the Polish Constitutional Tribunal judgments of 30 July 2014, K 23/11 and the ECJ of 8 April 2014 meet many reported earlier by the doctrine and practice demands. Still, issues remain that require changes or clarifications. In addition, some of the solutions introduced by the Act of 15 January 2016 doubt.

2. First of all, pay attention to the differences between the regulations k.p.k. and the provisions of special laws on the collection and sharing of the call. The changes introduced in the special laws not only unify the existing solutions, but even deepen. An example would be the scope of operational control, which in addition to the issue of correspondence, mail or the call, also provides for acquisition and consolidation of data contained in data media, telecommunications terminal equipment, information systems and telecommunications. Another example is the duration of the inspection and fixing talks k.p.k. and operational control in specific acts. Therefore, should call for standardization of solutions in this field operating in specific acts by their adaptation to the rules in k.p.k. Materials and information on the basis of special laws are in fact collected for the purpose of criminal proceedings. The exception is the validity of the principle of subsidiarity. In this respect, the existing solutions in k.p.k. should be equivalent to the solutions used in specific acts. Activities in the field of data collection should be the alternative means of receiving information or evidence about individuals, they can not be obtained in any other, less painful way for them. Following the changes introduced by the Act of 15 January 2016 this rule is already in special laws, as opposed to k.p.k.

3. The Law of 15 January 2016 introduced in specific acts subsequent court control over the data made available. Both the adoption of the principle of follow-up audit, as well as the lack of detailed regulations concerning the procedures in case of violations of the law, it can cause that, in practice, this inspection will be apparent. *De lege ferenda* should be adopted solutions that provide for subsequent inspection in special cases, and as a principle should apply control blueprints. It is justified all the more that the law of 15 January 2016 making changes at the same

time expanded the powers of departments in acquiring new data and information. An example would be to extend the operational control of access to data telephones.

4. Changes should be made not only in the specific acts, but also in telecommunications law. In practice, there is acquiring communications and data communications by means of telecommunications networks. Information transmitted via telecommunications networks are so phone calls, messages in the form of sms, mms, or sent by fax, as well as other communications by radio and the Internet, including e-mail, content posted on online forums or chat rooms. Product such information possible to obtain in the course of the inspection is open. Accepted and put into practice the technology does not always provide the possibility of full control as to the scope and quantity of available data telecommunications by the persons liable for the telecommunication companies. In practice, there are cases of transfer of data by telecommunications companies to a greater extent than required in the application. This is a violation of art. 160 par. 1, in conjunction with art. 159 par. 1 point 3-5 and par. 3 P.T. and art. 218 § 1 k.p.k. The provisions of the telecommunications law should therefore clearly indicate when and on what terms can be used automated systems.

5. *De lege ferenda* should be added to the provision in the Telecommunications Law clearly indicates that in the case of having the entrepreneur of telecommunications data for a period longer than one year can not be made available to authorized entities. This principle should be obliged regardless of what is causing the data storage for more than a year.

6. At present, in accordance with applicable law telecommunications for providing data retention are not charged any fee. The introduction of at least a symbolic payment will increase the level of care both to the amount of the requested data and their kind.

Bibliography

P. Chrzczonowicz, *Społeczeństwo inwigilowane w państwie prawa*, [in] P. Chrzczonowicz, V. Kwiatkowska-Darul, K. Skowroński red., *Materiały z konferencji naukowej*, Toruń 2003;

T. Grzegorczyk, *Kodeks postępowania karnego. Komentarz*, Zakamycze 2005;

T. Hanausek, *Kryminalistyka. Zarys wykładu*, Kraków 1996;

P. Hofmański, E. Sadzik, K. Zgryzek, *Kodeks postępowania karnego. Komentarz*, Volume I, Warszawa 2011;

P. Hofmański, A. Wróbel [w:] *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. Komentarz do artykułów 1-18,* Volume I, editing L. Garlicki, Warszawa 2010;

M. Jurkiewicz, *Definicje legalne w prawie nowych technologii*, Przegląd Legislacyjny 2011, No. 1;

W. Kozielewicz, *Postępowanie w przedmiocie zarządzenia kontroli operacyjnej*, [in] L. Paprzycki, Z. Rau, *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu. Nowoczesne technologie i praca operacyjna*, Warszawa 2009;

A. Krasuski, *Prawo telekomunikacyjne. Komentarz*, Warszawa 2010;

M. Łopaciński, *Poczta elektroniczna w prawie telekomunikacyjnym*, http://prawo.vagla.pl/node/7152;

S. Piątek, *Prawo telekomunikacyjne. Komentarz*, Warszawa 2013;

Z. Rau, *Czynności operacyjno-rozpoznawcze w polskim systemie prawa - działania w kierunku uniwersalnej ustawy*, [in] L. Paprzycki, Z. Rau, *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu. Nowoczesne technologie i praca operacyjna*, Warszawa 2009;

M. Rogalski, *Prawo telekomunikacyjne. Komentarz*, Warszawa 2010;

A. Sakowicz, *Opinia o projekcie ustawy o czynnościach operacyjno-rozpoznawczych*, www.sejm.gov.pl;

D. Szumiło-Kulczycka, *Czynności operacyjno-rozpoznawcze i ich relacje do procesu karnego*, Warszawa 2012;

A. Taracha, *Czynności operacyjno-rozpoznawcze. Aspekty kryminalistyczne i prawnopodatkowe*, Lublin 2006;

D. Zalewski, A. Melezini, *Ustawa o kontroli skarbowej. Komentarz praktyczny*, Warszawa 2015.