Ius Novum
2/2015

Maciej Rogalski

ARE THE REGULATIONS WITH RESPECT TO THE RETENTION AND PROVISION OF COMMUNICATIONS DATA APPROPRIATE IN POLAND? PROPOSALS FOR CHANGES

Introduction

In 2014 in Poland, the number of requests for communications data addressed to the telecommunications companies increased again. According to the Office of Electronic Communications (UKE), there were 2,177,916 such requests in 2014, which was an increase by 7% over the last year[1]. Thus, statistics show a constant growth of requests. Moreover, the number of requests is much bigger than in other European countries.

The issue of acquiring communications data is not only connected with the actions of the law enforcement agencies and entities obliged to provide them, but also intrudes into a very sensitive area of human rights and freedoms. A series of problems come into existence. The basic one is the necessity of fighting against crime, which is often connected with the state organs' interference in the citizens' rights. The assurance that there will not be too much interference is of key importance. Thus, the legal regulations constituting the grounds for the actions of the authorised and obliged entities in the area play a key role. It especially concerns legal regulations with respect to the provision of telecommunications messages and data. A question is raised whether the regulations are appropriate or allow for the acquisition of data inadequately to the objectives they serve with respect to both the amount and the range of telecommunications messages and data, especially the so-called billings. Another issue is the practical application of the regulations in force, i.e. whether they are proper, especially in connection with the co-called authorised entities' actions as referred to in Article 179 (3) of Act of 16 July 2004: Telecommunications Law[2], hereinafter TL, or whether they should also be amended. There is a related problem of supervising the

[1] Gazeta Wyborcza of 19 March 2015, No. 65, p. 4.
[2] Journal of Laws of 2004, No. 171, item 1800 with amendments that followed.

entities authorised to acquire communications data. Therefore, it seems that the present legal mechanisms and organisational solutions do not ensure sufficient supervision of the provision of telecommunications messages and data.

Legal regulations with respect to the collection and provision of communications data in Poland

1. In the Polish law, the issues connected with the provision of communications data for the needs of pending court and prosecution proceedings are regulated by the criminal procedure (Articles 218–218b of the Criminal Procedure Code[3], hereinafter CPC). The provision of Article 218 § 1 of the CPC obliges telecommunications companies to provide a court or a public prosecution office, on demand contained in the decision, with data specified in Articles 180c and 180d of the TL if they are important for the pending legal proceeding. The obligation is imposed on entities involved in telecommunications business regardless of their legal and organisational form and who their owner is, i.e. whether the entity is a private of a public company. The data to be provided are specified in Articles 180c and 180d of the TL, under the condition that they are essential for the pending legal proceeding. In practice, the grounds for the decision obliging to their provision shall be the circumstance that the communications data may be relevant for the procedure[4]. Moreover, the grounds for the request for communications data are the acts regulating operations of the so-called authorised entities. They are specified in the provision of Article 180d of the TL in connection with Article 179 (3) point 1 letter a) and (3) point 2 of the TL. They are, apart from the already mentioned courts and prosecution offices, the Police, the Border Guard, the Internal Security Agency, the Military Counterintelligence Service, the Military Police, the Central Anti-Corruption Bureau, the Customs Service and the Fiscal Intelligence Office. Apart from courts and prosecution offices, there are eight entities altogether that are authorised to obtain communications data in Poland.

The discussed issues concern only the provision of communications data and do not cover the surveillance and recording telephone conversations, i.e. the so-called telephone tapping. The issue is regulated in Chapter 26 of the CPC entitled *Surveillance and recording conversations* (Articles 237–242 of the CPC). The provisions of the CPC determine cases when surveillance and recording conversations may take place, entities authorised to apply those measures and the mode of applying them. On the other hand, the provisions of the Telecommunications Law determine the duties of the telecommunications

[3] Act of 6 June 1997: Criminal Procedure Code, Journal of Laws of 1997, No. 89, item 555 with amendments that followed.

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

companies in the area. In theory, there is a so-called proceeding-related tapping (the provisions of Chapter 26 of the CPC) and there is tapping that is not related to the proceeding (called 'operational control' tapping)[5], which is regulated in special acts, e.g. Act on the Police. The proceeding-related tapping includes both "surveillance and recording the contents of telephone conversations" (Article 237 § 1 of the CPC) as well as "the contents of other conversations or information transmissions, including correspondence transmitted by electronic mail" (Article 241 of the CPC). Acquiring the billings of telephone conversations or other information transmissions is laid down in Article 218 § 1 of the CPC. On the other hand, acquiring data from the IT systems and data storage devices, including electronic mail is laid down in Article 236a of the CPC.[6]

2. The practice of applying the provisions regulating the acquisition of communications data showed a range of problems connected with this acquisition. It is necessary to discuss the most important of them.

The first problem concerns the types of cases in which communications data may be acquired. In other words, are courts allowed to demand billings in cases different than criminal ones? It mainly concerns requests for data in family law cases, especially a divorce, without the telephone subscriber's consent, which is necessary in such cases. In practice courts have often requested the provision of short messages' contents in civil law cases. It is, however, not allowed to provide the contents of short messages without the prior ruling on surveillance and recording of telephone conversations as referred to in Article 237 of the CPC in order to pursue only some most serious types of crime. Due to the lack of legal grounds, communication data cannot be requested in civil law cases. In practice civil courts referred to Article 248 of the Code of Civil Proceeding (CCP), which stipulates the obligation to provide documents requested by court if it is a proof essential for the adjudication. The provisions of Article 248 of the CCP, unlike Articles 218, 218a or 237 of the CPC, do not repeal the confidentiality of communications. They are mainly procedural in character. This is an obstacle to the application of Article 248 of the CCP as grounds for civil courts' requests for the provision of data that are protected by the confidentiality of communications[7]. Court decisions also emphasise

---

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

[6] T. Grzegorczyk, *Kodeks postępowania karnego. Komentarz* [Criminal Procedure Code. Commentary], Zakamycze 2005, p. 590.

[7] Compare P. Barta, P. Litwiński, *Dane objęte tajemnicą zawodową* [Official secret data], [in:] *Prawo reklamy i promocji* [Law on advertising and promotion], (ed.) E. Traple, Warszawa 2007, p. 607; also see

that telephone billings are subject to the confidentiality of communications as referred to in Article 159 (1) point 1 and 3 of the TL. With the exception of cases referred to in the Act or other provisions, revealing and processing the contents or data that are confidential violates the obligation to keep them secret and is, as a rule, prohibited (Article 159 (2) and (3) of the TL)[8].

The provision of communications data in cases concerning offences raises many more doubts. Communications data are requested by law enforcement agencies pursuing perpetrators of offences in order to detect and punish them. Exemption from official and professional confidentiality in case of offences is regulated exclusively in Article 41 § 3 of Act of 24 August 2001: Code of Procedure in Petty Offences[9] (CPPO), which is very general in character as it refers to all types of professional confidentiality and does not meet the criteria for exemption from the obligation to keep communication secret, i.e. the requirement of definiteness and thoroughness, in accordance with Article 49 of the Constitution. First of all, however, it cannot constitute grounds for requesting telephone conversations billings by exemption from official and professional confidentiality because in cases concerning petty offences, Article 218 § 1 of the CPC is not applied, neither directly nor by analogy. The provision stipulating exemption form communication confidentiality in criminal cases cannot be applied to petty offences because in accordance with Article 1 § 2 of the CPPO in the petty offences procedure the provisions of the CPC are applied only when the CPPO stipulates that. Thus, the provision of billing data cannot be requested based on Article 41 § 3 of the CPPO because it would infringe the law allowing for the exemption of the witness from official confidentiality obligation[10].

Many problems result from the interpretation of the provisions of Act of 29 August 1997 on the protection of personal data (hereinafter APPD) and acts defining the organisation and authorisation of state agencies and organs in the field of the provision of mobile telephone subscribers' data in connection with legal proceedings against them resulting from offences they committed[11]. However, the lack of grounds for the application of Article 23 of the APPD should not raise any doubts because it stipulates broader access to personal data than Article 159 (1) point 2 of the TL. According to Article 5 of the APPD, if the provisions of other statutes referring to data processing stipulate stricter protection than Act on the protection of personal data does, the provisions of these statutes should be applied. Thus, the provision of Article 159 (1) point 1

---

ibid., *Ustawa o ochronie danych osobowych. Komentarz* [Act on the protection of personal data. Commentary], Warszawa 2009, p. 85.

[8] See the sentence of the Court of Appeal in Białymstok of 6 April 2011, I ACz 279/11, Orzecznictwo Sądów Apelacji Białostockiej 2011, No. 1, item 36.

[9] Journal of Laws of 2001, No. 106, item 1148 with the amendments that followed.

[10] Compare the sentences of the Voivodeship Administrative Court in Warsaw of 30 August 2006, II SA/Wa 809/05, LEX No. 283565; of 10 October 2006, II SA/Wa 643/05, unpublished.

[11] Journal of Laws of 2002, No. 101, item 926, with amendments that followed.

of the TL excludes the application of the provisions of Act on the protection of personal data in this area.

The current wording of Article 20c of Act of 6 April 1990 on the Police[12] also raises doubts. The provision of Article 20c of Act on the Police that stipulated that the data referred to in this provision may be provided for the Police and processed only in order to prevent or detect crime was repealed. Thus, the authorisation of the Police referred to in this provision concerned crime exclusively and could not be applied in petty offences cases. On the other hand, there is no provision in Act on the Police clearly stipulating that communications data may be acquired for the needs of the proceeding in petty offence cases[13]. The problem might be unambiguously solved by the introduction of a clear provision in Act on the Police, e.g. in place of the repealed Article 20c (1), stipulating that the provision of communications data for the Police is possible only for the need of pending criminal proceedings and not petty offences proceedings.

3. Another problem is connected with the length of time communications data shall be stored; at present it is 12 months. In practice, the authorised entities quite often request the provision of communications data for a period of time that is longer than the statutory one. The problem concerns especially the relation between the provision stipulating the maximum legal period of 12 months for storing retention data (Article 180a (1) point 1 of the TL) and the provisions stipulating longer periods of storing data, e.g. the provision of Article 168 (2) of the TL, allowing for a period longer than 12 months necessary to deal with a complaint. It seems that in the legal system in force, the only interpretation possible to be accepted is the interpretation allowing for the storage of communications data by the telecommunications companies for a period longer than 12 months only in cases clearly determined by the provisions of the TL, and – what is essential – only for purposes determined in these provisions, e.g. Article 168 of the TL. For the needs of criminal proceedings, on the request of a court or a prosecutor, in accordance with Article 180a (1) point 1 of the TL, communications data may be stored for no longer than 12 months.

Thus, considering doubts what the telecommunications services providers should do in case they possess the subscriber's data in accordance with Article 168 of the TL, which are also referred to in Article 180c of the TL, after a period of 12 months from the moment of their registration, if the authorised state organ requests the provision of the possessed data referred to in Article 180c and 180d of the TL, i.e. whether the service provider should in this situation refuse to provide the organ with the data on the grounds that Article 180a (1) point 1 of

[12] Uniform text: Journal of Laws of 2007, No. 43, item 277 with amendments that followed.

[13] B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Policji. Komentarz* [Act on Police. Commentary], Warszawa 2015, p. 157.

the TL entitles state organs to request data that are not older than 12 months or whether the communications company should provide the authorised organ with the data possessed in accordance with Article 168 of the TL and stored longer than for 12 months, it must be stated that the communications company should refuse to provide the data. It must also be added that the standpoint is not common. There are also opinions that if a company possesses communications data, in spite of the termination of the 12-month period, the data should be provided on the request made by the authorised entities. The interpretational doubts presented above indicate that there is a need to make amendments to Act on the Telecommunications Law that would unambiguously eliminate the discussed doubts. Although the issues were indicated to legal institutions, there was no initiative to amend the regulations in order to eliminate doubts and, as a result, reduce the amount of enquiries addressed to telecommunications companies.

De lege ferenda, a new provision should be added to the Telecommunications Law unambiguously indicating that in case the company possesses communications data for a period longer than 12 months, the authorised organs cannot be provided with them. The principle should be binding regardless of the reason why the data are stored for a period longer than one year. The storage may be longer on the grounds of other provisions of the TL, e.g. for the needs of dealing with a complaint, as well as simply because of the neglected duty to delete the data after a year's period. The truth is that in practice the process of deleting communication records and data is not always appropriately performed.

4. The provisions of the TL in the field of retention and provision of communications data constitute the implementation of the decisions of Article 6 of 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/EC[14] (hereinafter Directive 2006/24/EC). Directive 2006/24/EC was implemented in the national law by the amendments to TL of 24 April 2009. The Directive was a response to the varied conditions of retaining transmission data in the EU member states in connection with detecting and pursuing crime. Directive 2006/24/EC standardized the range of data that are subject to retention for the landline and cellular telephone services, access to the Internet, email services and Internet calling. In its decision of 8 April 2014, the European Court of Justice (the Grand Chamber) in combined cases C293/12 and C594/12 declared Directive 2006/24/EC[15] to be null and void. In the justification to this judgement, the Court indicated, inter alia, that Direc-

[14] L 105/54 PL, Official Journal of the European Union 13.4.2006.
[15] Official Journal of the EU L 105, p. 54.

tive 2006/24/EC refers in general to all the entities, means of electronic communications and traffic data on, but without any differentiation, limitation or exception made with regard to the aim to fight against serious crime (thesis 57 of the judgement). The Court noticed that on the one hand Directive 2006/24/EC covers, in a generalized manner, all persons using electronic communications services whose data are retained. It even applies to persons for whom there are no grounds, actual or legal, for initiating a criminal proceeding. Moreover, the Directive does not provide for any exceptions to any persons. This means that it is also applied to persons whose contacts and information obtained during those contacts are subject to protection of professional secrecy in accordance with national laws (thesis 58 of the judgment). The court also indicated that Directive 2006/24/EC not only fails to lay limits to its application scope but also does not provide for any objective criterion that would ensure access of the competent national authorities to the data and their use only for the purpose of prevention, detection and criminal prosecution. On the contrary, Directive 2006/24/EC simply refers to the concept of 'serious crime' in Article 1 (1), defined in national law of every member state (thesis 60 of the judgment). Finally, the Court indicated that Directive 2006/24/EC does not lay down any objective criterion by which the number of persons entitled to access and subsequently use the data retained is limited to cases when it is strictly necessary for obtaining the objective. The Court noticed that access by the competent national authorities to the data is not made dependent on the prior review of a court or an independent administrative organ. A court or an independent administrative organ should supervise access to and use of data so that it is limited to cases when it is strictly necessary for obtaining the objective pursued. A court or a competent administrative organ should adjudicate or decide, exclusively on a justified request made in connection with the pending proceeding for the purpose of prevention, detection and criminal prosecution. The Directive does not lay down any obligations on member states to establish such mechanisms (thesis 62 of the judgement).

As the Court declared Directive 2006/24/CE to be null and void, a problem appeared as to how the Court's judgement should be interpreted and understood. Despite the fact that Directive 2006/24/EC was repealed, it must be assumed that the retention of data is admissible and constitutes a limitation of human rights and freedoms that is justified by public interest. The model of data retention laid down in the Directive is defective and requires amending. In the present situation, telecommunications companies should apply national legislation until it is repealed or amended by the legislator directly or following the judgement of the Constitutional Tribunal. However, the amendment to the regulation will be necessary when a new data retention directive is passed. The application and compliance with the TL does not generate any serious legal risks for telecommunications companies in the analysed situation. Their attempts to

interpret the provisions of the TL in the light of the Court's judgement on their own, especially the refusal to apply the provisions of the TL on the data retention, may pose a risk for telecommunications companies of being fined and even excluded from the register of telecommunications companies.

Proposals for model solutions

1. The purposes of communications data retention should be precisely defined in particular statutes. Too general specification of the purpose of acquiring data allows for requesting them from the obliged entities in numerous cases. The catalogue of situations in which authorised agencies may request the provision of communications data should be precisely determined. It is of key importance for the assessment whether the provisions in force do not infringe the principle of proportionality, and thus, are admissible in the light of current regulations protecting human rights and freedoms.

2. The principle of subsidiarity should be binding. There should be legal guarantees safeguarding the application of the principle. In accordance with the provisions in force, authorised entities may request the provision of communications data in every case, and not only when "other means used in order to meet the statutory objectives proved to be ineffective". Thus, the provisions that lay down grounds for requesting the provision of communications data as well as the adequate provisions of the TL determining telecommunications companies' duties should be amended. Therefore, the provisions of the TL (Articles 179–180g, Articles 192 (1) point 5b and 5c of the TL) should be amended with respect to their effectiveness in the creation of conditions for the implementation of the principle of subsidiarity in the field of communications data acquisition by authorised entities.

3. Solutions creating additional guarantees in case of persons doing the job of public trust should be introduced. The provisions that are currently in force do not lay down the category of persons, from whom communications data cannot be acquired because their jobs' professional secrecy must be respected. The legislator did not exclude any category of persons from the group of entities whose data may be acquired although the data may be covered by e.g. the solicitor's professional secrecy, which may be only exempted if it is indispensable for the good of justice administration and the particular circumstance cannot be established on the grounds of another proof. There should be legal solutions ensuring additional guarantees for those persons, especially a legal mechanism that would make the acquisition of data dependent on the court's consent.

4. In practice, the acquisition of communications messages and data with the use of IT systems already exists. It constitutes an element of unavoidable changes resulting from technological progress. The technological solutions adopted and introduced in practice do not always ensure full control of the scope and quantity of communications data provided by the obliged telecommunications companies. As practice shows, errors and inaccuracy take place quite often and cannot be eliminated. In practice, telecommunications companies provide data in a wider scope than that specified in the request for them. That happens because some telecommunications companies' systems generate data in a wider scope than it is necessary from the perspective of the requests. It is a violation of Article 160 (1) in connection with Article 159 (1) points 3–5 and Article 159 (3) of the TL, and Article 218 § 1 of the CPC. The provisions of the TL should clearly lay down when and according to what principles automatic systems may be used. The legal provisions currently in force do not lay down such detailed regulations. *De lege ferenda*, it is necessary to call for the adoption of such regulations to Act on the Telecommunications Law and make a delegation to issue an ordinance defining technical requirements for the use of such systems.

5. The provision of data should be partially charged for. At present, in accordance with the TL in force, the provision of communications data is free of charge. The introduction of fees might reduce the number of requests made by the authorised entities. It would also result in more careful specification of requested communications data by the authorised entities.

6. Apart from the already presented solutions in the field of amending the proceeding provisions or the provisions determining grounds for the authorised entities' requests, legal solutions that are organisational and institutional in character should be introduced. A mechanism of effective control of the acquired communications data should be established. At present, there is no entity in the legal system that would supervise the use of the authorised entities' entitlements to request and use communications messages and data. The establishment of a legal mechanism ensuring the deletion of the acquired data when they are no longer necessary should be part of the presented solutions. A reporting mechanism ensuring detailed information on the scope of the acquired communications data, e.g. the number of persons whose data were acquired or the number of the established personal data of telephone users, should also be introduced.

Conclusions

1. The invalidity of 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/EC declared by the Court of Justice of the European Union (Grand Chamber) in joined cases C293/12 and C594/12 results in the necessity of starting work on the amendments to the Telecommunications Law with respect to the retention and provision of communications data.

2. It is necessary to work out new model solutions with respect to the retention and provision of communications data that must be dependent on the following assumptions:
– precise determination of the purpose of data collection;
– applicability of the subsidiarity principle;
– introduction of guarantees for persons doing the jobs of public trust;
– adoption of new regulations with respect to the acquisition of communications messages and data with the use of IT systems;
– introduction of partial payment for the provision of data;
– introduction of legal organisational and institutional solutions assuring effective control over the acquisition of communications data.

ARE THE REGULATIONS WITH RESPECT TO THE RETENTION AND PROVISION OF COMMUNICATIONS DATA APPROPRIATE IN POLAND? PROPOSALS FOR CHANGES

Summary

The article deals with the issue of the provision of communications data in Poland on demand made by authorised entities, especially courts and public prosecution. The article discusses interpretational doubts both with respect to the regulations giving authorised entities grounds for demanding communications data and the provisions regulating the telecommunications companies' duties with respect to the provision of these data. The article presents problems connected with the application of the provisions in practice. It contains a range of proposals for changes of the provisions regulating the sphere, aimed at eliminating the existing interpretational doubts and practical problems.

CZY UREGULOWANIA W ZAKRESIE GROMADZENIA I UDOSTĘPNIANIA DANYCH TELEKOMUNIKACYJNYCH W POLSCE SĄ PRAWIDŁOWE? PROPOZYCJE ZMIAN

Streszczenie

Przedmiotem artykułu jest problematyka udostępniania danych telekomunikacyjnych w Polsce na żądania podmiotów uprawnionych, w szczególności sądu i prokuratora. Artykuł omawia wątpliwości interpretacyjne zarówno w zakresie stosowania przepisów stanowiących podstawę do żądania danych telekomunikacyjnych przez uprawnione do tego podmioty, jak i przepisów regulujących obowiązki przedsiębiorców telekomunikacyjnych w zakresie udostępniania tych danych. Przedstawione są problemy w stosowaniu tych przepisów w praktyce. Artykuł zawiera szereg propozycji zmian przepisów regulujących omawianą problematykę, zmierzających do wyeliminowania istniejących wątpliwości interpretacyjnych i problemów praktycznych.

LES RÈGLEMENTS DU RAMASSAGE ET DE L'ACCÈS AUX DONNÉES DE TÉLÉCOMMUNICATION SONT-ILS RÉGULIERS EN POLOGNE? LES PROPOSITIONS DES CHANGEMENTS

Résumé

Le sujet de l'article concerne l'accès aux données de télécommunication en Pologne à la demande des services autorisés, en particulier le tribunal et la procurature. L'article parle des doutes de l'interprétation dans le cadre de l'application des règlements formant la base pour demandes des données de télécommunication par des services autorisés ainsi que des règlements qui régularisent les devoirs des entrepreneurs de télécommunication dans le cadre de l'accès à ces données. Les problèmes sont présentés à l'application de ces règlements en pratique. L'article contient plusieurs propositions des règlements qui régularisent la problématique pour éliminer les doutes actuels de l'interprétation et les problèmes pratiques.

ЯВЛЯЮТСЯ ЛИ УРЕГУЛИРОВАНИЯ В ОБЛАСТИ СБОРА И ДОСТУПА ТЕЛЕКОММУНИКАЦИОННЫХ ДАННЫХ В ПОЛЬШЕ ЗАКОНОМЕРНЫМИ? ПРЕДЛОЖЕНИЯ ИЗМЕНЕНИЙ

Резюме

Предметом статьи является проблематика предоставления доступа телекоммуникационных данных в Польше по запросу уполномоченных субъектов, прежде всего суда и прокурора. Статья рассматривает интерпретационные сомнения как в области применения положений, служащих основой для запроса телекоммуникационных данных уполномоченными субъектами, так и для положений, регулирующих выполнение обязанностей телекоммуникационных предпринимателей по предоставлению доступа к этим данным. Представлены проблемы, касающиеся применения этих положений на практике. Статья содержит ряд предложений, регулирующих обсуждаемую проблематику, направленных на устранение существующих интерпретационных сомнений и проблем практического характера.