STORING AND PROVIDING ACCESS TO TELECOMMUNICATIONS DATA IN POLAND (DATA RETENTION)

UCHOVÁVANIE A POSKYTOVANIE PRÍSTUPU K TELEKOMUNIKAČNÝM ÚDAJOM (UCHOVÁVANIE ÚDAJOV)

Maciej Rogalski
Łazarski University

ABSTRACT
This article deals with the issue of providing access to telecommunications data in Poland upon request made by authorized entities, the court and the prosecutor in particular. The article outlines the obligations of telecommunications entrepreneurs, indicates entities authorized to request data access, specifies the scope of data to which access is provided and their storage time. The article also discusses some interpretative doubts as well as problems with the application of telecommunications law provisions related to data retention, possible solutions to the existing problems are also suggested.

ABSTRAKT
Článok sa zaoberá problematike poskytovania prístupu k telekomunikačným údajom v Poľsku na základe žiadosti oprávnených osôb, súdu, či prokurátora. V najväčšej miere sa zameriava na analyzovanie povinností súkromných telekomunikačných spoločností, rozoberá okruh subjektov oprávnených požadovať prístup k jednotlivým dátam, rovnako sa obsah článku zameriava aj na analýzu rozsahu údajov, ku ktorým môže byť umožnený prístup ako aj celkovú dobu archivovania takýchto údajov. Článok sa taktiež venuje aj určitým výkladovým nezrovnalostiam, rovnako aj problémom s aplikáciou telekomunikačného zákona týkajúceho sa uchovávania telekomunikačných údajov, pričom v článku sú obsiahnuté aj určíté návrhy na riešenie už existujúcich problémov v praxi.

INTRODUCTION

Under Polish law, the issues of providing access to telecommunications data for the purpose of pending court and prosecution proceedings are regulated by the criminal law procedure (Article 218-218b of the Code of Criminal Procedure[1]) (the "CCP") and by Article 179 and subsequent articles of the Telecommunications Law[2] (the "TL"). The issue of exercising surveillance over and recording telephone conversations, i.e. "interception" is regulated in Chapter 26 of the CCP, titled "Surveillance and recording conversations" (Articles 237-242 of the CCP). CCP provisions specify cases in which the surveillance and recording of telephone conversations is permitted, entities authorized to conduct the surveillance and the methods of conducting it. TL provisions specify the relevant obligations

[1] The Act of 6 June 1997 – Code of Criminal Procedure, Journal of Laws 1997, No 89, item 555 as amended.
[2] The Act of 16 July 2004 – Telecommunications Law, Journal of Laws 2004, No 171, item 1800 as amended.

of telecommunications entrepreneurs. In this article, the issue of providing access to telecommunications data is discussed only from the viewpoint of a telecommunications entrepreneur as an entity obliged to store telecommunications data and provide access to them.

Pursuant to Article 218(1) of the CCP, telecommunications entities are required to surrender to the court or public prosecutor, upon request included in their order, any data referred to in Article 180c and 180d of the TL if such data are relevant to the pending proceedings. This requirement refers to all telecommunications entities regardless of their legal form, entrepreneurial organisation, or ownership structure, and especially of whether they are private or public entities. Access to data specified in Article 180c and 180d of the TL is provided on condition that such data are relevant to the pending proceedings. In practice, the decision requiring access provision is based on the assumption that the data may be relevant to the proceedings. It is not possible, however, to confirm the relevance until the contents of such data have been revealed. Should the court or public prosecutor deem the retained correspondence or transmissions irrelevant to the proceedings, they should be immediately returned to the entity from which they were obtained (Article 218(3) of the CCP)[3].

1. OBLIGATIONS OF TELECOMMUNICATIONS ENTREPRENEURS

1. Obligations of telecommunications entrepreneurs related to the storage and retention of telecommunications data are set out in Article 180a of the TL. Provisions of this Article constitute national implementation of 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[4] ("Directive 2006/58/EC"). Data retention is especially intended to support the detection of crimes against defence, state security, public order and of fiscal offences.

Pursuant to Article 180a(1) of the TL, public telecommunications network operators and providers of publicly available telecommunications services are obliged, at their own expense, to:

1) retain and store data referred to in Article 180c of the TL, generated in a telecommunications network or processed by that operator or provider within the territory of the Republic of Poland, for a period of 12 months from the date on which a communication was successfully or unsuccessfully established and, at the end of this period, to destroy the data except those that have been accessed and preserved under separate provisions;
2) provide access to data referred to in item (1) to authorized entities in accordance with the rules set out by separate provisions;
3) protect data referred to in item (1) against accidental or unlawful destruction, loss or alteration, or unauthorized or unlawful storage, processing, access or disclosure.

"Data retention", a term used in Article 180a(1) of the TL, is not defined in the Telecommunications Law. The term corresponds, however, to the official translation of Directive 2002/58/EC. The obligation referred to in Article 180a(1) covers the data necessary to: 1) trace the network termination point, telecommunications terminal equipment and the end-user originating the call and to whom the call is made; 2) identify: a) the date and time of a call and its duration; b) type of a call; c) location of telecommunications terminal equipment

[3] P. HOFMAŃSKI, E. SADZIK, K. ZGRYZEK, *Kodeks postępowania karnego. Komentarz [The Code of Criminal Procedure. Comments]*, Vol. I, Warsaw 2011, 1233.
[4] Official Journal of the European Union, L 105, 13 April 2006.

used in public mobile communications network, which pertains both to successful and failed connections (Article 180c of the TL). This refers to data generated in a telecommunications network or processed by that operator or provider within the territory of the Republic of Poland. Pursuant to Article 180a(1)(1) of the TL, it is not necessary to retain and record data concerning failed connections. This regulation is in line with Article 161 of the TL which only allows to record and store data which refer to a particular service or are necessary for the service to be performed. Telecommunications entrepreneurs do not record nor process data concerning failed connections.

Public telecommunications network operators and providers of publicly available telecommunications services are obliged to provide access to data referred to in Article 180(1)(1) of the TL to authorized entities as well as to the courts and public prosecutor. The procedure for making such data available to the courts and the public prosecutor is outlined in the Code of Criminal Procedure (Article 180a(1)(2) of the TL). As far as the remaining entities are concerned, the relevant procedures are covered by separate provisions.

Pursuant to Article 180a(1)(2), telecommunications entrepreneurs are obliged, at their own expense, to provide access to the data referred to in Article 180c of the TL to the court and the public prosecutor. Thus, retained data is to be made available at a telecommunications entrepreneur's "own expense". Making such data available by submitting itemized bills of performed telecommunications services to the court or public prosecutor is done free of charge. It is worth pointing out as well that Article 218(1) of the CCP does not contain any reference to Article 180a of the TL. The only reference to the costs borne by telecommunications entrepreneurs is made in the TL provisions.

Public telecommunications network operators and providers of publicly available telecommunications services are obliged to protect data referred to in Article 180(1)(1) of the TL against accidental or unlawful destruction, loss or alteration, or unauthorized or unlawful storage, processing, access or disclosure. The data should be protected in accordance with the provisions of Articles 159-175 of the TL referring to telecommunications confidentiality and end users data (Part VII of the TL) as well as with the provisions of Article 180e thereof. Pursuant to Article 180e of the TL, telecommunications entrepreneurs are obliged to adopt appropriate technical and organizational measures to ensure data protection referred to in Article 180a(1)(3) of the TL and provide access to such data only to authorized employees.

2. The obligation referred to in Article 180a(1) of the TL is deemed fulfilled if an operator of a public telecommunications network or a provider of publicly available telecommunications services, upon ceasing their business activity, submit the data to be stored, made available and protected by another operator of a public telecommunications network or a provider of publicly available telecommunications services (Article 180a(2) of the TL). The data may be used as important evidence in criminal proceedings, which is why it should continue to be retained by the operator succeeding the one whose business ceased to operate. Operators of a public telecommunications network and providers of publicly available telecommunications services ceasing to operate their business are not automatically released from the obligation to store and provide access to telecommunications data. This obligation becomes ineffective only after the data have been submitted to be stored, made available and protected by another operator of a public telecommunications network or a provider of publicly available telecommunications services. Another operator of a public telecommunications network or a provider of publicly available telecommunications services must of course agree to receive such data. A relevant contract should be signed. The only exception refers to a situation when an operator of a public telecommunications network or a provider of publicly available telecommunications services are declared bankrupt. Operators or providers who have been declared bankrupt are obliged to submit the data referred to in

Article 180a(1) of the TL to be stored, made available and protected by the President of UKE (Office of Electronic Communications).

The obligation referred to in Article 180a(1) of the TL should be fulfilled in a manner which does not lead to the disclosure of telecommunications messages (Article 180a(6) of the TL). An operator of a public telecommunications network or a provider of publicly available telecommunications services are obliged to adopt appropriate technical and organizational measures enabling them to fulfil this obligation, which means they have to protect such data against unauthorized access.

Unless otherwise provided for in separate provisions, access to data referred to in Article 180c of the TL, generated in a telecommunications network or processed by that operator or provider within the territory of the Republic of Poland, may be provided by means of a telecommunications network (Article 180a(7) of the TL). This provision allows the submission of data referred to therein by means of telecommunications networks. Other ways of submitting data may be provided for in separate provisions.

2. JOINT PERFORMANCE OF THE OBLIGATION TO STORE AND PROVIDE ACCESS TO TELECOMMUNICATIONS DATA

1. Pursuant to Article 180b(1) of the TL, the obligation to store and provide access to telecommunications data may be performed jointly by two or more operators of public telecommunications networks or providers of publicly available telecommunications services. As stated in Article 180b(2) of the TL, an operator of a public telecommunications network or a provider of publicly available telecommunications services may authorize another telecommunications entrepreneur to perform the obligation to store and provide access to telecommunications data on their behalf. However, this authorization does not release the authorizing operator or provider from performing this obligation.

The scope of cooperation referred to in Article 180b(1) of the TL may cover all activities connected with the performance of the above mentioned obligation, i.e. data retention, storage, access provision and protection. The cooperation may only be started upon prior consent of the entities authorized to obtain access to telecommunications data. The terms and conditions of such cooperation as well as its scope should be set out in a contract concluded between the entrepreneurs.

Pursuant to Article 180b(2) of the TL, entities authorized to perform the obligation to store and provide access to telecommunications data on behalf of another entity may receive remuneration. Entities authorized to perform the above mentioned obligations should be granted all authorizations to process personal and transmission data necessary to perform retention obligations. The entrepreneur wishing to authorize another entity to perform retention obligations on its behalf does not have to obtain a consent to do so from the entities authorized to obtain access to the retained data nor from the subscribers.

3. THE CATEGORIES AND SCOPE OF DATA TO WHICH ACCESS CAN BE GRANTED

1. The categories and scope of data to which access can be granted are regulated by the TL provisions and further elaborated upon in the Regulation of the Minister of Infrastructure of 28 December 2009 on the detailed specification of data and types of public telecommunications network operators or providers of publicly available telecommunications services obliged to retain and store such data. The Regulation was passed on the basis of

Article 180c(2) of the TL. 5 The Regulation of 28 December 2009 specifies the division of retention related responsibilities between entrepreneurs providing services to call originators and entrepreneurs handling call reception. In this regard, each telecommunication entity is required to retain data generated in its own network as well as data concerning the called party indicated by the user of its own services. Telecommunication entrepreneurs should jointly retain all data required by the TL and the Regulation. The provisions of both TL and the above mentioned Regulation implement the provisions set out in Article 5 of Directive 2002/58/EC.

Article 180c(1) of the TL, referred to in Article 218(1) of the CCP, specifies the scope of data covered by retention obligations. In practice, retention obligations pertain to four types of activities: data retention, storage, access provision and protection. Pursuant to Article 180c(1) of the TL, access must be provided to data that are necessary to:

1) trace the network termination point, telecommunications terminal equipment and the end-user: a) originating the call, b) to whom the call is made;

2) identify: a) the date and time of a call and its duration; b) type of a call; c) location of telecommunications terminal equipment used in a public mobile communications network.

Data belonging to the first category will vary depending on the type of network, i.e. fixed or mobile network. As regards services provided within a fixed public telecommunications network, data covered by retention obligations include: network termination point number of the subscriber originating a call and the one to whom the call is made, name and address of both subscribers. As regards services provided within a mobile public telecommunications network, retention obligations refer to the MSISDN number, name and address of both subscribers, if such data were made available, user's IMSI number, the first 14 digits of the IMEI number (a unique number to identify mobile devices) or the ESN number (a unique number of devices operating within the CDMA network); in the case of pre-paid services, the obligation also refers to the date and time of the initial activation of the service to a mobile public telecommunications networks according to local time and the location label from which the service was activated (BTS). In the case of Internet access services, Internet e-mail and Internet telephony the following categories of data are to be retained: user ID, the calling telephone number for dial-up access (using a dial-up modem), user ID and the number assigned to the end user originating a call to a public telecommunications network, IP address, name and address of the end user to whom an IP address was assigned during a call, and user ID or a number assigned to this user in Internet telephony, the identification of the digital subscriber line (DSL) or other end point of the originator of the communication, network port number or MAC address of terminal equipment. In the case of Internet e-mail and Internet telephony the called subscriber's data are limited to the assigned Internet telephony number or name and address of a registered end user of Internet e-mail and Internet telephony services as well as the ID of this user6.

The second category of data to be retained includes the date, time and duration of a communication. Thus, both in fixed and mobile networks the following data is identified: date and time of an unsuccessful call attempt or the start and end of a communication (according to local time), as well as the duration of the communication with the accuracy to 1 second. In the case of Internet access services, the date and time of the log-in and log-off of the Internet access service together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user. In the case of Internet e-mail and Internet telephony services, the date and

[5] Journal of Laws 2009 No 226, item 1828 .

[6] S. PIĄTEK, Prawo telekomunikacyjne. Komentarz [Telecommunications Law. Comments], Warsaw 2013, 1096-1097.

time of the log-in and log-off of the Internet e-mail service or Internet telephony service, according to local time. This category entails data related to the type of communication as well. For fixed and mobile network services the type of service used is identified (e.g. voice calls, short text messaging and multi-media services). In the case of Internet e-mail and Internet telephony services, the type of service used is identified together with the network port number. Finally, this category includes data necessary to identify the location of terminal equipment. As regards fixed networks, the address of terminal equipment is identified. As regards mobile networks, BTS antenna ID is identified at the start of or during a communication, as well as the geographic coordinates of the BTS within the coverage of which terminal equipment was located and the azimuth, the beam and the operating range of the BTS antenna. For devices located outside the territory of Poland, mobile country code (MCC) and mobile network code (MNC) are determined for both the source and destination of a communication. It must be pointed out that data necessary to identify the location of mobile equipment are to be retained only at the start of the communication. Data identifying the geographic location of cells by reference to their location labels are to be stored during the whole period for which retained data are stored. Retaining location related data throughout the ongoing call is not permissible7.

4. AUTHORIZED ENTITIES

1. Entities authorized to obtain access to telecommunications data are specified in Article 180d of the TL in connection with Article 179(3)(1)(a) and (3)(2) thereof. Authorized entities include: a) courts; b) public prosecutor's office; c) the Police; d) the Border Guard; e) the National Security Agency; f) the Military Counterintelligence Service; g) the Military Gendarmerie; h) the Central Anti-Corruption Bureau; i) the Customs Service; j) fiscal intelligence. Apart from courts and prosecutor's offices, in Poland there are 9 entities authorized to obtain access to telecommunications data.

5. PERIODS OF RETENTION AND ACCESS TO TELECOMMUNICATIONS DATA

1. The period for which telecommunications data should be retained and made available to authorized entities upon their request is specified in the Telecommunications Law. Pursuant to Article 180a of the TL, public telecommunications network operators and providers of publicly available telecommunications services are obliged to retain and store data referred to in Article 180c of the TL, generated in a telecommunications network or processed by that operator or provider within the territory of the Republic of Poland, for a period of 12 months from the date on which a communication was successfully or unsuccessfully established.

The twelve-month data retention period adopted in Poland is the result of the amendment to the Telecommunications Law of 16 November 2012. 8 Under this amendment, which came into effect on 21 January 2013, the provisions of Article 180a(1)(1) of the TL were changed and the retention period for data specified in Article 180c(1) of the TL for the authorized public bodies was shortened from 24 to 12 months from the date on which a communication was successfully or unsuccessfully established. What prompted the change was the fact that the two-year retention period used to be questioned by the bodies responsible for protecting citizens' rights and in the literature9.

---

7 S. PIĄTEK, Prawo telekomunikacyjne…, 1097-1098.

8 Journal of Laws 2012, item 1445.

9 See M. WACH, Zatrzymywanie danych telekomunikacyjnych przez dwa lata w celach bliżej nieokreślonych a prawo do prywatności [Retaining telecommunications data for two years without specifying the reason versus privacy rights], Radca Prawny Dodatek naukowy 2011, No 115-116, 22

Pursuant to Article 180a(1)(1) of the TL, retained telecommunications data must be destroyed immediately upon expiry of the twelve-month period, except those data that have been accessed and preserved under separate provisions. Destruction of data means their permanent deletion from the telecommunications entrepreneur's databases. Data must be deleted irreversibly, only then can this obligation be deemed fulfilled. It is not enough to transfer the data from the database covered by retention obligations to another database. Having fulfilled the obligation to destroy the retained data, the entrepreneur should be unable to recover the data by means of ordinary technological measures used for the conduct of telecommunications activities10.

2. Current regulations concerning the duration of data retention period raise numerous doubts as to their practical interpretation. On one hand, Article 180a(1)(1) provides for a twelve-month retention period, but on the other, there are some other Articles in the TL which provide for retention periods longer than 12 months (Article 164, 165 and 168). The scope of data to be retained under separate provisions is much narrower than the scope of data covered by retention obligations, and it mainly refers to performed telecommunications services and their settlement. For example, data retention period exceeding 12 months from their registration is provided for in Article 168(2) of the TL. Pursuant to this Article, a provider of publicly available telecommunications services is obliged to store the data concerning the performed telecommunications services for at least 12 months within the scope which allows it to determine the amount due for performing these services as well as to investigate a complaint, and in the event of a complaint being filed, for the time necessary to resolve a dispute. In view of the current legislation, it seems that the only acceptable interpretation is the one which permits data retention periods by telecommunications entrepreneurs exceeding 12 months, but only in specific cases clearly defined by the provisions of the Telecommunications Law and, what is crucial, only for purposes defined by the said provisions. As regards Article 168 of the TL, for example, for the purpose of complaint handling procedures. As stated in Article 180a(1)(1), data retained for the purpose of criminal proceedings, upon court's or prosecutor's request, can only be stored for up to 12 months.

6. INFORMATION SUBMITTED TO THE PRESIDENT OF UKE

1. Pursuant to Article 180g(1) of the TL, by 31 January telecommunications entrepreneurs are obliged to submit to the President of UKE previous year information concerning:

1) total number of cases in which telecommunications data were made available to authorized entities, the Customs Service, the court and the prosecutor;
2) time that elapsed between the date of data retention and the date of submitting a written or oral request for access to such data by an entity referred to in item 1;
3) total number of cases in which a written or oral request referred to in item 2 could not be satisfied.

The information is then submitted to the European Commission by the President of UKE (Article 180g(2) of the TL) on an annual basis. The manner in which this obligation should be fulfilled was specified in the Regulation of the Minister of Infrastructure of 30 December 2009 on the form template to be used by telecommunications entrepreneurs for the submission of data access related information to the President of the Office of Electronic Communications11. Under the said Regulation, the form template for the submission of data is laid out. Telecommunications entrepreneurs submit information concerning all cases in which telecommunications data were made available, regardless of the scope of requested

[10] S. PIĄTEK, Prawo telekomunikacyjne…, 1091.
[11] Journal of Laws 2010, No 3, item 15.

data. Data concerning the time that elapsed between the date of data retention and the date of submitting a written or oral request for access to such data are rounded off upwards to 1 month.

Telecommunications entrepreneurs may authorize another telecommunications entrepreneur to submit the above mentioned information to the President of UKE on their behalf. In order to do so both parties must conclude an authorisation contract. In this case, the entrepreneur submitting information to the President of UKE may submit its own and the authorizing party's information in a joint form. This authorization does not release the authorizing party from the responsibility for the performance of this obligation (Article 180g(4) of the TL).

7. LEGAL CONSEQUENCES OF THE JUDGMENT PASSED ON 8 APRIL 2014 BY THE COURT OF JUSTICE OF THE EUROPEAN UNION IN JOINED CASES C-293/12 AND C-594/12

1. In passing its judgment of 8 April 2014 in Joined Cases C-293/12 and C-594/12, the Court of Justice of the European Union annulled Directive 2006/24/EC of the European Parliament and 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/EC12.

The annulled by judgment of 8 April 2014 of the Court of Justice of the European Union Directive 2006/24/EC was implemented into the Polish Telecommunications Law, hence a question arises as to whether telecommunications entrepreneurs and authorized entities such as the prosecutor's offices and courts should continue to comply with the relevant provisions of the Telecommunications Law relating to data retention. These provisions have not yet been changed by the Polish lawmakers following the judgment of the Court of Justice. Neither have they been repealed by the Polish Constitutional Tribunal ruling.

In this situation, telecommunications entrepreneurs should adhere to national regulations until they have been repealed or amended by the lawmakers directly or following the judgment of the Polish Constitutional Tribunal. Changing the provisions will be necessary if a new data retention directive is passed. Meanwhile, adherence to the provisions of the Telecommunications Law does not generate any serious legal risks for telecommunications entrepreneurs with regard to the analyzed situation. Telecommunications entrepreneurs attempting to come up with their own interpretation of the Telecommunications Law provisions with reference to the judgment delivered by the Court of Justice of the European Union, by refusing to comply with the Telecommunications Law provisions concerning data retention in particular, could face penalties or be removed from the register of telecommunications entrepreneurs.

KEY WORDS

telecommunications data, data retention, access to data.

KĽÚČOVÉ SLOVÁ

Telekomunikačné údaje, uchovávanie údajov, prístup k údajom.

BIBLIOGRAPHY

[12] Official Journal of the European Union, L 105. , 2014

1. P. HOFMAŃSKI, E. SADZIK, K. ZGRYZEK, *Kodeks postępowania karnego. Komentarz [The Code of Criminal Procedure. Comments]*, Vol. I, Warsaw 2011
2. S. PIĄTEK, Prawo telekomunikacyjne. Komentarz [Telecommunications Law. Comments], Warsaw 2013.
3. M. WACH, Zatrzymywanie danych telekomunikacyjnych przez dwa lata w celach bliżej nieokreślonych a prawo do prywatności [Retaining telecommunications data for two years without specifying the reason versus privacy rights], Radca Prawny Dodatek naukowy 2011.

CONTACT DETAILS OF AUTHOR

Prof. dr hab. Maciej Rogalski

Łazarski University, Warsaw, Poland
rogalscy1@neostrada.pl
tel. mobile +48 602 206 138