Ius Novum
3/2017

OBTAINING OF COMMUNICATIONS DATA BY THE INTERNAL SECURITY AGENCY AFTER THE CONSTITUTIONAL TRIBUNAL JUDGEMENT OF 30 JULY 2014

BARTŁOMIEJ OPALIŃSKI*

1. INTRODUCTION

The Republic of Poland is a democratic state, which results from the declaration laid down in the Constitution of the Republic of Poland of 2 April 1997[1] as well as the political system practice. One of the key issues in every democracy is the scope of the state apparatus interference into different areas of the citizens' activity. One of the areas is the sphere of citizens' rights and freedoms and, within it, a serious issue of obtaining telecommunications data, especially telecommunications billings.[2] The problem is related to ensuring efficient crime prevention and constitutes one of the tools used by law enforcement agencies.[3]

* PhD, Assistant Professor, Department of Administration Studies, Faculty of Law and Administration of Łazarski University in Warsaw

1 In accordance with Article 2 of the Constitution of the Republic of Poland, the Republic of Poland is a democratic state ruled by law and implementing the principles of social justice.

2 See, L. Garlicki, *Uwaga nr 3 do art. 49 Konstytucji RP* [Comment No. 3 on Article 49 of the Constitution of the Republic of Poland], [in:] L. Garlicki (ed.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz* [Constitution of the Republic of Poland. Commentary], Vol. II, Warsaw 2002, p. 1.

3 It seems that the numerous terrorist attacks, especially the one on the World Trade Center on 11 September 2001 as well as terrorist attacks in Madrid (11 March 2004) and in London (7 July 2005), were significant stimuli to the introduction of legal regulations allowing the retention of telecommunications data and giving the police, state security services and justice institutions access to them. That period initiated the global war with terrorism. Its efficient implementation required preparation of appropriate legal instruments to be able to undertake activities in the area. See, M. Kiziński, *Retencja danych telekomunikacyjnych* [Retention of telecommunications data], Prokuratura i Prawo No. 1, 2016, p. 138; Fundacja Panoptykon, *Telefoniczna Kopalnia Informacji. Przewodnik* [Telecom Information Mine. A Guide], p. 20, http://panoptykon.org/biblio/telefoniczna–kopalnia–informacji–przewodnik.

In accordance with Article 180a of the Act of 16 July 2004: Telecommunications law (hereinafter TL),[4] public telecommunications network operators and providers of publicly available telecommunications services are obliged to retain telecommunications data and give access to them.[5] The provision stipulates directly that the addressees of the obligation to retain telecommunications data are public telecommunications network operators and providers of publicly available telecommunications services.[6] Definitions of each of those entities are laid down in Article 2(27) TL. In accordance with this provision, an operator is

---

[4] Journal of Laws [Dz.U.] of 2014, item 243, as amended.

[5] A question arises what those telecommunications data that are subject to retention and provision are. The answer to this question is rather complicated because it requires an analysis of many provisions. In accordance with Article 180c(1) TL, the data that are subject to provision are those concerning the network end facility, the telecommunications end device, the end user initiating a connection or receiving a connection as well as data concerning the day and time of the connection, its length, type and location of the telecommunications end facility. On the other hand, Article 180d TL does not lay down the catalogue of data that are subject to provision to the state services. It refers to Article 159(1(1) and (3) to (5)), Article 161 and Article 179(9) TL. The legislator, based on the provisions indicated, authorised given entities to obtain data concerning a user, transmission data (i.e. data processed in order to transmit messages in telecommunications networks or calculate fees for communications services, including location data that concern any data processed in the network indicating the geographical location of the end device of the user of the public telecommunications services), localisation data that concern localisation data going beyond what is necessary telecommunications services, data concerning location, i.e. localisation data exceeding the data that are necessary to transmit a massage or issue an invoice, data concerning attempts to obtain a connection between the end devices, including unsuccessful attempts to make connections indicating connections between the telecommunications end devices or network ends that have been listed but not answered by the end user or there has been a break of the listed connections. In accordance with Article 161 TL, a provider of public telecommunications services may also retain a subscriber's personal data, including given names, a surname, their parents' names, the place and date of birth, the address of residence and for correspondence, the PESEL number of the Polish citizen, an identification document number and series number, a passport number or residence permit in case of a citizen of a country that is not the European Union Member State or the Swiss Confederation, and data contained in documents confirming the possibility of fulfilling the obligations towards the provider of public telecommunications services resulting from a contract concerning the provision of telecommunications services. Moreover, if the provider of public telecommunications data was given consent from the subscriber who is a natural person to process his/her other data in connection with the service provided, especially the bank account number, banker's card number, the address for correspondence (if it is different from residence address), email address and telephone numbers, the police services and the state security services may also obtain and process those data being at the operator's disposal for the purposes laid down in statute. In addition, the state services may obtain data referred to in Article 179(9) TL, i.e. data every telecommunications business is obliged to include in the register of subscribers, users or end devices, data obtained during the conclusion of a contract. Summing up, it is possible to obtain three types of data: concerning a subscriber, the traffic (the billing data) and localisation.

[6] The introduction of the regulations concerning telecommunications data retention to the Polish legal system resulted from the implementation of Directive 2006/24/EC. It should be noted, however, that legal mechanisms allowing police institutions and state security bodies to obtain data retained by telecommunications businesses, although in a less extensive form than at present, existed in the Polish legal system also before the implementation of Directive 2006/24/EC. They were introduced on 24 January 2003 on the basis of the Regulation of the Minister of Infrastructure on the fulfilment of operators' tasks in connection with defence, state security and security and public order, Journal of Laws [Dz.U.] No. 19, item 166, as amended. However, the transposition of Directive 2006/24/EC ensured legal specification of the businesses' obligations in the field of data retention.

a telecommunications business authorised to provide public telecommunications networks or accompanying services. A provider of services, on the other hand, is a telecommunications business authorised to provide telecommunications services. It is necessary to emphasise that the legislator stressed the different plane of activities of telecommunications businesses. The activity of the operator focuses on the provision of a telecommunications network, which means preparation of this network for the provision of services within it. The activity of the service provider focuses on the provision of telecommunications services with the use of its own network or the network owned by another operator.[7]

What correlates with the obligation to retain telecommunications data is authorised bodies' entitlement to request access to the data (Article 180a (1(2)) TL and Article 180d TL). The group of those entities is quite large because it encompasses a court and a prosecutor's office[8] and eight police and state protection institutions, i.e. the Police,[9] the Border Guard,[10] Military Police (Żandarmeria Wojskowa),[11] the Internal Security Agency (Agencja Bezpieczeństwa Wewnętrznego, ABW),[12] the Military Counterintelligence Service,[13] Central Anticorruption Bureau (Centralne Biuro Antykorupcyjne, CBA),[14] the Customs Service,[15] and also fiscal authorities.[16]

One of the special services authorised to obtain telecommunications data is the Internal Security Agency. As it has already been mentioned, the issue was regulated in Article 28 of the Act on the Internal Security Agency (ABW) and the Intelligence Agency (AW). In accordance with the provision, the obligation to obtain a court's consent referred to in Article 27(1) does not apply to information necessary to implement ABW tasks referred to in Article 5(1) of the Act on ABW and AW in the form of data referred to in Articles 180c and 180d TL and data identifying an entity using postal services and concerning the fact, circumstances of postal services provision or their use (para. 1). It is also stipulated that an entity doing business in the field of telecommunications or

---

[7] A third option is also noted in the literature. Namely, a provider of telecommunications services may resell services bought from another provider. See, K. Kawałek, M. Rogalski (ed.), *Prawo telekomunikacyjne. Komentarz* [Telecommunications law. Commentary], Warsaw 2010, p. 64.

[8] See, Article 218 of the Act of 6 June 1997: Criminal Procedure Code, Journal of Laws [Dz.U.] No. 89, item 555, as amended, hereinafter: CPC.

[9] See, Article 20c of the Act of 6 April 1990 on the Police, Journal of Laws [Dz.U.] of 2015, item 355, as amended, hereinafter: Act on the Police.

[10] See, Article 10b of the Act of 12 October 1990 on the Border Guard, Journal of Laws [Dz.U.] of 2014, item 1402, as amended, hereinafter: Act on BG.

[11] See, Article 30(1) of the Act of 24 August 2001 on the Military Police and military order keeping bodies, Journal of Laws [Dz.U.] of 2016, item 96, as amended, hereinafter: Act on MP.

[12] See, Article 28 of the Act of 24 May 2002 on the Internal Security Agency (ABW) and the Intelligence Agency (AW), Journal of Laws [Dz.U.] of 2015, item 1929, as amended, hereinafter: Act on ABW and AW.

[13] See, Article 32 of the Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service, Journal of Laws [Dz.U.] of 2016, item 1318, as amended, hereinafter: Act on MCS and MIS.

[14] See, Article 18 of the Act of 9 June 2006 on the Central Anti-corruption Bureau (CBA), Journal of Laws [Dz.U.] of 2016, item 1310, as amended, hereinafter: Act on CBA.

[15] See, Article 75d of the Act of 27 August 2009 on Customs Service, Journal of Laws [Dz.U.] of 2015, item 990, as amended, hereinafter: Act on CS.

[16] See, Article 36b of the Act of 28 September 1991 on fiscal control, Journal of Laws [Dz.U.] of 2016, item 720, as amended, hereinafter: Act on FC.

an operator providing postal services must provide the data referred to in para. 1 free of charge to an ABW officer indicated in the ABW Head's written motion or a person authorised by that body, on verbal request of an ABW officer authorised by the ABW Head in writing as well as to an ABW officer authorised by the ABW Head in writing via the telecommunications network (para. 2). In the last of the cases mentioned, the telecommunications data are provided without the participation of the employees of the telecommunications business or with their indispensable co-participation if it is possible on the basis of an agreement between the ABW Head and this entity (para. 3). The provision of data referred to in Articles 180c and 180d TL and data identifying the user of postal services and concerning the fact, circumstances of postal services provision or of using them, may take place via the telecommunications network if this network makes it possible to identify an ABW officer obtaining the data, their type and the time of obtaining them as well as the technical and organisational measures protecting those data against unauthorised access (para. 4).

Since they entered into force, the legal regulations concerning communications data retention and their provision to ABW as well as other authorised state bodies have provoked controversies.[17] As a result, the Supreme Audit Office (Najwyższa Izba Kontroli, NIK) verified the way of obtaining and processing billing data, information about location and other data referred to in Article 180c and Article 180d TL by the authorised entities. In the audit report, NIK indicated that it is necessary to determine the catalogue of matters for the needs of which telecommunications data can be obtained. Attention was also drawn to the need to introduce legal solutions additionally providing protection for people doing jobs of public trust. It was also recognised that it is purposeful to introduce internal control mechanisms of the process of obtaining data, their verification and disposal of useless data.[18]

The Constitutional Tribunal judgement of 30 July 2014 (case No. K 23/11, i.e. the "billings and communication interception" case) was the consequence and in a way recapitulation of the controversies over telecommunications data retention. The judgement was issued as a result of the motions filed by the Ombudsman and the Prosecutor General to examine the constitutionality of the provisions regulating obtaining telecommunications data by entitled entities, including the Internal Security Agency. As a consequence, it was necessary to amend particular pragmatic acts in order to adjust the regulations on telecommunications data retention and provision to the standards indicated by the Constitutional Tribunal. The aim of this Article is related to that. It is an analysis of the above-mentioned Constitutional Tribunal judgement on billings and communication interception concerning the Internal Security Agency and the legislator's response to its content and recommendations in the field of obtaining telecommunications data by this state service.

---

[17] They concerned various issues, inter alia, arrest of data concerning all telecommunications services users or grounds for the retention of data for a period of 24 months. See, M. Wach, *Zatrzymywanie danych telekomunikacyjnych przez dwa lata w celach bliżej nieokreślonych a prawo do prywatności* [Retention of telecommunications data for two years for undefined reasons and the privacy right], Radca Prawny scientific supplement No. 115–116, 2011.

[18] Information of the NIK audit results: http://www.nik.gov.pl/plik/id, 5421,vp,7038.pdf [accessed on 16 June 2016].

2. CONTENT OF THE MOTIONS OF THE OMBUDSMAN AND THE PROSECUTOR GENERAL

Formally, it was the Ombudsman and the Prosecutor General who initiated the review concerning obtaining telecommunications data by entitled entities, which the Constitutional Tribunal performed. In a motion of 1 August 2011, based on the analysis of Articles 180c and 180d TL regulating particular services' access to data protected by communication secrecy, the Ombudsman questioned the conformity of two provisions of the Act on ABW[19] with the Constitution of the Republic of Poland. One of them is Article 28 (1(1)) of the Act on ABW and AW. The petitioner challenged the conformity of this provision with Article 49 in conjunction with Article 31(3) of the Constitution and Article 8 ECHR. The other provision is Article 28 of the Act on ABW and AW concerning the scope in which ABW is authorised to obtain data referred to in Articles 180c and Article 180d TL but is not obliged to dispose of data that are insignificant for the conducted proceedings. In the Ombudsman's opinion, the provision is in conflict with Article 51(2) in conjunction with Article 31(3) of the Constitution of the Republic of Poland.[20]

The Ombudsman formulated five objections to the above-mentioned regulation. Firstly, the provisions discussed do not precisely regulate the aim of data retention. They only refer to the scope of ABW tasks or a general statement that the data are obtained in order to prevent or detect crimes. Secondly, the provisions do not indicate the category of persons whose right to professional confidentiality should be respected. Thirdly, the requirement for obtaining access to those data is not the exhaustion of other means of obtaining necessary information that are less intrusive in the sphere of citizens' rights and freedoms. Fourthly, the procedure of obtaining data in this mode is not subject to any external supervision. Finally, a considerable amount of data retained by ABW is not disposed of even when the data are no longer useful from the point of view of performed tasks.[21]

In his motion of 21 June 2012 filed to the Constitutional Tribunal, the Prosecutor General challenged the conformity of Article 28(1(1)) in conjunction with Article 5

---

[19] The content of the motion was originally broader. For the purpose of this article, it is important to discuss only those issues that concern the provisions of the Act on ABW and AW. However, apart from the provisions of this Act, the Ombudsman also questioned the provisions of other acts, namely Article 36b(5) of the Act on FC, Article 18 of the Act on CBA and Article 32 of the Act on MCS and MIS, concerning the scope in which they allow that data referred to in Articles 180c and 180d TL be obtained and do not envisage disposal of data that are insignificant for the conducted proceedings. In the Ombudsman's opinion, the provisions are in conflict with Article 51(2) in conjunction with Article 31(3) of the Constitution. The content of the provisions questioned is similar. Based on them, the Police and state protection services are granted competence to obtain and process data referred to in Articles 180c and 180d TL in order to prevent and detect crimes or fulfil the statutory tasks of those services.

[20] It is worth noting that on 27 April 2012, the Ombudsman filed another motion to the Constitutional Tribunal concerning data retention and their provision for the Customs Service. On 1 September 2011 and on 8 May 2012, the President of the Constitutional Tribunal ruled the two Ombudsman's motions should be joined and examined together.

[21] See, the motion of the Ombudsman to the Constitutional Tribunal of 1 August 2011: http://db.trybunal.gov.pl/sprawa/sprawa_pobierz_plik62.asp?plik=F–274604174/ K_23_11_Wns_2011_06_29.pdf&syg=K%2023/11 [accessed on 10 June 2016].

(1(2a)) of the Act on ABW and AW as far as it uses a phrase "and other crimes against the security of the state" as well as Article 28(1(1)) in conjunction with Article 5 (1(2b and 2c)) and Article 5(1(5)) of the Act on ABW and AW with Articles 2, 47 and 49 in conjunction with Article 31(3) of the Constitution and Article 8 ECHR.[22] The provisions challenged entitle the Internal Security Agency

[22] In the same way as in case of the Ombudsman's motion, due to the aim of this article, the analysis of issues other than the provisions of the Act on ABW and AW is insignificant and is not conducted here. However, in order to be reliable, it is necessary to indicate that the Prosecutor General also questioned the conformity of the provisions listed below with Article 2, Article 47 and Article 49 in conjunction with Article 31(3) of the Constitution and Article 8 ECHR: Article 20c(1) of the Act on the Police in conjunction with: Article 212 §§1 and 2, Article 216 §§1 and2, Article 217 §1, Article 221, Article 278 §§1–3 and 5, Article 284 §§1–3, Article 288 §§1 and 2 and Article 290 §1 CC, Article 45, Article 46(1), Article 49 and Article 49a of the Act of 26 January 1984: Press law, Journal of Laws [Dz.U.] No. 5, item 24, as amended; with Article 34(2), (3) and (4) of the Act of 16 April 2004 on construction products, Journal of Laws [Dz.U.] No. 92, item 881, as amended; Article 33 of the Act of 25 February 2011 on chemical substances and their mixtures, Journal of Laws [Dz.U.] No. 63, item 332, as amended; Article 77(2), (2a) and (3) of the Act of 11 March 2004 on protection of animal health and eliminating contagious diseases in animals, Journal of Laws [Dz.U.] of 2008, No. 213, item 1342, as amended, and in conjunction with Article 52(2) and (4) of the Act of 13 October 1995: Hunting law, Journal of Laws [Dz.U.] of 2005, No. 127, item 1066, as amended; Article 10b(1) of the Act on the Border Guard in conjunction with: Article 212 §§1 and 2, Article 216 §§1 and 2, Article 217 §1, Article 221, Article 278 §§1–3 and 5, Article 284 §§1–3, Article 288 §§1 and 2 and Article 290 §1 CC, Article 45, Article 46(1), Article 49 and Article 49a of the Press law, Article 34(2), (3) and (4) of the Act on construction products, Article 33 of the Act on chemical substances and their mixtures, Article 77(2), (2a) and (3) of the Act on protection of animal health eliminating contagious diseases in animals, and in conjunction with Article 52(2) and (4) of the Hunting law; Article 30(1) of the Act on MP, in conjunction with: Article 212 §§ and 2, Article 216 §§1 and 2, Article 217 §1, Article 221, Article 278 §§1–3 and 5, Article 284 §§1–3, Article 288 §§1 and 2 and Article 290 §1 CC, with Article 60 §§2 and 3, Article 61 §1, Article 62 §§1, 3 and 4, Article 80 §§1 and 2, Article 93 §§2 and 3, Article 95 §1, Article 108 §2 and Article 109 FPC, Article 45, Article 46(1), Article 49 and Article 49a of the Press law, with Article 34(2), (3) and (4) of the Act on construction products, Article 33 of the Act on chemical substances and their mixtures, Article 77(2), (2a) and (3) of the Act on protection of animal health and in conjunction with Article 52(2) and (4) of the Hunting law; Article 36b(1(1)) of the Act on FC in conjunction with Article 60 §§2 and 3, Article 61 §1, Article 62 §§1, 3 and 4, Art. 80 §§1 and 2, Article 93 §§2 and 3, Article 95 §1, Article 108 §2 and Article 109 FPC; Article 36b(1(1)) in conjunction with Article 2(1(12)) of the Act on FC, in conjunction with Article 85 §4, Article 86 §4, Article 87 §4, Article 88 §3, Article 89 §3, Article 90 §3, Article 91 §4, Article 92 §3, Article 94 §3, Article 95 §2 and Article 96 §1 FPC and in conjunction with Article 100(1) and Article 101(1) of the Act of 19 March 2004: Customs law, Journal of Laws [Dz.U.] of 2004, No. 68, item 662, as amended; Article 32(1(1)) in conjunction with Article 5(1(1a)) of the Act on MCS and MIS in the scope related to the phrase "and also other acts and international agreements"; Article 32(1(1)) in conjunction with Article 5(1(1g)) of the Act on MCS and MIS in the scope related to the phrase "and other than laid down in (a) to (f), against the security of the state defence potential, the Armed Forces of the Republic of Poland and organisational units of the Ministry of National Defence, and the states ensuring reciprocity"; Article 32(1(1)) in conjunction with Article 5(1(9) of the Act on MCS and MIS; Article 18(1(1)) in conjunction with Article 2(1(2)) of the Act on CBA in conjunction with Article 4, Article 12(3) to (6), Article 13 and Article 15 of the Act of 21 August 1997 on the limitation on business activities conducted by persons holding public posts, Journal of Laws [Dz.U.] of 2006, No. 216, item 1584, as amended; Article 18 (1(1)) in conjunction with Article 2(1(5)) of the Act on CBA in conjunction with Article 8(1) and (3) and Article 10(1), (2), (5) and (6) of the Act on the limitation on business activities conducted by persons holding public posts, with Article 35(1) of the Act of 9 May 1996 on the mandate of an MP and a senator, Journal of Laws [Dz.U.] of 2011, No. 7, item 29, as amended; with Article 87 §1 of the Act of 27 July 2001: Law on the system of common courts, Journal of Laws [Dz.U.] of 2001, No. 98,

to retain and process telecommunications data concerning persons suspected of committing crimes of low social harmfulness. In the Prosecutor General's opinion, they constitute disproportional interference into constitutionally protected status of an individual. The indicated catalogue of illegal acts does not substantiate limiting constitutional rights to privacy and secrecy of communication.

3. CONSTITUTIONAL TRIBUNAL JUDGEMENT CONCERNING ABW AND AW

The system of data retention by telecommunications businesses developed by the provisions of the Polish law is an important tool in the state bodies' fight against criminality. As such, it matches European regulations in this field. The system is not, however, a perfect tool. Quite the contrary, it is necessary to introduce far-reaching changes to the system so that the statutory regulations comply with the provisions of the Constitution of the Republic of Poland. Many conclusions concerning that can be drawn from the Constitutional Tribunal judgement of 30 July 2014 (K 23/11). Having examined the motions of the Ombudsman and the Prosecutor General, the Tribunal held that Article 28(1(1)) of the Act on ABW and AW is in conflict with Articles 47 and 49 in conjunction with Article 31(3) of the Constitution because it does not lay down independent supervision of the provision of telecommunications data referred to in Articles 180c and 180d TL. Moreover, the Tribunal held that Article 28 of the Act on ABW and AW in the scope in which it does not envisage disposal of data insignificant for conducted proceedings is in conflict with Article 51(2) in conjunction with Article 31(3) of the Constitution. At the same time, the loss of binding force of the provisions that are in conflict with the Constitution of the Republic of Poland was postponed for a period of 18 months after its promulgation in Journal of Laws (Dziennik Ustaw [Dz.U.]).

---

item 1070, as amended; with Article 38 of the Act of 23 November 2002 on the Supreme Court, Journal of Laws [Dz.U.] of 2002, No. 240, item 2052, as amended; with Article 49a(1) of the Act of 20 June 1985 on the public prosecution office, Journal of Laws [Dz.U.] of 2011, No. 270, item 1599, as amended; with Article 24h(1) of the Act of 8 March 1990 on commune (*gmina*) self-government, Journal of Laws [Dz.U.] of 2001, No. 142, item 1591, as amended; with Article 25c(1) of the Act of 5 June 1998 on county (*powiat*) self-government, Journal of Laws [Dz.U.] of 2001, No. 142, item 1592, as amended and in conjunction with Article 27c(1) of the Act of 5 June 1998 on voivodeship self-government, Journal of Laws [Dz.U.] of 2001, No. 142, item 1590, as amended; Article 18(1(1)) in conjunction with Article 2(1(3)) of the Act on CBA in conjunction with Article 1(1) and (2) of the Act of 21 June 1990 on the refund of benefits unlawfully obtained at the expense of the State Treasury or other state legal persons, Journal of Laws [Dz.U.] of 1990, No. 44, item 255, as amended; Article 18(1(1)) in conjunction with Article 2(1(4)) of the Act on CBA in conjunction with Article 200 of the Act of 29 January 2004: Public procurement law, Journal of Laws [Dz.U.] of 2010, No. 113, item 759, as amended; Article 46(1), Article 75(1) to (4) and Article 110(1) of the Act of 2 July 2004 on freedom of business activity, Journal of Laws [Dz.U.] of 2010, No. 220, item 1447, as amended and in conjunction of Article 3(1), Article 20a(1) to (3), Article 3la, Article 36(1), Article 39(1) and Article 69e of the Act of 30 August 1996 on commercialisation and privatisation, Journal of Laws [Dz.U.] of 2002, No. 171, item 1397, as amended; Article 18(1(1)) in conjunction with Article 2(1(6 and 7)) of the Act on CBA; Article 75d(1) in conjunction with para. 5 of the Act on CS in conjunction with Article 108 §2 and Article 109 FPC.

In the justification of its judgement, the Constitutional Tribunal explained that Article 28(1(1)) of the Act on ABW and AW, unlike the provisions of other acts (including the Act on the Police or the Act on fiscal control), excludes the obligation to obtain a court's consent, namely an obligation to issue a decision granting permission for the provision of telecommunications data to ABW officers. At the same time, the legislator did not envisage any alternative mechanisms of independent control over the process of obtaining data by ABW officers, which might be recognised as not meeting constitutional standards.

The Constitutional Tribunal did not determine what this control should be like and which body should perform it. The Tribunal only suggested that the introduction of a follow-up control as a rule should not be excluded. Interception and provision of various types of data can cause different interference into human rights and freedoms, and thus justify certain differentiation of mechanisms of control in relation to particular types of data. Regulating this mechanism, the legislator should especially take into account the specificity of particular services' operations and their statutory scope of tasks, urgent situations in which fast obtaining of telecommunications data may be indispensable for preventing the commission of crime or its fast detection. However, the Tribunal noticed arguments for the introduction, in some cases, of prior control. For example, it is necessary to mention the access to telecommunications data of persons doing jobs of public trust or situations when the services do not need to act urgently.

As the Tribunal noticed, the legislator granted ABW the right to obtain telecommunications data in a very broad range. It does not only concern recognition, detection and prosecution of crimes (which is regulated in Article 5(1(2)) of the Act on ABW and AW), but also other tasks referred to in Article 5(1) of the Act on ABW and AW. These include: recognition and fight against threats to internal security of the state and its constitutional order, especially sovereignty and international position, independence and inviolability of its territory as well as the state defence and prevention of such threats (para. 1), implementation, within the scope of its competence, of tasks connected with the protection of classified information and the fulfilment of the function of the national security authority in the field of the protection of classified information in international relations (para. 3), obtaining, analysing, processing and providing relevant state bodies with information that can be of crucial importance for the internal security of the state and its constitutional order (para. 4), and undertaking other activities specified in other acts and international agreements (para. 5). At the same time, some tasks such as recognition and detection listed in Article 5(1(2) of the Act on ABW and AW and prevention of those crimes were formulated in a very general way and, as a result, specific circumstances in which ABW officers may be given access to telecommunications data cannot be determined based o them.

The Constitutional Tribunal also emphasised that courts do not have to have control over the provision of telecommunications data. However, it is absolutely necessary for that supervisory body to be independent from the government and not to be in direct or indirect command hierarchy relations with the officers obtaining data.

Justifying its judgement, the Constitutional Tribunal emphasised that just the relatively general specification of the tasks of the public authority body (in this case ABW) is not in conflict with the Constitution. The problem occurs, however, when

the public authority bodies fulfilling those tasks can undertake activities interfering in individuals' rights and freedoms by obtaining data in a secret way. Whenever a public authority body is authorised to obtain information about an individual's private life, including communications data, it is necessary for the legislator to precisely determine the subjective scope of the possibilities of fulfilling this task. Taking into consideration an extremely broad range of circumstances in which ABW may be provided communications data, the exclusion of the necessity to obtain a court's permission and the lack of obligation to obtain a permission from any other independent body, the Tribunal held that the provision challenged does not contain even the minimum procedural guarantee necessary from the perspective of the compliance with the Constitution. In the Tribunal's opinion, this circumstance is sufficient to recognise that Article 28(1(1)) of the Act on ABW and AW is in conflict with Articles 47 and 49 in conjunction with Article 31(3) of the Constitution because it does not stipulate independent control over the provision of communications data referred to in Articles 180c and 180d TL.

It must be noted that the Constitutional Tribunal did not refer to all the objections filed by the Ombudsman and the Prosecutor General. There was no comment on the complaint that obtaining communications data is not subsidiary in nature. It is admissible in every case when the authorised services request that. The requirement for providing access to data is not the exhaustion of other less intrusive legal measures not violating privacy and secrecy of correspondence.

On the other hand, the Tribunal made detailed comments on the legislator's failure to specify special requirements for the protection of information that is subject to professional privilege (legal professional privilege, journalistic privilege, physician-patient privilege).[23] The Constitutional Tribunal explained that there are no grounds for unconditional exclusion of admissibility of surveillance operations, including obtaining information in the interception mode, for some categories of entities.

In the Tribunal's opinion, the Constitution of the Republic of Poland does not stipulate any subjective exemptions in this field. This does not mean, however, admissibility of obtaining information from everyone in the same mode, to the same extent and following the same rules. Persons performing the jobs of public trust should be subject to higher constitutionality standards of regulations concerning a low-key mode of obtaining information about them. Professional privilege and a guarantee that it will be respected in court proceedings are instruments of protecting trust. They include, inter alia, conditional and unconditional bans on

[23] With regard to the objection formulated by the Ombudsman, the Tribunal explained in its judgement substantiation that no arguments were presented to support it. The Ombudsman's motion does not meet, in the Tribunal's opinion, formal requirements laid down in Article 32(1(4)) of the Act on the Constitutional Tribunal, i.e. it does not contain justification and evidence supporting the objection. As a result, the proceedings in this matter shall be discontinued pursuant to Article 39(1(1)) of the Act on the Constitutional Tribunal. On the other hand, referring to the similar objection presented by the Prosecutor General, despite some deficiencies noted in argumentation, the Tribunal held that his intentions were clear enough. The content of the motion indicates that the essence of the objections presented consists in the imprecise regulation of operational control and failure to ensure sufficient protection of constitutional freedoms and rights of individuals, in the interest of which the obligation to keep professional confidentiality and the bans on evidence were established.

evidence in court proceedings. The Constitutional Tribunal drew attention to the fact that professional privilege and evidence bans in court proceedings that are strictly connected with it are not autotelic values.

Although confidentiality of persons doing the jobs of public trust must always be seen as an integral value of a democratic state ruled by law, their basic function is to protect constitutional freedoms and rights of individuals providing them with private information to be treated with discretion (compare the Constitutional Tribunal judgement of 2 July 2007, K 41/05, Part III, para. 7). Each time, professional privilege should be seen as an expression of the protection of an individual's freedoms and rights, especially the right to protect privacy (Article 47), information provision autonomy (Article 51(1)), the right to defence (Article 42(2)), the right to hearing before a court (Article 45(1), the freedom of conscience and religion (Article 53) or freedom to acquire information, including the freedom of the press (Article 54(1) of the Constitution). Because of this, referring to a solicitor's privilege, the Tribunal emphasised that not solicitors but their clients have the right to privacy and information confidentiality. However, a solicitor is obliged to respect that right (see, the Constitutional Tribunal judgement of 22 November 2004).[24] The Constitutional Tribunal explained that this interpretation also applies to other professional privileges. Moreover, it explained that the collision between the two values does not influence the fact that the protection of an individual's freedoms and rights, and indirectly also the professional privilege, must always be a priority. In relation to this area, the Tribunal referred to its former judgements[25] and explained that "general exclusion of entities obliged to keep professional secrets from operational control as well as exclusion of information recognised as professional secrets that are absolutely unavailable in this mode would lead to considerable difficulties in the collection of evidence in some types of crime, e.g. those committed with the use of modern technologies".

On this basis, the Tribunal held that "the point of gravity is moving towards ensuring some procedural guarantees eliminating groundless acquisition by policing entities and state security services of information that, because of its content and circumstances of its provision, should be protected by law". In the Tribunal's opinion, a model solution to this conflict between the two values is laid down in Article 180 §2 of the Criminal Procedure Code (CPC), which consists in a mechanism of exemption from professional confidentiality in a situation when it is necessary for the benefit of justice institution and a given circumstance cannot be established in any other way. Similar legal solutions should, in the Tribunal's opinion, also apply to the protection of professional privilege in the course of operational-surveillance activities, including operational control. Indeed, there are no substantiated grounds for using lower standards than those laid down in criminal procedure provisions. Just the opposite, it is necessary to recognise that those standards, because of the extra-procedural confidential character of control, should be at least identical to the standards of criminal proceedings.

---

[24] SK 64/03, OTK ZU No. 10/A/2004, item 107, Part III, para. 3.

[25] See, the Constitutional Tribunal judgements of: 22 November 2004, SK 64/03, Part III, para. 3; 2 July 2007, K 41/05, Part III, para. 7; 13 December 2011, K 33/08, OTK ZU No. 10/A/2011, item 116, Part III, para. 6.4.

As it has been explained above, based on the Constitutional Tribunal judgement of 30 July 2014, K 23/11, the provision of Article 28 of the Act on ABW and AW, in the former wording, in the scope in which it did not envisage disposal of data insignificant for the conducted proceedings, was recognised to be in conflict with Article 51(2) in conjunction with Article 31(3) of the Constitution. The Constitutional Tribunal explained that the requirement for obtaining information on individuals, including their communications data, in a secret way is the establishment of the procedure of immediate selection and disposal of useless and inadmissible material. Such a solution prevents unauthorised use of legally collected information by the state services and their retention just in case they might be useful for other purposes. Not only a single instance of an individual's data acquisition (inter alia, in the mode laid down in Article 28(1) of the Act on ABW) but also each successive instance of processing of those data, including their retention and subsequent use in the curse of other proceedings, constitute interference in individuals' privacy. The legislator added a new provision of para. 7 to Article 28. In accordance with it, data referred to in para. 1 that are insignificant for criminal proceedings or the state security must be disposed of without delay, in the presence of a commission and be subject to reporting. The legislator did not stipulate the disposal of all other communications, postal and Internet data other than those that are insignificant for the conducted criminal proceedings. This way, the legislator allowed the retention of data specified as "significant for the state security".

4. NEW WORDING OF ARTICLE 28 ACT ON ABW AND AW

The subject of the Tribunal's judgement, the provision of Article 28 of the Act on ABW and AW did not regulate the proceedings concerning telecommunications data after retention pursuant to Article 28(1) of the Act on ABW and AW. The legislator did not lay down the procedure of dealing with the data collected in this mode. Thus, there are no legal grounds for relevant use of the provisions regulating disposal of data collected in the course of operational control or the provisions of CPC regulating interception and recording of conversations (Article 237 and the following CPC). This meant that on the basis of Article 28 of the Act on ABW, there were no regulations concerning verification and disposal of useless data. Therefore, it was not possible to exclude the retention of useless data in conducted proceedings, in the course of which they were requested, or in any other constitutionally justified purposes. The Constitutional Tribunal does not negate the admissibility of further retention (after their analysis and recognition of potential uselessness in the conducted proceedings in a given case) of communications data concerning foreigners being under the authority of the Republic of Poland, especially in case there are serious and justified suspicions that they might be involved in activities endangering the state security, including terrorism and organised crime. Such differentiation of the level of protection has grounds mainly in Article 51(2) and Article 37(2) of the Constitution.

In order to adjust the provisions derogated by the Constitutional Tribunal, the Act amending Act on the Police and some other acts was passed on 15 January

2016.[26] The Act adopted the new wording of Article 28(2)–(3) of the Act on ABW and AW. Pursuant to Article 28(2), a telecommunications business, a postal operator or a provider of electronic services are required to provide data referred to in Article 28(1) of the Act on ABW and AW free of charge:

1) to an ABW officer indicated in a written motion of the ABW Head or a person authorised by this body;
2) to an ABW officer being authorised in writing by the ABW Head on his verbal request;
3) to an ABW officer authorised by the ABW Head referred to in para. 2 via electronic telecommunications network.

In case of data provision based on a verbal request of an ABW officer authorised in writing by the ABW Head, the provision of data is conducted without the participation of the employees of the telecommunications business, postal operator or provider of electronic services or with their necessary cooperation, provided that the agreement between the ABW Head and this entity envisages that (Article 28(3) of the Act on ABW and AW).

Providing ABW with data referred to in Articles 180c and 180d TL may take place via telecommunications network, provided that the network safeguards:

1) the possibility of establishing the ABW officer obtaining data, their type and time when they have been obtained;
2) technical and organisational measures preventing an unauthorised person from getting access to those data (Article 28(4) of the Act on ABW and AW).

5. JUDICIAL CONTROL OVER THE ACQUISITION OF TELECOMMUNICATION DATA BY ABW

One of the objections of the Constitutional Tribunal concerning the Act on ABW and AW with regard to examination resulting from the motions filed by the Ombudsman and the Prosecutor General was the lack of judicial control over the acquisition of telecommunications data by ABW officers. It seems that it is the most important issue, which the Constitutional Tribunal discussed in its judgement. Because of its significance, the issue needs a separate analysis. The provision of telecommunications data for special services is of key importance from the perspective of interference into constitutional rights and freedoms, inter alia, the secrecy of correspondence and the freedom of communication. Therefore, it must be deemed that depriving courts of the control over those procedures and, in fact what the Tribunal noted, the lack of regulations safeguarding whatever control of the process independent from the government are highly undesirable phenomena. This does not match any constitutional standards established by the Polish legislator. Legislation does not provide any judicial or any other alternative mechanism of independent control over the acquisition of telecommunications data by ABW officers. Thus, due to the fact that the catalogue of circumstances that allow ABW officers to obtain telecommunications data is really broad, it is necessary to state that there were no even the minimum procedural guarantees that the constitutional standards were respected in this area.

[26] Journal of Laws [Dz.U.] of 2016, item 147.

In order to solve that problem, based on the discussed the Act of 15 January 2016, a new provision of Article 28a was added to the Act on ABW and AW. In accordance with that provision, the District Court in Warsaw has control over the acquisition of telecommunications, postal or Internet data by ABW officers (para. 1). In accordance with the provisions on the protection of classified information, the ABW Head provides the Court with mid-year reports on:

1) the number of cases of obtaining telecommunications, postal or Internet data and the type of those data in the period covered;
2) legal classification of acts in connection with which telecommunications, postal or Internet data have been requested (para. 2).

Within this control, the Court may get to know the materials justifying the provision of telecommunications, postal or Internet data for ABW. The Court informs the ABW Head about the results of the control within the period of 30 days from its completion (para. 3).

Thus, based on Article 28a of the Act on ABW and AW, the legislator introduced the preferred follow-up control of the provision of telecommunications data for ABW. In its judgement of 30 July 2014, K 23/11, the Constitutional Tribunal indicated that the general constitutional standard does not determine what the procedure of granting access to telecommunication data should look like, especially whether it should be necessary to obtain a permission for this provision in relation to every type of arrested data referred to in Articles 180c and 180d TL. Not all data of this type result in the same intensity of interference in human rights and freedoms. In the Constitutional Tribunal's opinion, the introduction of the follow-up control over the provision of telecommunications data in the course of operational-surveillance activities as a rule is not out of the question. Regulating this mechanism, the legislator should take into consideration, inter alia, the specificity of activities and the statutory scope of tasks of particular services, urgent situations when fast acquisition of telecommunications data is indispensible to prevent the commission of crime or its detection. In accordance with the constitutional principle of efficiency in the work of public bodies, which is laid down in the Preamble, it is necessary to create a mechanism allowing services responsible for the state security and public order to efficiently combat threats. However, the Tribunal notes arguments for the introduction of prior control in some cases. It may especially concern access to telecommunications data of persons doing jobs of public trust or when there is no urgent need for the services to act. The legislator should weigh the issues properly.

A few questions arise in relation to the new regulation. Firstly, it is necessary to analyse the effectiveness of the solution adopted. It is important to what extent judicial control will be real and not just illusory, because control is not obligatory but optional. Data that are subject to control will be provided periodically, in mid-year periods. The district court responsible for the control may, within its competence, get acquainted with the material that substantiates giving ABW access to telecommunications data, which will result in the submission of a court's report to ABW. The court's activity aimed at verifying the appropriateness of providing ABW with telecommunications data ends with the court's report submission. The legislator did not determine procedural issues related to potential further activities in

case a court recognises violation of regulations in the area. A court, having finished the control, may in fact only inform the service concerned about its control results. However, a court has no competence to rule the disposal of the data retained.[27]

Secondly, it is necessary to consider whether, from the point of view of the protection of citizens' rights and freedoms, but also in the interest of the services, it would not be a better solution to introduce, as a rule, a prior judicial control. It does not mean abandoning the follow-up control but its application in urgent situations requiring that ABW should act without delay. Such a solution would certainly improve the appropriateness of motions developed by ABW bodies and other services as well as would increase their number.

The above-presented doubts are also discussed in the CJEU judgement of 8 April 2014. The Court held that access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body. A court or an independent administrative body should limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued.[28] The CJEU clearly mentions prior control performed by an independent body.

It is also worth highlighting that in accordance with Article 28a(5) of the Act on ABW and AW, obtaining data based on Article 28a(1) of the Act on ABW and AW, is not subject to control. Pursuant to this provision, it concerns a broad scope of information including data:

1) from the list referred to in Article 179(9) TL;
2) referred to in Article 161 TL;
3) in case of a user who is not a natural person, the number of the network end device and the head office or location where business is done, the company or the name and organisational form of this user;
4) in case of public land-line telecommunications networks, also the name of town and street – where there is the network end device provided for the user.

6. CONCLUSIONS

The importance of case law for the practice of applying specified legal institutions does not raise doubts. Thus, it can be said that there is more to court judgements than meets the eye in every legal regulation because they shape the application of law in practice. It does not only concern common courts' decisions but also the Constitutional Tribunal judgements, to which the legislator assigned a basic role of examining and adjudicating on hierarchical conformity of legal acts.[29]

---

[27] A similar solution was adopted in case of other entities authorised to conduct operational control. See, Article 18a of the Act on CBA; Article 36ba of the Act on FC; Article 20ca of the Act on the Police; Article 75da of the Act on CS; Article 10ba of the Act on BG; Article 32a Act on MCS and MIS; Article 30b of the Act on MP.

[28] Theses 60–62 of the CJEU judgement of 8 April 2014, OJ of 2014, L 105.

[29] See M. Zubik, *Status prawny sędziego Trybunału Konstytucyjnego* [Legal status of a judge of the Constitutional Tribunal], Warsaw 2011, p. 22.

The Constitutional Tribunal does not only establish but also often provides content in constitutional norms, which, as a rule, are at a higher level of generality than in case of standard acts. It should be acknowledged that the Tribunal is not only a restorer of the content of legal norms but, as a result of the binding power of its judgements, actually co-creates the content of a legal norm for the needs of constitutional practice. Moreover, in case of the assessment of the constitutionality of acts, it has a jurisdictional monopoly. Those entitlements of the Tribunal become especially significant in a situation when an act reviewed by the Tribunal implements constitutional provisions. There are no doubts that the Act on ABW and AW with regard to retention and provision of telecommunications data belongs to this category. It introduces limits on the exercise of the constitutional right to communication freedom, which, like any other freedoms, cannot be unlimited in nature. This would negate its essence and might lead to conflicts consisting in one person's interference into the freedom of another person or in the instrumental treatment and, as a result, the abuse of due freedom. The constitutional legislator, being aware of those threats, stipulated two constitutional bases for the limitation of communication freedom. One of them is laid down in Article 49 of the Constitution, i.e. the provision establishing this freedom. The content of this provision stipulates that any limitation to the freedom of communication may be imposed only in cases and in the manner specified by statute.[30] Therefore, the statutory limitation of the constitutional freedom of communication may be introduced when the exercise of this freedom might lead to the infringement of the rights and freedoms of another individual and other values protected by the Constitution.

Another basis is laid in Article 31(3) of the Constitution, which formulates general limits to the use of the constitutional rights and freedoms.[31] The provision is composed of two parts. The first of them is a general clause referring to the limitations upon the exercise of the constitutional freedoms and rights. The legislator adopted a principle commonly accepted in democratic constitutional systems, in accordance with which determination of boundaries of constitutional rights and freedoms may take place only in statute.[32] The other part of Article 31(3) of the

---

[30] The norm laid down in Article 49, 2nd sentence of the Constitution indicates three consequences. Firstly, the legislator has the constitutionally granted right to decide on the scope of communication freedom. Secondly, the only act which can admit interference in the freedom of communication, is statute. Thirdly, a standard act should establish specific cases and methods of limitation. Thus, there is a requirement of specificity excluding the possibility of using general clauses. See, the Constitutional Tribunal judgement of 12 December 2005, K 32/04, OTK-A No. 11, item 132, 2005.

[31] It reads as follows: "Any limitation upon the exercise of constitutional freedoms and rights may be imposed only by statute, and only when necessary in a democratic state for the protection of security or public order, or to protect the natural environment, health or public morals, or the freedoms and rights of other persons. Such limitations shall not violate the essence of freedoms and rights".

[32] Both in the literature and the case law, the phrase is interpreted similarly. Statute does not have to constitute the only source of limitation. There are situations admissible when only general elements of limitations are determined at the statute level. They are specified in detail in secondary legal acts, e.g. regulations or bylaws. Statutory regulations should, however, give those limitations basic shape and determine their scope. See, K. Wojtyczek, *Granice ingerencji ustawodawczej w sferę praw człowieka w Konstytucji RP* [Limits on statutory interference in the

Constitution is a specification of substantive premises admitting the limitation of rights and freedoms.[33] These are: security or public order, protection of the natural environment, health or public morals, or the freedoms and rights of other persons.

As the judgement of 30 July 2014, K 23/11, explains, the Constitutional Tribunal questioned the provisions of the Act on ABW and AW in connection with the legislator's failure to establish an independent system of controlling the provision of telecommunications data as well as disposing of data that are insignificant for the conducted proceedings. The judgement should be approved of. Firstly, every limitation upon the constitutional freedom to communicate is an exception to the constitutional principle and as such should be subject to control. In this area, it is necessary to agree with the proposal formulated in the literature, according to which the regulation of limitations on communication freedoms and their exercise should be subject to judicial review.[34] Secondly, having in mind that obtaining telecommunications data constitutes a departure from the secrecy of communication, which is a rule, it seems that immediate disposal of data that are insignificant for the proceedings is indispensible.

Making use of its entitlements, the Constitutional Tribunal ruled that the provisions recognised as unconstitutional should lose their legal force within the maximum period of 18 months after the promulgation of the judgement in the Journal of Laws. In the meantime, the legislator should undertake relevant legislative work in order to eliminate unconstitutional provisions. This is what actually happened. Based on Article 7 of the Act of 15 January 2016 amending the Act on the Police and some other acts, fulfilling the legal task assigned, the legislator introduced the required changes in the Act on ABW and AW, eliminating the provisions the Constitutional Tribunal recognised as unconstitutional.

BIBLIOGRAPHY

Banaszak B., *Konstytucja Rzeczypospolitej Polskiej. Komentarz* [Constitution of the Republic of Poland. Comentary], Warsaw 2012.

Garlicki L., *Uwagi do art. 49 Konstytucji RP* [Comments on Article 49 of the Constitution of the Republic of Poland], [in:] L. Garlicki (ed.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz* [Constitution of the Republic of Poland. Commentary], Vol. II, Warsaw 2002.

Kawałek K., Rogalski M. (ed.), *Prawo telekomunikacyjne. Komentarz* [Telecommunications law. Commentary], Warsaw 2010.

Kiziński M., *Retencja danych telekomunikacyjnych* [Retention of telecommunications data], Prokuratura i Prawo No. 1, 2016.

Wach M., *Zatrzymywanie danych telekomunikacyjnych przez dwa lata w celach bliżej nieokreślonych a prawo do prywatności* [Retention of telecommunications data for two years for undefined reasons and the privacy right], Radca Prawny a scientific supplement No. 115–116, 2011.

---

area of human rights under the Constitution of the Republic of Poland], Kraków 1999, p. 110; the Constitutional Tribunal judgement of 12 January 2000, P 11/98, OTK No. 1, item 3, 2000.

[33] See, the Constitutional Tribunal judgement of 25 February 1999, K 23/98, OTK No. 2, item 25, 1999.

[34] See, B. Banaszak, *Konstytucja Rzeczypospolitej Polskiej. Komentarz* [Constitution of the Republic of Poland. Comentary], Warsaw 2012, p. 256.

Wojtyczek K., *Granice ingerencji ustawodawczej w sferę praw człowieka w Konstytucji RP* [Limits on statutory interference in the area of human rights under the Constitution of the Republic of Poland], Kraków 1999.

Zubik M., *Status prawny sędziego Trybunału Konstytucyjnego* [Legal status of a judge of the Constitutional Tribunal], Warsaw 2011.

Legal regulations

Constitution of the Republic of Poland of 2 April 1997, Journal of Laws [Dz.U.] of 1997, No. 78, item 483, as amended.

Convention for the Protection of Human Rights and Fundamental Freedoms opened for signature in Rome on 4 November 1950 and force in 1953, Journal of Laws [Dz.U.] of 1993, No. 61, item 284, as amended.

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, OJ, L 105.

Act of 26 January 1984: Press law, Journal of Laws [Dz.U.] No. 5, item 24, as amended.

Act of 8 March 1990 on commune (*gmina*) self-government, Journal of Laws [Dz.U.] of 2001, No. 142, item 1591, as amended.

Act of 6 April 1990 on the Police, Journal of Laws [Dz.U.] of 2015, item 355, as amended.

Act of 12 October 1990 on the Border Guard, Journal of Laws [Dz.U.] of 2014, item 1402, as amended.

Act of 28 September 1991 on fiscal control, Journal of Laws [Dz.U.] of 2016, item 720, as amended.

Act of 13 October 1995: Hunting law, Journal of Laws [Dz.U.] of 2005, No. 127, item 1066, as amended.

Act of 9 May 1996 on the mandate of an MP and a senator, Journal of Laws [Dz.U.] of 2011, No. 7, item 29, as amended.

Act of 30 August 1996 on commercialisation and privatisation, Journal of Laws [Dz.U.] of 2002, No. 171, item 1397, as amended.

Act of 6 June 1997: Criminal Procedure Code, Journal of Laws [Dz.U.] No. 89, item 555, as amended.

Act of 21 August 1997 on the limitation on business activities conducted by persons holding public posts, Journal of Laws [Dz.U.] of 2006, No. 216, item 1584z, as amended.

Act of 5 June 1998 on voivodeship self-government, Journal of Laws [Dz.U.] of 2001, No. 142, item 1590 as amended.

Act of 5 June 1998 on county (*powiat*) self-government, Journal of Laws [Dz.U.] of 2001, No. 142, item 1592 as amended.

Act of 10 September 1999: Fiscal Penal Code, Journal of Laws [Dz.U.] of 2013, item 186, as amended.

Act of 27 July 2001: Law on the system of common courts, Journal of Laws [Dz.U.] of 2001, No. 98, item 1070 as amended.

Act of 24 August 2001 on the Military Police and military order keeping bodies, Journal of Laws [Dz.U.] of 2016, item 96, as amended.

Act of 24 May 2002 on the Internal Security Agency (ABW) and the Intelligence Agency (AW), Journal of Laws [Dz.U.] of 2015, item 1929, as amended.

Act of 23 November 2002 on the Supreme Court, Journal of Laws [Dz.U.] of 2002, No. 240, item 2052, as amended.

Act of 29 January 2004: Public procurement law, Journal of Laws [Dz.U.] of 2010, No. 113, item 759, as amended.
Act of 11 March 2004 on protection of animal health and eliminating contagious diseases in animals, Journal of Laws [Dz.U.] of 2008, No. 213, item 1342, as amended.
Act of 19 March 2004: Customs law, Journal of Laws [Dz.U.] of 2004, No. 68, item 662, as amended.
Act of 16 April 2004 on construction products, Journal of Laws [Dz.U.] No. 92, item 881, as amended.
Act of 2 July 2004 on freedom of business activity, Journal of Laws [Dz.U.] of 2010, No. 220, item 1447, as amended.
Act of 9 June 2006 on the Central Anti-Corruption Bureau (CBA), Journal of Laws [Dz.U.] of 2016, item 1310, as amended.
Act of 9 June 2006 on Military Counterintelligence and Military Intelligence Service, Journal of Laws [Dz.U.] of 2016, item 1318, as amended.
Act of 27 August 2009 on Customs Service, Journal of Laws [Dz.U.] of 2015, item 990, as amended.
Act of 25 February 2011 on chemical substances and their mixtures, Journal of Laws [Dz.U.] No. 63, item 332, as amended.
Act of 15 January 2016 on amendment to the Act on the Police and some other acts, Journal of Laws [Dz.U.] of 2016, item 147.
Regulation of the Minister of Infrastructure of 24 January 2003 on the fulfilment of operators' tasks in connection with defence, state security and security and public order, Journal of Laws [Dz.U.] No. 19, item 166, as amended.

Court judgements

Constitutional Tribunal judgement of 25 February 1999, K 23/98.
Constitutional Tribunal judgement of 12 January 2000, P 11/98.
Constitutional Tribunal judgement of 12 December 2005, K 32/04.
Constitutional Tribunal judgement of 30 July 2014, K 23/11.

Websites

Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180c i d ustawy prawo telekomunikacyjne [Obtaining and processing by the entitled entities of data from billings, information on location and other data defined in Article 180c and d of the Telecommunications law], http://www.nik.gov.pl/plik/id, 5421,vp,7038.pdf [accessed on 15 August 2016].
Motion of the Ombudsman to the Constitutional Tribunal of 1 August 2011, p. 15; http://db.trybunal.gov.pl/sprawa/sprawa_pobierz_plik62.asp?plik=F–274604174/K_23_11_Wns_2011_06_29.pdf&syg=K%2023/11 [accessed on 15 August 2016].
Fundacja Panoptykon, *Telefoniczna Kopalnia Informacji. Przewodnik* [Telecom Information Mine. A Guide], http://panoptykon. org/biblio/telefoniczna–kopalnia–informacji–przewodnik [accessed on 15 August 2016].

OBTAINING OF COMMUNICATIONS DATA BY THE INTERNAL SECURITY AGENCY AFTER THE CONSTITUTIONAL TRIBUNAL JUDGEMENT OF 30 JULY 2014

Summary

The Article aims to analyse the Constitutional Tribunal judgement of 30 July 2016 (file no. K 23/11), on the Internal Security Agency obtaining telecommunications billings and intercepting communications in order to obtain communications data. It is connected with the establishment of the legislator's legislative response to the content of the judgement and its recommendations as far as obtaining communications data by this agency is concerned. In order to conduct the analysis and meet the set objectives, the author uses a dogmatic-legal method and examines the content of legal acts and the Constitutional Tribunal judgements issued in relation to them. Based on that, it is established that the Constitutional Tribunal rightly recognised the provisions of the Act on the Internal Security Agency (ABW) and the Intelligence Agency (AW) as partly unconstitutional because the legislator did not envisage independent supervision of telecommunications data provision and did not regulate the destruction of data that are insignificant for conducted proceedings. Both deficiencies were rectified in the Act of 15 January 2016 amending the Act on the Police and some other acts.

Keywords: Telecommunications law, communications data, data retention, Internal Security Agency, Constitutional Tribunal

POZYSKIWANIE DANYCH TELEKOMUNIKACYJNYCH PRZEZ AGENCJĘ BEZPIECZEŃSTWA WEWNĘTRZNEGO PO WYROKU TRYBUNAŁU KONSTYTUCYJNEGO Z 30 LIPCA 2014 ROKU

Streszczenie

Celem tego artykułu jest analiza wyroku TK z dnia 30 lipca 2016 r. sygn. akt K 23/11 w sprawie bilingów i podsłuchów w zakresie, w jakim dotyczy on pozyskiwania danych telekomunikacyjnych przez Agencję Bezpieczeństwa Wewnętrznego. Wiąże się z tym ustalenie reakcji legislacyjnej ustawodawcy na treść tego wyroku i wytyczne trybunalskie w zakresie, w jakim odnosi się on do pozyskiwania danych telekomunikacyjnych przez tę właśnie służbę. Do przeprowadzenia badań nakierowanych na osiągnięcie założonych celów wykorzystano metodę dogmatyczno-prawną poprzez badanie treści aktów prawnych oraz wydawanego w tym zakresie orzecznictwa Trybunału Konstytucyjnego. Na podstawie przeprowadzonych rozważań ustalono, że Trybunał Konstytucyjny zasadnie uznał za niezgodne z Konstytucją przepisy ustawy o ABW i AW w zakresie, w jakim ustawodawca nie przewidział niezależnej kontroli udostępniania danych telekomunikacyjnych, jak również w zakresie, w jakim nie przewidziano zniszczenia danych niemających znaczenia dla prowadzonego postępowania. Oba te mankamenty zostały prawidłowo zmodyfikowane w ustawie z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji i niektórych innych ustaw.

Słowa kluczowe: Prawo telekomunikacyjne, dane telekomunikacyjne, retencja danych, Agencja Bezpieczeństwa Wewnętrznego, Trybunał Konstytucyjny