Maciej Rogalski

THE PERIOD OF RETENTION OF TELECOMMUNICATIONS DATA WHICH MUST BE DISCLOSED AT THE REQUEST OF THE COURT OR THE PROSECUTOR IN CONNECTION WITH PENDING CRIMINAL PROCEEDINGS

1. Under the Polish law, the issues relating to the disclosure of correspondence and mail and telecommunications data for the purpose of pending court and prosecution proceedings are regulated by the criminal procedure and by the Act – Telecommunications Law.

The issues relating to the disclosure of correspondence and mail and data, referred to in the Telecommunications Law, are regulated by Article 218 of the Code of Criminal Procedure (CCP). However, issues such as the monitoring and recording of telephone calls are regulated in Chapter 26 CCP. The provisions of Article 218 CCP lay down the obligation to disclose correspondence, mail or billings and other data at the request of the court or prosecutor. This obligation is imposed on offices, institutions and other entities referred to in Article 218 § 1 CCP, irrespective of the legal and organisational form of their business and ownership, in particular, of whether it is private entity or a state-owned one.

Pursuant to Article 218 § 1 CCP, all offices, institutions and entities engaged in postal activity or telecommunications activity, as well as customs offices and transport institutions and enterprises, are obliged to disclose to the court or prosecutor, at the request included in the decision, any correspondence and mail and data, referred to in Article 180c and 180d of the Act of 16 July 2004 – Telecommunications Law[1] (TL), if those are relevant to the pending proceedings.

The scope of things and information to be disclosed is defined in section one of Article 218 CCP. Those include: correspondence, mail and data referred to in Article 180c and 180d TL, provided that they are relevant for the pending proceedings. In practice, the decision obliging to disclose the same will be based on the fact that the correspondence, mail or billings may be relevant

[1] Journal of Laws No 171, item 1800, as amended.

for those proceedings. However, it will not be evident whether or not they are relevant until their content has been identified. If the court or the prosecutor acknowledge that the retained correspondence or mail is of no relevance for the proceedings, they should be immediately returned to the entity from which they were taken (Article 218 § 3 CCP). However, the obligation to return will not apply to billings, as they represent only the graphic form (printout) of the data stored at the network operators[2].

The provisions of criminal procedure define entities obliged and authorised to disclose data and the mode of disclosure thereof. The types and the scope of data being disclosed are defined by the provisions of the Telecommunications Law which are further specified by the regulation of the Minister of Infrastructure of 28 December 2009 on the detailed list of data and type of operators of the public telecommunications network, or providers of publicly available telecommunications services obliged to retain the same. This regulation was issued on the basis of Article 180c(2) TL[3]. Pursuant to Article 180c(1) TL, the obligation referred to in Article 180a(1) TL extends to data necessary to:

1) determine the terminal point of a network, the terminal telecommunications equipment, the end user:
   a) initiating the communication,
   b) receiving the communication;
2) determine:
   a) the date and time of the communication and duration thereof,
   b) the type of communication,
   c) location of the telecommunications terminal equipment.

The provision of Article 180a TL, referred to in Article 180c(1) TL, applies to the obligation to retain and disclose data. Provisions of Article 180a(1)(2) TL impose on operators of the public telecommunications network and providers of commonly available telecommunications services the obligation to disclose, namely to search, create appropriate data sheets, and send via the telecommunications network to authorised entities, including the court and the prosecutor, the data referred to in Article 180c(1) TL. Pursuant to Article 180a (1) TL, subject to Article 180c(2)(2), the operator of the public telecommunications network and the provider of publicly available telecommunications services are obliged, at their own expense, to:

1) retain and store the data, referred to in Article 180c TL, generated in the telecommunications network or processed by them, in the territory of the Republic of Poland, during the period of 12 months, counting from the date of communication or unsuccessful communication, and to destroy these data

[2] P. Hofmański, E. Sadzik, K. Zgryzek, *Kodeks postępowania karnego. Komentarz* [Code of Criminal Procedure. Commentary], vol. I, Warszawa 2011, p. 1233.

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

after that period, with the exception of the data protected under separate provisions;
2) disclose the data, referred to in section 1, to authorised entities, and to the Customs Services, the court and the prosecutor, on terms and conditions and in the manner defined in separate provisions;
3) protect the data, referred to in section 1, against accidental or unlawful destruction, loss or modification, unauthorised or unlawful retention, processing, access or disclosure, in accordance with the provisions of Article 159–175a, Article 175c and Article 180e TL.

In addition, pursuant to Article 180d TL, telecommunications operators are obliged to ensure conditions for access and recording, and to disclose to authorised entities, and also to the Customs Services, the court and the prosecutor, at their own expense, the data processed by them, referred to in Article 159(1) (1) and 3–5 TL, in Article 161 TL and in Article 179(9) TL, connected with the telecommunications service provided, on terms and conditions and in compliance with procedures defined in separate provisions.

2. The provisions of Article 218 CCP do not specify the duration for which the data referred to herein should be retained. The data retention period is the period during which those data should be also disclosed at the request of authorised entities. During that period, authorised entities may request that the telecommunications operator disclose the data. The data retention obligation extends to four types of activities: retention, storage, disclosure and protection of data.

The retention period is calculated individually for data relating to each communication or unsuccessful communication. Thus, the operator calculates the retention period individually for each daily data filing system being subject to retention. The expiration of that period should be calculated on the basis of Article 57 § 3 of the Code of Administrative Procedure under which the time periods specified in months end when that day in the last month which corresponds to the initial day of the time period ends. The initial day of the time period is the day on which the communication or unsuccessful communication occurred[4].

The period during which the data should be retained is specified in the Act – Telecommunications Law. Pursuant to Article 180a TL, the public telecommunications network operator and the provider of publicly available telecommunications services are obliged to retain the data, referred to in Article 180c TL, generated in the telecommunications network or processed by them, in the territory of the Republic of Poland, during the period of 12 months, counting from the date of communication or unsuccessful communication.

---

[4] S. Piątek, *Prawo telekomunikacyjne. Komentarz* [Telecommunications Law. Commentary], Warszawa 2013, p. 1090–1091.

The 12-month period of data retention adopted in Poland is the effect of the amendment to the Telecommunications Law of 16 November 2012[5]. As of 21 January 2013, Article 180a(1)(1) TL was changed under that amendment, namely the data retention period referred to in Article 180c(1) TL for authorised entities was reduced from 24 to 12 months, counting from successful communication or unsuccessful communication. The two-year data retention period was challenged by authorities responsible for protection of civic rights and in the literature[6].

The provision of Article 180a(1)(1) TL constitutes the implementation of provisions of Article 6 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[7]. Directive 2006/24/EC was implemented into the national law by the amendment of the Telecommunications Law of 24 April 2009. This directive was the reaction to diverse terms and conditions of retention of transmission data in EU Member States in connection with the need to detect and prosecute criminal offences. Directive 2006/24/EC standardised the scope of data being subject to retention for the services of fixed network telephony and mobile telephony, Internet access, Internet e-mail and Internet telephony. Pursuant to Article 6 of the aforesaid directive: "Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication"[8].

According to the final clause of Article 180a(1)(1) TL, after the expiration of the period of 12 months those data need to be destroyed, except those data which were protected in accordance with separate provisions. Destroying the data means removing them permanently from the information resources of the telecommunications operator. Data must be removed in an irreversible manner, as only in then the obligation to destroy data may be regarded as fulfilled. It is not sufficient to transfer the data from the database used to fulfill the retention obligation to other databases. Once the obligation to destroy data has been fulfilled, the economic operator should be unable to recover the data using ordinary technical means used to conduct the telecommunications activity[9].

---

5 Journal of Laws of 2012, item 1445.

6 Cf. M. Wach, *Zatrzymywanie danych telekomunikacyjnych przez dwa lata w celach bliżej nieokreślonych a prawo do prywatności* [Retention of telecommunications data for two years for unclear purposes versus the right to privacy], Radca Prawny: Dodatek Naukowy 2011, No. 115–116, p. 22.

7 L 105/54 PL Official Journal of the European Union 13.4.2006.

8 Cf. D. Adamski, *Retencja danych telekomunikacyjnych – uwagi de lege ferenda wynikające z przepisów wspólnotowych* [Retention of telecommunications data – de lege ferenda notes following from community law], Monitor Prawniczy 2007 No. 4, dodatek Prawo Mediów Elektronicznych 2007, Monitor Prawniczy 2007; No. 6; S. Piątek, *Telecommunications Law*, p. 1086–1087.

9 S. Piątek, *Prawo telekomunikacyjne…*, p. 1091.

The obligation to destroy does not apply to data where a legal basis exists for continued retention by the operator. The legal basis may be formed by regulations which oblige the operator to retain data for a definite period longer than 12 months, and regulations which merely allow him to retain data longer than 12 months for a definite period. After the expiration of 12 months, the operator himself decides if they will continue to process the data, and for how long, i.e. for the whole period possibly required for data processing (allowing for the principle of adequacy) or only for a part of that period.

The legal basis for retention of data for a period longer than 12 months by the telecommunications operator is formed by the provisions of the Act – Telecommunications Law – Article 164, 165 and 168 TL. The scope of data which may be retained under separate provisions of the law is much smaller than the scope of data covered by retention and it extends mostly to performed telecommunications services and their settlement. An exemplary provision which allows to retain data, which are substantially the same as the data referred to in Article 180c(1) TL, for a period longer than 12 months from the date of recording thereof is Article 168(2) TL. The aforesaid provision obliges the provider of publicly available telecommunications services to retain for a minimum period of 12 months the data on performed telecommunications services, the scope of which allows to determine amounts payable for the performance of those services and to review complaints, and in case any complaint is filed, for a period necessary to resolve the dispute.

The minimum period of retention of data which was set out in Article 168(2) at 12 months corresponds to the overall period of data retention under Article 180a TL. The provision of Article 168(2) TL does not specify the moment from which the expiration of the period of 12 months should be counted. The earliest moment from which the expiration of that period may be counted is the moment of recording of the data on the service performed. In the case of periodical settlements, the correct solution, which is also included in the provision of Article 168(2) TL, is the retention of data for a period of 12 months from the end of the settlement period. It is not permitted to shorten this period, but section 2 allows to extend it. However, this period may be extended only within boundaries permitted by the Act[10].

In practice, the way in which the duration of the data retention period is calculated gives rise to numerous interpretation doubts. Under Article 180a(1)(2) TL, the provider of telecommunications services is obliged to disclose to authorised state bodies the data, referred to in Article 180a(1)(1) TL. Article 180c(1)(1) TL refers both to data which the provider of telecommunications services is obliged to possess within the scope referred to in Article 180c for the period of 12 months from the date of their recording, and data from the same

[10] *Ibidem*, p. 982–983.

scope in respect to which a legal basis exists for continued retention thereof after the prescribed 12-month period, for example in the aforesaid Article 168 TL. In consequence, authorised state bodies have, under Article 180a(1) TL the right of access to the data, referred to in Article 180c TL, during the whole period wherein the provider of services retains those data. The same conclusion follows from Article 180d TL which obligates the provider of telecommunications services to disclose all data processed and possessed by them, as referred to in Article 159(1)(1) and (3–5), Article 161 and Article 179(9) TL. Those data are the same as the data referred to in Article 180c TL. Pursuant to Article 180a(1) (2) and (3) TL, the obligation of retention extends to all data referred to in Article 180c(1) TL during the period of 12 months of the date of recording the same, and also to data which have not been destroyed after 12 months in the case when there is a prerequisite for further retention thereof by the operator.

It needs to be emphasised that the terms and conditions, and the mode of disclosure should be standardised for data, referred to in Article 180c(1) TL, and retained under Article 180a TL, both during the period of the first 12 months of the date of their recording, and after the expiration of that period in the case of continued retention of data of a specific type. It follows clearly from Article 180a(1)(3) and 3 TL that the terms and conditions, and the mode of disclosure of data, defined in the regulations governing data retention, should also apply to data retained after the expiration of 12 months of their recording date.

It does not follow either from the justification of the amendment to the Act Telecommunications Law, implementing, in particular, the provisions of Article 180a and 180c TL, or from Directive 2006/24/EC that authorised bodies may be denied access, in the mode provided for by the regulation of the Minister of Justice of 28 April 2003 on the method of technical preparation of systems and networks used to transmit information – for gathering billings and other communications of information and methods of protection of IT data[11], to data referred to in Article 180c(1) TL, retained by the operator longer than 12 months.

In addition, there are no rational arguments in favour of the reasoning that, on the basis of the request to disclose data referring to Article 180c TL, the authorised entity is not allowed to request access to data older than 12 months, as it may obtain the said access under Article 180d TL.

Thus, the aforesaid provisions give rise to doubts about the relationship between Article 180a(1) TL, and other provisions justifying the ability of providers of publicly available telecommunications services to reuse data which are analogous to those referred to in Article 180c(1) TL for a period longer than 12 months from the data recording date. Under the current law, there is no provision to clearly determine the period after the expiration of which authorised state bodies will not be permitted to request access to any data retained

[11] Journal of Laws of 2003, No. 100, item 1023.

by providers of telecommunications services. Similarly, no consistent position has been taken in practice on the interpretation of the aforesaid provisions. It is worthwhile to quote the position of the Supreme Audit Office[12] which audited on a comprehensive basis the practices and compliance with the law of the gathering and disclosing of billings. It follows from those documents that according to the Supreme Audit Office actions such as "requesting the disclosure of telecommunications data for a period extending beyond the lawful retention period" are improper. Thus, there may arise doubts about the right conduct of the provider of telecommunications services, possessing the data relating to a given subscriber under Article 168 TL for a period longer than 12 months from the recording thereof, in a situation where the authorised state body requests in the appropriate mode that the data relating to the indicated subscriber, referred to in Article 180c and 180d TL, be disclosed.

It seems that under the current law the only acceptable interpretation is the one permitting a longer retention of data than 12 months by the telecommunications operator but only in the cases expressly provided for by the provisions of the Telecommunications Law and, which is crucial, only for the purpose specified therein. For example, as in Article 168 TL, for the purposes of complaint procedures. However, for the purposes of criminal proceedings, at the request of the court or the prosecutor, telecommunications data may be retained, in accordance with Article 180a(1)(1) TL, for a period no longer than one year. Thus, in the case of doubts concerning the right conduct of the provider of telecommunications services possessing, under Article 168 TL, any subscriber's data which are the same as the data referred to in Article 180c TL, after 12 months of the date of recording thereof, when an authorised state body requests that the provider of services disclose the data relating to that subscriber, possessed by the provider of services, referred to in Article 180c and 180d TL, i.e. if, in this situation, the provider of services is obliged to refuse to disclose the data to the state body, concluding that under Article 180a(1)(1) TL authorised state bodies are empowered to request data not older than 12 months of the date of recording thereof, or if the provider of telecommunications services should disclose to the authorised body those data, under Article 168 TL, as are retained longer than 12 months from the date of recording thereof, the answer will be – the provider should refuse to provide the data in question.

---

[12] Cf. *Komunikat Najwyższej Izby Kontroli pt. NIK o billingach oraz dokument pt. Informacja o wynikach kontroli. Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180 c i d ustawy Prawo telekomunikacyjne* [The communication of the Supreme Audit Office entitled SAO commenting on billings and the document entitled The audit report. Obtaining and processing data from billings, location information and other data by authorised entities, as referred to in Article 180 c and d of the Act – Telecommunications Law], http://www.nik.gov.pl/aktualnosci/nik-o-billingach.html].

3. The right to request disclosure of data and information, referred to in Article 218 § 1 CCP, is available to the court or the prosecutor. Those entities may request disclosure of correspondence, mail or data (billings), issuing a relevant decision. The decision should specify the thing to be disclosed. In the case of billings, the decision should name the user of the telephone whose billing is requested (or the electronic address whose list of correspondence is requested), and the period for which the billing is requested[13]. It is not required to issue a separate decision for each mail.

The right to open correspondence and mail and to order to open the same are reserved for the court or the prosecutor (Article 218 § 1 sentence 2 CCP). Pursuant to Article 143 § 1(7) CCP, the opening of any correspondence and mail is ranked among activities which must be recorded in writing. The provision of Article 218 § 1 sentence 2 CCP applies not only to correspondence or mail but also to billings, thus a reasonable assumption is made that the printed billing should be delivered in a sealed envelope[14].

In practice there are situations where the court or the prosecutor sends the decision relating to the disclosure of data under Article 218 CCP, protected by telecommunications confidentiality, by fax. In such cases, the bodies authorised invoke Article 132 § 3 CCP, stating that the service is effective and the decision should be implemented. In view of the contents of Articles 128 and 131 CCP, a question arises whether or not the decision should be implemented only when an authenticated decision issued under Article 218 CCP has been sent by mail to the obliged entity.

One should voice serious doubts as to whether a copy of the decision, referred to in Article 218 § 1 CCP, is effective if sent by fax. Pursuant to Article 128 § 1 CCP, judgments and orders are served in the form of authenticated copies if the Act demands that those be served. Decisions, without any doubt, qualify as judgments, referred to in Article 128 § 1 CCP. In consequence, a copy of the decision must be authenticated. Authentication involves the official confirmation of conformity with the original. The purpose is to confirm the authenticity of the document, thus allowing to make sure that a specific decision comes from the entity which issued the same. In order to confirm the authenticity of a document one needs to have the original.

Pursuant to Article 128 § 2 CCP, "all letters designed for participants of the proceedings shall be served in such a manner that the content thereof is not disclosed to any unauthorised persons". When the decision of the court containing data protected by the telecommunications secrecy is sent by fax, the data may come to the attention of unauthorised persons. Sending the decision by mail requires that the content be protected by a sealed envelope, and naming the

[13] P. Hofmański, E. Sadzik, K. Zgryzek, *Kodeks postępowania karnego…*, p. 1231.
[14] *Ibidem*, p. 1233–1234.

sender results in the correspondence to be addressed only to authorised persons and required to implement the content thereof[15]. Attention should be drawn to the judgment of the Supreme Court of 23 November 2007, court file number IV CSK 228/07, which emphasised that "in the case of the declaration of will made by fax, it is impossible to establish whether or not the signature has been copied from another document to the document sent to the recipient. Neither is it possible to ascertain that the document signed was the definitive declaration, and not a a draft thereof, or a text containing a statement that the party concerned did not intend to make at all. For that reason, an assumption is made in the doctrine that sending the content of a declaration of will by fax serves only the purpose of prima facie evidence and must be confirmed in writing"[16]. An analogous position was taken by the Supreme Court in the resolution of 20 December 2006, court file number I KZP 29/06, where the court explained that, in view of the inability to meet the requirement of official confirmation of the signature authenticity, sending letters by fax does not ensure sufficient security with respect to the elimination of undesired interference with the content thereof[17]. However, in the order of 26 January 2012, court file number III KZ 93/11, the Supreme Court stated that the use of electronic media to serve letters (including letters sent by fax) did not lie within the discretion of the body, or participants of the proceedings, but applied only in cases strictly defined in the Act[18].

However, there is no consensus on the issue in question in the doctrine. According to one position, it is not permitted to serve judgments and orders in the mode referred to in Article 132 § 3 CCP. Those are served, according to Article 128 § 1 CCP, in the form of authenticated copies, whereas the transmission via electronic mail, like the serving of a photocopy of the letter, may not be equated with the serving of an authenticated copy thereof, even if it allows for viewing the letter[19]. The provision of Article 132 § 3 CCP refers to serving the statements of case but there is a difference between serving in this manner summons or notices, and serving copies of judgments and orders.

Other representatives of the doctrine present a completely opposite position. In their opinion, the possibility of serving letter via telefax or electronic mail may not be limited to sending summons and notices. There are no obstacles preventing the use of this "technical" method to send also judgments and orders, provided that a format is used which makes possible the transmitting of documents

---

[15] Cf. *Zarządzenie Nr 81/03/DO Ministra Sprawiedliwości z dnia 12 grudnia 2003 r. w sprawie organizacji i zakresu działania sekretariatów sądowych oraz innych działów administracji sądowej* [Regulation No 81/03/DO of the Minister of Justice of 12 December 2003 on the organisation and scope of activity of court secretariats and other departments of court administration], § 18, Official Gazette of the Minister of Justice, No. 5, item 22 as amended.

[16] OSNC 2008, No. 3, item 88.

[17] OSNKW 2007, No. 1, item 1.

[18] OSNKW 2012, No. 3, item 34.

[19] P. Hofmański, E. Sadzik, K. Zgryzek, *Kodeks postępowania karnego…*, p. 791–792.

in a graphic form bearing the stamp and signature of the authenticating person. In this way the form of serving of the judgment or order, provided for in Article 128 § 1 CCP would be preserved. This solution would also be consistent with the spirit and provisions of the Act of 17 February 2005 on Computerisation of the Activities of Entities Performing Public Tasks (Journal of Laws No 64, item 565 as amended) which – establishing the State Computerisation Plan – imposes on public entities the obligation to facilitate the exchange of information, also in electronic form, through the exchange of electronic documents in matters within the scope of their activities (Article 16(1))[20]. In an analogous position it has been stressed that criminal proceedings should follow the development of technology, especially electronic communication. Seizing those opportunities is in the interest of participants of the proceedings themselves, as in most cases it substantially streamlines and expedites the proceedings. Therefore, it is assumed that the mode of service defined in Article 132 § 3 CCP may also be used with respect to all letters, including judgments or orders. In such cases, in view of the principle of that mode of service, the addressee would receive a copy, however, there is no doubt that this should be an authenticated copy of the judgment or order, e.g. a scan of the document in PDF format which guarantees the integrity of data contained therein[21]. However, it should be noted that this mode of service defined in Article 132 § 3 CCP may be used only with regard to persons who provid their telefax number or electronic mail address, and thus conclusively accept this form of service[22].

However, one needs to agree with the position that it is not permitted to serve judgments in the manner defined in Article 132 § 3 CCP. Those are served, according to Article 128 § 1 CCP, in the form of authenticated copies, whereas the transmission via electronic mail, even if, similarly to the serving of a photocopy of the letter, it allows for viewing the letter may not be identified with the serving of an authenticated copy thereof.

---

[20] J. Skorupka (ed.), *Kodeks postępowania karnego. Komentarz*, [Code of Criminal Procedure. Commentary], Legalis [online], volume 10, on Article 132.

[21] Cf. L. K. Paprzycki [in:] J. Grajewski (ed.), J. Grajewski, L.K. Paprzycki, S. Steinborn, *Kodeks postępowania karnego. Komentarz* [Code of Criminal Procedure. Commentary], Zakamycze 2006, p. 399.

[22] Cf. S. Steinborn [in:] J. Grajewski (ed.), L.K. Paprzycki, S. Steinborn, *Komentarz aktualizowany do art. 1–424 ustawy z dnia 6 czerwca 1997 roku Kodeks postępowania karnego*, [Updated commentary on Article 1–424 of the Act of 6 June 1997 – Code of Criminal Procedure], Lex [online] 2014, commentary on Article 132.

THE PERIOD OF RETENTION OF TELECOMMUNICATIONS DATA WHICH MUST BE DISCLOSED AT THE REQUEST OF THE COURT OR THE PROSECUTOR IN CONNECTION WITH PENDING CRIMINAL PROCEEDINGS

Summary

Following the implementation of the EU Directive by Poland, the period of retention of telecommunications data has been reduced from 2 years to one year. However, regulations permitting longer retention of data remain in force. This paper presents some doubts concerning the interpretation of those regulations, and problems of their application in practice, as well as a proposition to resolve existing discrepancies. It also addresses a major practical problem, namely the possibility of serving the decision obliging to disclose telecommunications data by fax or electronic mail, instead of sending the original by post.

OKRES PRZECHOWYWANIA DANYCH TELEKOMUNIKACYJNYCH PODLEGAJĄCYCH WYDANIU NA ŻĄDANIE SĄDU LUB PROKURATORA

Streszczenie

Przedmiotem artykułu jest problematyka udostępniania danych telekomunikacyjnych na żądania sądu i prokuratora w związku z toczącymi się postępowaniami karnymi. W następstwie zaimplementowania przez Polskę Dyrektywy UE skróceniu uległ okres przechowywania danych telekomunikacyjnych z 2 lat do jednego roku. Obowiązują jednak nadal przepisy, które pozwalają na dłuższy okres przechowywania danych. Artykuł przedstawia wątpliwości interpretacyjne oraz problemy w stosowaniu tych przepisów w praktyce, z propozycją rozwiązania powstałych rozbieżności. Zajmuje się także, posiadającym bardzo duże znaczenie praktyczne, problemem dotyczącym możliwości dostarczenia postanowienia zobowiązującego do udostępnienia danych telekomunikacyjnych faksem lub pocztą elektroniczną, zamiast przesłania oryginału pocztą.

LA PÉRIODE DE STOCKER DES DONNÉES DE TÉLÉCOMMUNICATION QUI SONT PASSIBLES D'UNE EXTRADITION À LA DEMANDE DE LA COUR OU DU PROCUREUR

Résumé

L'objet de l'article forme la problématique de l'accessibilité des données de télécommunication à la demande de la cour et du procureur nécessaires pour des procédures pénales mise en vigueur. A la suite de l'implémentation par la Pologne de la Directive de l'Union européenne la période de stocker des données de télécommunication a été réduit de 2 ans à 1 an. Pourtant il y a des règlements valides qui permettent de stocker ces données pour une période plus longue. L'article présente ces quelques doutes interprétatifs et les problèmes d'appliquer ces règlements en pratique ainsi que la proposition de résoudre des divergences actuelles. Il s'occupe aussi du problème qui a une très grande valeur pratique, celui qui concerne la possibilité de pourvoir la décision obligeant à l'accessibilité des données de télécommunication par fax ou par le courrier électronique au lieu d'envoyer l'original par la poste conventionnelle.

СРОК ХРАНЕНИЯ ДАННЫХ ТЕЛЕКОММУНИКАЦИИ, ПОДЛЕЖАЩИХ ВЫДАЧЕ ПО ТРЕБОВАНИЮ СУДА ИЛИ ПРОКУРОРА

Резюме

Предметом статьи является проблематика предоставления доступа к данным телекоммуникации по требованию суда и прокурора в связи с текущими уголовными делами. После принятия Польшей Директивы ЕС сократился срок хранения данных телекоммуникации с двух лет до одного года. Однако ещё действуют положения, позволяющие на более длительный срок хранения данных. Статья представляет собой интерпретационные сомнения, а также проблемы, касающиеся применения этих положений на практике, с предложением решения возникших несоответствий. Исследование посвящено также решению имеющей большое практическое значение проблемы, касающейся возможности передачи постановления, обязывающего предоставить доступ к данным телекоммуникации, посредством факса либо электронной почты, вместо высылки оригинала по почте.