Articles

Studia Iuridica Lublinensia vol. XXX, 2, 2021
DOI: 10.17951/sil.2021.30.2.263-284

Jacek Kudła
Polish Forensic Association, Warmia and Mazury Branch, Poland
ORCID: 0000-0002-4077-3900
jkjacekudla@gmail.com

Alfred Staszak
University of Zielona Góra, Poland
ORCID: 0000-0003-1318-6513
alfredstaszak@wp.pl

Operational Control in the Information Technology System (Postulates *de lege ferenda*)

Kontrola operacyjna w systemie informatycznym (postulaty de lege ferenda)

ABSTRACT

The article presents a proposal for changes in the regulations concerning broadly understood wiretapping. The dynamics of the development of crime using new technologies, in particular cybercrime, poses increasing challenges to the judiciary, law enforcement authorities and special services, which can only be met by introducing new legal solutions to enable the latest technological developments to be applied. At the same time, judicial case law imposes an obligation on the legislator to seek and create new legal solutions that would be able to reconcile the interests and rights of an individual with the common good. The question, therefore, arises whether a further revision of the rules is necessary in this regard, or whether a completely new approach is needed to look at the way of legal regulations concerning issues related to procedural and operational wiretapping. The article attempts to present this issue, taking into account, in particular, the changes in surveillance regulations due to the continuous and progressive development of the 5G network and the planning of the gradual implementation of the 6G network. In the authors' opinion, the presented constructive comments *de lege ferenda* should be helpful in establishing a new law on operational control. The law that would comply with constitutionally guaranteed standards on civil rights while equipping the state and its

CORRESPONDENCE ADDRESS: Jacek Kudła, Expert Witness, Polish Forensic Association, Warmia and Mazury Branch, 10-719 Olsztyn, Dybowskiego 11, Poland; Alfred Staszak, PhD, Assistant Professor, University of Zielona Góra, Faculty of Law and Administration, 65-069 Zielona Góra, Plac Słowiański 9, Poland.

law enforcement and special services with effective tools to combat new forms and manifestations of crime. The authors intend to present the issue of wiretapping – in the broad sense, against the background of modern technologies and new legal solutions, while respecting the principles of the Polish criminal trial and the expectations of practice in combating the most serious crimes effectively.

Keywords: information technology system; cybercrime; operational control; surveillance regulations; civil rights; modern technologies; procedural and operational wiretapping

INTRODUCTION

The modern way of obtaining data from IAP[1] providers, in order to combat crime[2] and the associated progressive development of 5G networks with 6G perspectives, requires the legislator to gradually and rationally adapt the footnotes of the law to technological[3] developments. At present, taking into account the strict legal criteria, it is no longer only possible to speak of a telecommunications system. Today, we should refer to operational control in the information technology (IT)[4] system or even using the plural – in the IT systems. In Article 2 para. 14 of the National Cybersecurity System Act, the "information system" is predefined as the telecommunications system referred to in Article 3 para. 3 of the Act of 17 February 2005 on the computerisation of the activities of entities performing public tasks along with the data processed in it in electronic form.[5] However, the process of data processing in electronic form means that the scope of the information system includes: the telecommunications system, including data from the cloud,[6] IT data concerning telecommunications transmission, and telecommunications data. The

[1] The term Internet Access Provider (IAP) or Internet Service Provider (ISP) means an Internet service provider. The range of services provided by providers include domain preparation, provision of space and memory for individual servers, creation of a database, e-mail addresses and numerous additional services (for example, online stores, blogs). Suppliers usually tailor their offer to the individual needs of customers, offering complete domain packages for an appropriate fee.

[2] W. Filipkowski, *The use of data mining technology for fighting cyber crimes – selected forensic aspects*, [in:] *Current Problems of the Penal Law and Criminology*, eds. E. Guzik-Makaruk, E.W. Pływaczewski, vol. 7, Warszawa 2017, pp. 386–395.

[3] See K. Ożóg-Wróbel, *Katalog metod prowadzenia czynności operacyjno-rozpoznawczych*, „Roczniki Nauk Prawnych" 2012, vol. 4, p. 122.

[4] The information system and the need to distinguish it were already mentioned in 2015 by B. Hołyst (*Podsłuchiwanie i inwigilacja użytkowników mediów elektronicznych w kontekście bezpieczeństwa informacyjnego*, „Prokuratura i Prawo" 2015, no. 3, p. 7).

[5] Act of 5 July 2018 on the National Cybersecurity System (consolidated text Journal of Laws 2020, item 1369 as amended) implements Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of network and information systems in the territory of the Union (OJ EU L 194/1, 2016).

[6] A. Krasuski, *Chmura obliczeniowa. Prawne aspekty zastosowania*, Warszawa 2018, pp. 75–80.

area of data related to the message, which consists of technical data, metadata and what constitutes the "essence" of the message, i.e. the content of the information, should be categorically separated from each other for the purposes of fair application of the law.[7] The relevant characteristics of the information system are specified in the European Electronic Communications Code, which had to be implemented into national law by 21 December 2020.[8] According to the above-mentioned Code, the basic service in the information system is the so-called "electronic communications service"[9] (hereinafter, respectively, interpersonal communications service).

In this context, the question arises whether the time has come to thoroughly remodel the process and operational control system, so that the regulations can be applied in developing IT systems, where information is exchanged simultaneously between multiple participants in the communication process. The communication process is a complex process of mutual information exchange, and the control of this process cannot be based on the fiction that the wiretapping concerns only one person involved in this process.

THE CURRENT LEGAL STATUS AND OPERATIONAL CONTROL METHODS USED IN IT SYSTEMS

Interpersonal communications services are services that enable interpersonal and interactive exchange of information and include services such as traditional voice calls between two people, or all types of email, messaging or group chat services.[10] Interpersonal communications services include only communication between a "finite" or a certain number of natural persons, as indicated by the person sending the message.

Communication between legal persons should be covered by this definition where natural persons act on behalf of those legal persons or form at least one party to the communication process. Interactive connectivity means that the service allows the recipient of the information to respond. Services that do not meet these requirements,

---

[7] See J. Kudła, A. Staszak, *Procesowa i operacyjna kontrola korespondencji przechowywanej w tzw. chmurze*, „Prokuratura i Prawo" 2017, no. 7–8, pp. 31–57.

[8] Article 124 para. 1 of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)Text with EEA relevance (OJ EU L 321/36, 2018).

[9] Cf. E. Patkowski, *Big Data w służbie służb – sięganie po owoc zakazany (?)*, [in:] *Przestępczość teleinformatyczna 2017*, ed. J. Kosiński, Szczytno 2018, p. 144.

[10] Cf. K. Ożóg-Wróbel, *Przestępstwo kradzieży sygnału telewizyjnego w świetle ustawy o ochronie niektórych usług świadczonych drogą elektroniczną, opartych lub polegających na dostępie warunkowym. Sharing internetowy*, [in:] *Własność intelektualna w sieci*, ed. D. Żak, Lublin 2014, pp. 183–196.

such as linear media services, video-on-demand services, websites, internet networks, social media networks, blogs or the exchange of information between devices respectively, should not be considered as interpersonal communications services. In exceptional circumstances, a service should not be regarded as an interpersonal communications service if the interpersonal and interactive communication tool is only a minor addition to another service and cannot be used without that main service for objective technical reasons and its integration into the service does not serve to bypass the rules governing electronic communications services.

The terms "insignificant" and "purely auxiliary", which are part of the definition, should be interpreted narrowly and from the perspective of the end-user. The interpersonal communication function may be considered insignificant where its objective suitability for the end-user is very limited and when in fact it is barely used by end-users. An example of a function which could be considered not to be covered by the definition of an interpersonal communications service may, in principle, be a communication channel in internet games, depending on the function of the communication tool used in the service. However, interpersonal communications services, and this is very important for the application of operational control, should be divided into those that use numbers from the national or international numbering plan and those that do not use such numbers. What is important, in this case, is the actual control of the provider concerned over signal transmission.

Hence, an interpersonal communication service should be clearly distinguished from an electronic communications service. Electronic communications service is a broader concept and means – a service normally provided, for remuneration, by means of an electronic communications network which includes (with the exception of services related to the provision or control of content transmitted using electronic communications networks or services) the following types of services:

- internet access service as defined in Article 2 point 2 of Regulation (EU) 2015/2120,[11]
- interpersonal communications service (as above),
- services consisting wholly or partly in the conveyance of signals, such as transmission services, used for the provision of machine-to-machine communication services and for broadcasting (the so-called Internet of Things, IoT[12]).

[11] Regulation 2015/2120 of the European Parliament and of the Council, establishing measures relating to open internet access and retail charges for regulated intra-EU communications services and amending Directive 2002/22/WE, as well as Regulation (EU) no. 531/2012 of 25 November 2015 (OJ EU L 310/1, 2015).

[12] Jacek Kudła was an expert of the Working Group for IoT established by the Minister of Digital Affairs in 2018. The result of the work of the Working Group for IoT was a report for the government and educational materials allowing, i.a., the future correct legislation of this issue in the Polish legal system. At the first meeting of the Working Group, he proposed the topic entitled "Obtaining data

All these areas are subject to operational control applied by authorized services in the event of the occurrence and fulfilment of admissibility conditions, respectively. The provisions on operational control still require a new statutory form due to the progressive development of Big Data. For example, in such necessary areas of data separation, for the purposes of proper application of legal provisions (including operational control or data protection pursuant to Article 218a of the Criminal Procedure Code[13]), as "transferring the voice call service to the data transmission domain". It is a legislative activity that will occur sooner or later, due to the adaptation of legal provisions on operational control to modern technological development. However, this should be done in compliance with all information security rules in cyberspace.

Sceptics should be reminded that ensuring security in the network is not an obstacle to the proper regulation of the new operational control in the laws of all services. On the contrary, it draws attention to the areas of the system that should be subject to specific safeguards in order to prevent unauthorized access. This problem has been repeatedly flagged by the authors in the media, which are primarily intended for the legal community.

from IAP and ISP for the purposes of sound law-making, including the development of the Internet of Things (IoT)". Along with the justification saying: "In order to avoid future legal barriers limiting the development of the Internet of Things, and above all, to introduce standards and regulations for this part of the market – it is worth paying attention to the clear distinction between data in cloud computing, further in information and communication systems – for the purposes of establishing and applying legal provisions. The further proceedings of the relevant authorities will then depend on a fair and legal differentiation of data. Therefore, first of all, it is necessary to determine what type of service we are dealing with and then what specific data it is about. The Act on the national cybersecurity system allows the separation of the operator of key services and, respectively, the provider of digital services, which facilitates not only cybersecurity, but also technical aspects of obtaining information technology (IT) data. This Act also allows, with the proper interpretation of the rules, to some extent, to prevent the creation of unjustified legal barriers limiting the development of IoT (e.g. in the field of personal data protection). However, there is still a need to specify in the legislative acts or implementing acts – what data are concerned. In my opinion, the basic criterion for distinguishing data should be their division into technical data and information in all legislative acts, including the IoT industry. From which it is possible to properly read the content of information, reproduce sound and image, and then distinguish them from those from which only technical data can be obtained – also in cloud computing, which is possible in modern teleinformatics and the law-making process".

[13] Act of 6 June 1997 – Criminal Procedure Code (consolidated text Journal of Laws 2021, item 534), hereinafter: CPC.

SECURITY AND DEVELOPMENT OF 5G AND 6G NETWORKS (INTELLIGENT NETWORKS AND SERVICES)

The technical measures of the latest technologies that should be defined in the new regulations on operational control include those listed in the European Electronic Communications Code. These include, i.a., new forms of network management[14] (software emulated networks or programmable networks), Internet Protocol (IP) technology, voice communication service (it's bidirectional), broadly understood IoT,[15] internet telephony (Voice over Internet Protocol, VoIP), messaging services and Internet email services, interpersonal communication service and services consisting solely or mainly in the transmission of signals (i.e. radio spectrum), services consisting wholly or partly in the transmission of signals (such as transmission services, used for the provision of machine-to-machine; IoT) and for broadcasting, as well as Internet access service, femtocells, picocells, metrocells or microcells, etc.

The provisions of the Telecommunications Law Act[16] and other cover the use of radio spectrum by all electronic communication networks, including the new type of radio spectrum use,[17] on the so-called own needs, by new types of networks consisting exclusively of autonomous systems of mobile radio devices which are connected by wireless links. Without central management or a centralised network operator and not always as part of a specific economic activity.[18] In the emerging 5G wireless communications environment such networks are being created, outside buildings by roads, for the purposes of transport (connected cars),[19] energy, research, e-health, public protection and organization of a rescue system in the event of disasters, IoT communications machine-machine. Therefore, the application by Member States, pursuant to Article 7 of Directive 2014/53/EU,[20] additional

[14] E. Guzik-Makaruk, K. Laskowska, *Poczucie bezpieczeństwa oraz zagrożenie cyberterroryzmem w świetle wyników badań empirycznych*, [in:] *Przestępczość w XXI wieku – zapobieganie i zwalczanie. Problemy technologiczno-informatyczne*, eds. E.W. Pływaczewski, W. Filipkowski, Z. Rau, Warszawa 2015, p. 646.

[15] See A. Krasuski, *op. cit.*, p. 221.

[16] Article 111 para. 3 item 2, Article 112 para. 4 item 8 and Article 189 para. 2 item 2 letter e of the Act of 16 July 2004 – Telecommunications Law (Journal of Laws 2019, item 2460).

[17] Annexes 1, 2 and 3 of the Commission Implementing Decision 2020/167 on harmonised standards for radio equipment, drawn up for the purposes of Directive 2014/53/EU of the European Parliament and of the Council of 5 February 2020 (OJ EU L L 34/46, 2020).

[18] Cf., i.a., identification of the legal requirements related to the performance of business activities by a cloud computing broker in A. Krasuski, *op. cit.*, p. 524 ff.

[19] See respectively Article 3 point 1 of the Commission Implementing Regulation (EU) 2020/911 of 30 June 2020 specifying the characteristics of small-area wireless access points pursuant to Article 57(2) of Directive (EU) 2018/1972 of the European Parliament and the Council establishing the European Electronic Communications Code (Text with EEA relevance) (OJ EU L 208/48, 2020).

[20] Directive 2014/53/EU of the European Parliament and of the Council on the harmonization of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/WE of 16 April 2014 (OJ EU L 153/62, 2014).

national requirements with regard to the putting into service or operation of such radio equipment, with a view to the effective and efficient use of the radio spectrum and the prevention of harmful interference, should comply with the internal market rules, safety rules and the needs of the services, as appropriate.

In order to ensure greater coordinated availability of the radio spectrum, to obtain very fast fixed and wireless networks, in the context of 5G, the Radio Spectrum Policy Team identified the frequency ranges: 3.4–3.8 GHz and 24.25–27.5 GHz – as appropriate priority bands to meet the 5G Action Plan objectives. The 40.5–43.5 GHz and 66–71 GHz frequency bands have been indicated for further analysis in terms of their possible future use. It was therefore necessary to ensure that, by 31 December 2020, all or part of the 3.4–3.8 GHz and 24.2–27.5 GHz bands are available for terrestrial systems capable of providing wireless broadband electronic communications services, in accordance with harmonized conditions established by technical implementing measures adopted in accordance with Article 4 of Decision no. 676/2002/EC[21] (in addition to Decision 2017/899[22]). As these ranges have specific characteristics in terms of coverage and data throughput, they can be properly combined to meet 5G requirements. However, EU Member States could be exposed to interference which may originate from third countries which, in accordance with the ITU Radio Regulations,[23] have allocated these bands to services other than international mobile telecommunications communications. This may have an impact on the obligation to meet the common implementation deadline. Most likely, the future use of the 26 GHz band for 5G terrestrial wireless services will, i.a., focus on urban and peri-urban areas and hotspot areas. However, it is possible to anticipate the implementation of a certain part of them along the main roads and railway tracks in rural areas. This makes it possible to use the 26 GHz band for services other than 5G wireless networks, outside these geographic areas, for example for business communications or indoor applications. The EU Member States will thus have the possibility to designate and make this band available on a non-specific basis.

The availability of very high-speed networks will be visible in such 5G and 6G coverage areas as: schools, transport hubs, major public service providers and digitally advanced enterprises. This will ensure the availability of uninterrupted 5G coverage in urban areas and on major surface transport lines, as well as the availability of electronic communications networks capable of delivering speeds

[21] Decision no. 676/2002/EC of the European Parliament and of the Council of 7 March 2002 on a regulatory framework for radio spectrum policy in the European Community (Radio Spectrum Decision) (OJ EU L 108/1, 2002).

[22] Decision (EU) 2017/899 of the European Parliament and of the Council of 17 May 2017 on the use of the 470–790 MHz frequency band in the Union (OJ EU L 138/131, 2017).

[23] Regulamin Radiokomunikacyjny. Artykuły, 2016, www.il-pib.pl/images/stories/rozne/Regulamin_Radiokomunikacyjny/pdf/Regulamin_Radiokomunikacyjny_2016-2019-Tom1.pdf [access: 10.02.2021].

of at least 100 Mbps, with the possibility of increasing to gigabit speeds, for all households. Therefore, the development of new technologies is so rapid that it becomes necessary to adapt to it regulations regarding, i.a., operational control.

It should be emphasized that under the next "Horizon Europe" program the Commission has taken action on 6G networks (smart grids and services). According to the Communication from the Commission to the European Parliament and the Council, the European Economic and Social Committee, and the Committee of the Regions of 29 January 2020 states (see also the Risk Category Annex),[24] the Commission intends to complete the implementation of the 5G network and start preparations for the 6G network, i.e. next-generation mobile technology. All these arguments mentioned above, in a way, require new regulations.[25] Not only for warranty purposes, but also for the needs of new operational activities of the services.

OPERATIONAL CONTROL IN THE INFORMATION SYSTEM – CONSTRUCTIVE COMMENTS *DE LEGE FERENDA* AS A VOICE IN THE DISCUSSION ON THE LEGAL LIMITS OF OPERATIONAL CONTROL

We would like to start not so much with the operational control, but with the code-based call control and recording, and above all, with the presentation of the question: Are the call control and recording referred to in Article 237 CPC useful in practice? Practitioners (mainly prosecutors) argue these thare the so-called "dead legal norms".[26]

As a rule, one should agree with this thesis, taking into account the statistics and the results of trial wiretapping in preparatory proceedings. So, what could be the cause of this fact? Well, according to the interpretation of the law, when a pre-trial is conducted, procedural wiretapping should, in principle, be used.[27] After all, it provides guarantees that cannot be found in operational wiretapping. The basic premises which in practice speak for the use of operational control rather than pro-

[24] Communication from the Commission to the European Parliament and the Council, the European Economic and Social Committee and the Committee of the Regions – Safe deployment of the 5G network in the EU – Implementation of the EU Toolkit, Brussels, 29.01.2020, COM(2020) 50 final.

[25] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions – A New Industrial Strategy for Europe – Brussels, 10.03.2020, COM(2020) 102 final.

[26] A. Staszak, *Ewolucja przepisów dotyczących podsłuchu procesowego – niewielkie zmiany o istotnym znaczeniu*, [in:] *Zmiany w prawie karnym materialnym i procesowym w latach 2013–2017. Zagadnienia wybrane*, ed. H. Paluszkiewicz, „Acta Iuridica Lebusana" 2017, no. 7, p. 113.

[27] Cf. P. Hofmański, S. Zabłocki, *Elementy metodyki pracy sędziego w sprawach karnych*, Warszawa 2011, pp. 453–456.

cess control and consolidation of conversations are precisely the issues of specific guarantees. The practice therefore forces us to address this controversial legal issue.

A trial wiretapping may be started after the proceedings have been initiated and shall be ordered by the court at the request of the prosecutor. It is inadmissible as part of operational and exploratory activities. This is the problem that occurs during process wiretapping and determines its rare use. Disabling the so-called operational mode in its inference, as a consequence, in practice causes countless obstacles related to, i.e., circulation of documentation from process wiretapping, to which operational staff has difficult or no access. This further entails a lack of analysis of the wiretapping information, which is in principle carried out by the prosecutor or the designated officer conducting the preparatory proceedings. As a result, the wiretapping is so highly formalized in terms of processes that, as a consequence, it becomes useless (without going into further details).

The explanation for this situation, however, is that in accordance with Article 239 § 2 CPC announcement of the decision on the control and recording of telephone conversations to a person in preparatory proceedings may be postponed until such proceedings have been concluded. Hence, when it comes to procedural guarantees, it is a reliable solution, but when it comes to the practical prerequisites for the effectiveness of wiretapping, it comes down to "notifying" the person to whom the trial wiretapping was used fairly quickly, already at the end of the proceedings. In the case of the latter, one of the authors using both operational wiretaps and observing trial wiretaps encountered a situation in which trial wiretapping had just been ordered, and only within three weeks – the person to whom it was used – has been notified of the decision on call control and recording (as the preparatory proceedings have been completed).

This is also the case today and it results not so much from the incompetence of the procedural authority, but from the strict application by this authority of the legal norms of the Criminal Procedure Code and other guarantee provisions, including EU regulations. Unfortunately, an additional obstacle is the necessity of "forced" finding true factual evidence by the officers of operational and exploratory divisions of the services, constituting the basis for applying operational control, when the preparatory proceedings are already underway. It should be said *expressis verbis*, because the current structure of regulations often forces them to search for new factual findings that would allow for managing operational controls in the event that preparatory proceedings are already underway. During operational control, officers also have greater detection capabilities related to the use (i.e. "operating kitchen"), which in the case of trial wiretapping are missing (i.e. complete lack of operational work). This further affects its effectiveness. Therefore, it is necessary to consider a complete change of regulations, in this respect, in order to prevent the functioning in the Polish legal system of ineffective and unnecessary call control and recording. As Z. Brodzisz repeatedly emphasized, "it is therefore justified in this

situation to incorporate into the CPC the so-called unconventional evidence, which is currently obtained to combat crimes in operational and exploratory activities, on the basis of police regulations and other".[28]

It should also be added that the decision to control and record conversations should be delivered to the person affected by the wiretapping,[29] which causes further procedural consequences. *A contrario*, in the case of operational control pursuant to Article 19 para. 16 of Act of 6 April 1990 on the Police[30] the person against whom the operational control was applied shall not be made available to the materials collected during the control.[31] The provision does not affect the rights under Article 321 CPC. It does not mean, however, that the person to whom the operational control was applied cannot get acquainted with the materials from this control. This takes place accordingly at a given stage of the criminal proceedings. Therefore, in a simplified way, the legal norms of regulations should not be constructed in such a way as to lead to cases of almost immediate "notification" of a given person to whom wiretapping was used. Such investigative and, respectively (*de lege ferenda*) operational and exploratory activities would be ineffective and, consequently, useless. Hence, it is necessary to adapt the regulations to the new requirements of operational control, in the information system, while maintaining the guarantee standards in a proportionate manner. These standards should not have a negative impact on the effectiveness of operational and exploratory activities, and at the same time should constitute procedural and further constitutional guarantees. Maintaining the proportions between the values mentioned in the case of operational wiretapping is particularly desirable.[32] As A. Staszak stated, "as long as the prosecutor and the court are not sufficiently responsible for the outcome of the proceedings (they will not be responsible for determining the perpetrator of the crime, its trial and conviction), they will not have the practical application".[33] Also today, the critical remarks concerning Article 239 CPC presented in doctrine seem to be valid.[34] They are the answer to the question of why monitoring and recording conversations are rarely or not used in practice.[35]

---

[28] J. Skorupka, *Kodeks postępowania karnego. Komentarz*, Warszawa 2020, p. 858.

[29] *Ibidem*, p. 587.

[30] Act of 6 April 1990 on the Police (consolidated text Journal of Laws 2020, item 360), hereinafter: P.A.

[31] *Ochrona danych osobowych w ściganiu przestępstw. Standardy krajowe i unijne*, eds. M. Kusak, P. Wiliński, Warszawa 2020, p. 116.

[32] A. Grzelak, *Data Retention Saga Continues: Decision of the Polish Constitutional Tribunal of 30 July 2014 in Case K 23/11*, "European Public Law" 2016, vol. 22(3), pp. 475–488.

[33] Staszak, *Ewolucja przepisów…*, p. 125.

[34] K. Ponikwia, *Uwagi krytyczne do art. 239 k.p.k.*, „Prokuratura i Prawo" 2002, no. 10, p. 142.

[35] Cf. P. Kosmaty, *Podsłuch procesowy – zamierająca instytucja walki z przestępczością*, „Prokurator" 2009, no. 2, pp. 9–21.

Another problem in the modern practice of applying operational control is the issue of getting acquainted with the materials justifying the use of wiretapping by the locally competent district prosecutor. In the event that the Voivodeship Police Commander requests the operational wiretapping, but the requesting police unit is, e.g., a police station (i.e. the lowest-level organizational unit of the Police). This raises a number of questions about the district attorney's jurisdiction and the possibility of the district attorney's office being acquainted with the materials for the initial approval, in the form of consent and further transfer to the court, or not consenting to further action, on the application of operational control.

Firstly, it should be emphasized that the Act on the Police does not limit applications for operational wiretapping only to the scope of competence of the Voivodeship Police Headquarters. The fact that the application is made by the Voivodeship Police Commander does not mean that it comes, e.g., from the criminal department of the Voivodeship Police Headquarters. It may come from the District Police Headquarters or even, in justified cases, from the police station. Although, in the authors' opinion, small operational units in police stations are not properly prepared for handling the so-called application of operational controls. If it is necessary to apply it by small units, i.e. with only few numbers of staff, the operational matter should be taken over by the superior unit. Therefore, if the application for an operational control was drawn up by an officer from the operational and exploratory unit of the Police station, this process should be further monitored by a designated person from the superior unit until the district prosecutor is thoroughly familiarized with the materials justifying the operational control. Or such a case should be taken over, e.g., by the Voivodeship Police Headquarters or other higher-level units, respectively (e.g. Central Police Investigation Bureau or Police Internal Affairs Office). In the authors' opinion, this problem should be solved today through the appropriate use of operational control coordinators referred to in the instructional regulations.[36] Unfortunately, the instructional regulations should also be changed, and even some regulations should be introduced into the laws of the services. At present, the Voivodeship Police Commanders designate the regional operational control coordinators, and their duties are:

- monitoring of problems that hinder efficient and effective operational control and providing advisory assistance to Police organisational units in the area of the voivodeship with regard to performing activities related to operational control,
- ensuring proper knowledge of regulations governing the performance of operational controls and the ability to apply them in practice by police officers of Police organizational units operating in the voivodeship.

[36] Decision no. 290 of the Chief Commander of the Police of 13 August 2014 on defining the division of official tasks of police officers performing activities in the scope of preparation and handling of operational documentation (Official Journal of the Police Headquarters, item 53).

In our opinion, the position of the operational control coordinator should be regulated in statutory provisions. His obligations shall not be limited to those set out in § 16 of the Decision no. 290[37]. Among the tasks listed in the instructional provision, the most important one is missing, namely obliging the operational control coordinator to participate in the presentation and adequately discussing the basic materials justifying the operational control. The new regulations should create opportunities for the prosecutor to obtain, apart from the application for an operational control with justification, at least the most important (basic) materials from the operational case justifying the subsequent ordering of an operational control. Naturally, this is by no means about disclosing the so-called "operating kitchen".[38] In an interview with the prosecutor and when presenting materials excluded from an operational case – the principles of using the operational technique or special technique, including the broadly understood masking, should not be disclosed. When speaking about the materials constituting the basis for the application for wiretapping, the Police officer should present, e.g, a thoroughly prepared "analytical" official memo or the results of certain operational methods without revealing the details of these methods. In addition, it should indicate the premises for the Police to comply with the principle of subsidiarity and other materials that would meet the legislator's expectations, constituting the conditions for the admissibility of the application of operational control, which were listed in the Act. These arguments will convince the prosecutor and then the court of the legitimacy of applying operational control. The authors' dream is that the officers applying for operational control should be able to argue the knowledge gained during the operational and exploratory activities in a statutory language, understandable for the prosecutor and judge. This role would be *de lege ferenda* fulfilled by the operational control coordinator mentioned in the legislation. Not only the voivodeship coordinator, but also the operational control coordinator in the Central Police Investigation Bureau and Police Internal Affairs Office.

The question arises about organizational issues. This issue should be left to internal regulation by individual services, as there is no need to create a section of operational control coordinators in organizational units, e.g. the Police. It is simply about appointing a person who would be responsible for the preparation of materials justifying the application of operational control for the court or the prosecutor in the voivodeship, and then be able to substantively talk about them with the prosecutor and present them to the court accordingly. This is to convey to the authorities the statutory rationale enabling them to make a positive or negative decision. The operational control coordinator should be neutral. Therefore,

[37] *Ibidem*.

[38] See J. Kudła, *Glosa do wyroku SA w Warszawie z 29.01.2020 r., sygn. akt II AKa 219/19*, LEX/el. 2020.

if during the presentation of materials and a (substantive) discussion, e.g. with the prosecutor, new findings and assessments affecting the actual state of affairs were made, the coordinator would also be able to understand the negative decision of the authority. He would then be able to pass it on and substantively justify it to the Voivodeship Police Commander. Hence, he would act as an independent, neutral person. One should fully agree with the Court of Appeal in Bialystok that "the court's decision to consent to an operational control may be of a blank form, referring to the contents of the application for such control. The admissibility of such a form of a court order results from specific regulations, and therefore it does not violate the requirements of Article 94 § 1 CPC".[39] However, the materials that justify its conduct can no longer be of a blank form, which results *expressis verbis* from the interpretation of the law.

Against the background of the above position taken by the Court of Appeal in Bialystok, another legal issue arises concerning the application of the new operational control in the information system. In this case, it does not apply directly to the services, but to the body which ultimately manages the operational control, pursuant to Article 19 para. 1 P.A. and accordingly consents to it, pursuant to Article 19 para. 3 P.A. – that is, the district court.

According to the current legal status, the district court may issue two types of decisions after considering the Police application (other services respectively). Firstly, it may consent to the application of operational controls in the form of an order. The decision to give consent must specify the time for which the operational control may be applied and the time when it may begin. Secondly, the court may disregard the Police application, i.e. the Police Chief Commander, Central Police Investigation Bureau Commander, Police Internal Affairs Office Commander or the Vivodeship Police Commander (relevant entities in the case of other services). It should be noted that if the regional court orders or expresses its consent to apply the operational control, it does not have to prepare a justification for the issued decision (Article 98 § 3 CPC applies accordingly). However, it is obligatorily required to do so, in the event of not ordering or not consenting to operational wiretapping. If the court does not order or does not consent to the activity in question, then it is bound by the seven-day period referred to in Article 98 § 2 CPC. Namely, in a complex case or for other important reasons, the preparation of the justification for the decision may be postponed for up to seven days. This deadline is of an instructional nature, so exceeding it does not have procedural consequences. This is the case when the judgement is subject to appeal (Article 98 § 3 last sentence CPC).[40]

[39] Judgement of the Court of Appeal in Bialystok of 16 January 2014, II AKa 260/13, LEX no. 1422328.

[40] Based on Article 19 para. 20 P.A. on court decisions referred to in Article 19 para. 1, 3, 8 and 9 P.A. an appeal may be lodged by the Police authority which submitted the application for this deci-

It seems, while still analysing the legal norm of Article 98 § 3 CPC and taking into account the guarantee of the whole procedure, that the role of the prosecutor participating in a closed session remains extremely important, who, while maintaining the principle of adversarial procedure, remains independent and fully objective. Also taking into account the criteria of his prior consent.

De lege ferenda the authors propose that the district court should prepare a justification statement for the order in question, regardless of whether it ordered or consented to the application of operational control or refused to do so. The district court's justification for all decisions issued on operational control, in addition to meeting the basic procedural guarantees, would additionally justify the final and reliable substantive assessment of the materials received. Moreover, it would make it easier for the services to carry out a legal analysis of all the decisions made. This would consequently affect the quality of police work in the conducted operational cases.

Similarly, *de lege ferenda* should be followed in the case of application of Article 168b CPC. Currently, the decision on the use of this evidence, at a certain stage of criminal proceedings, the legislator has reserved for the prosecutor, as it is only the prosecutor at the stage of formulating the accusation that decides what supporting evidence will be presented to the court. The "subsequent consent" of the prosecutor, pursuant to Article 168b CPC, does not close the further judicial assessment of the evidence in question unless the prosecutor does not express "quasi-authentic consent".[41] As emphasized, in the current legal state, the procedural decision on granting the "quasi-subsequent consent" referred to in Article 168b CPC, or the decision not to grant such consent is made by the prosecutor.[42] This decision is not specified in the Act as a form of decision reserved only for the court. It is a procedural decision which, under the Code of Criminal Procedure, should take the form of a decision.

As a rule[43], the public prosecutor issues a decision pursuant to Article 93 § 3 CPC. The right to lodge a complaint against the prosecutor's decision concerning the subsequent consent under Article 168b CPC has not been expressly provided for by law in the case of operational control. Therefore, Article 465 § 2 CPC is only a provision allowing to determine the jurisdiction to hear a complaint, if such a possibility *de lege ferenda* is included in the Act. Separately, in the case of procedural wiretapping, i.e. call control and recording, appealing against the pros-

sion. As well as the court decision referred to in Article 19 par. 3 P.A. the complaint may be lodged by the competent public prosecutor referred to in Article 19 para. 1 P.A. The provisions of the Code of Criminal Procedure apply accordingly to the complaint.

[41] S. Hoc, J. Kudła, *Zgoda następcza z art. 168b Kodeksu postępowania karnego. Komentarz praktyczny*, LEX/el. 2016.

[42] D. Szumiło-Kulczycka, *Dalsze wykorzystywanie materiałów z kontroli operacyjnej (uwagi na tle art. 168b k.p.k.)*, „Państwo i Prawo" 2018, no. 10, pp. 107–120.

[43] According to Article 93 § 3 CPC the prosecutor may issue an order as to the materials received from the police requiring the so-called "successive consent".

ecutor's decision to the court is possible pursuant to Article 240 CPC. Therefore, *de lege ferenda*, the possibility of appealing against the prosecutor's decision in the scope of the so-called "subsequent consent" referred to in Article 168b CPC would ensure the full guarantee of the provisions. It would also allow the Police to lodge a complaint, also in this respect.

Another legal issue strictly related to the operational control applied in the information system is the so-called "catalogue of offences" referred to in Article 19 para. 1 P.A. For years, the legislator and the doctrine have justified the need for its changes, which, however, consist in its continuous extension with new crimes. In the opinion of the authors, the most difficult question is whether to completely abolish the current catalogue in favour of a more general catalogue, i.e. not referring to specific crimes *expressis verbis* indicated in the enumerative system. Conditioning to the use of wiretapping, e.g., could then be associated with an intentional crime punishable by imprisonment from one year (this is, of course, the statutory penalty), as well as a sexual offence, as well as a crime resulting in the death of a human being (in this case also an unintentional offence).

In view of the conflict of many positions on this legal issue, arguments must be put forward both for changing the catalogue and for maintaining its current normative form. Certainly, the constant change of the catalogue is in favour of certain statutory changes. Therefore, how many times should it be amended taking into account the legal guarantees in force in this matter. One of the proposals is such a change of the catalogue, which would consist in indicating that it is permissible to apply operational control only in the case of intentional crimes punishable by imprisonment, the lower limit of the statutory threat is not lower than one year of imprisonment. However, in the case of fiscal offences that expose the state to a reduction in public fiscal liabilities, in a certain amount – as a consequence, indicating its amount either by amount or by referring it to a multiple of the remuneration.[44] These thresholds must, however, be selected appropriately so that offences with a high social harmfulness do not remain beyond them, as is currently the case with the crime of rape under Article 197 § 1 of the Penal Code. On this occasion, it would be worth considering the limits of the statutory threat to certain crimes of a particularly high degree of social harmfulness (e.g. the crime of forced abortion under Article 152 of the Penal Code, environmental pollution of significant proportions under Article 182 of the Penal Code, inappropriate handling of waste under Article 183 of the Penal Code, etc.), as well as increasingly common fiscal offences. A similar solution was indicated by the legislator, respectively, in Article 607b CPC – this is the case of the European Arrest Warrant. Such

[44] A. Staszak, *Refleksje na temat procesowego wykorzystania materiałów zgromadzonych podczas stosowania kontroli operacyjnej (w świetle uchwały SN z 28 czerwca 2018r., I KZP 4/18)*, [in:] *Zmiany w prawie karnym materialnym i procesowym w latach 2013–2017. Zagadnienia wybrane*, ed. H. Paluszkiewicz, „Acta Iuridica Lebusana" 2019, no. 11, p. 117.

a framework of the catalogue of crimes could be supplemented with sexual crimes and crimes resulting in the death of a human being, regardless of the intention of the perpetrator and the final classification of the act adopted.[45]

The current normative form of the so-called "catalogue of crimes" is supported by the current interpretation of the law. It is about the principle of benevolent interpretation of all civil rights and freedoms. These rights can be interpreted broadly, while their limitations – strictly or even narrowly. This is the case in the catalogue of crimes under Article 19 para. 1 P.A. All the limitations that we deal with above all, when applying the legal norms on operational control, "must be treated as an exception and therefore interpreted strictly or narrowly".[46]

The regulation of the catalogue of crimes through the prism of the threat of a penalty raises some doubts. First of all, concerning the possibility of expanding it even further than it is now, in a "twisted" manner, i.e., through constant changes to the Penal Code. Next, "manipulation" at the lower limit of the statutory threat of imprisonment for intentional crimes. The argument supporting this thesis is the multitude of amendments to the Penal Code Act – starting with its great reform and the announcement of the Act on 2 August 1997 to this day.[47] Hence, the catalogue should be clear and legible, not only for lawyers, but also for everyone, and above all for Police officers (respectively officers of other services) who apply operational control. By changing the catalogue in Article 19 para. 1 P.A. *ex officio* the catalogues of crimes referred to in Articles 19a and 19b P.A. are changed. Hence, it is necessary to return to the case where the unclear interpretation of provisions, even enumerated in the current catalogue of crimes, led the officers to unintentional errors.[48]

The much-anticipated changes include the need to regulate the provisions on operational control so that they do not apply to one person and their conversation, as it is now. This change is related to technological development and is necessary for the correct and reliable application of the law. It directly concerns: firstly, the communication process itself, secondly, the possibilities of conducting conversations, and then recording the image and sound, which currently exist in the information system, including the cloud, i.e. in big data sets (Big Data). An interlocutor, i.e. a person conducting a conversation with someone, always performs this process with another entity. This is, according to the communication process, the exchange of information between at least two people. The current legal regulations are inconsistent with the basic communication process taking place in the relation: sender – message

[45] *Ibidem*, p. 118.

[46] L. Morawski, *Zasady wykładni prawa*, Toruń 2010, p. 199.

[47] See all changes since 2 August 1997 of the Act of 6 June 1997 – Penal Code (consolidated text Journal of Laws 2019, item 1950).

[48] Judgement of the Court of Appeal in Katowice of 11 October 2012, II AKa 368/12, LEX no. 1236427 with a gloss by J. Kudła.

– recipient.[49] In turn, when referring to Big Data, it should be noted that the modern information system environment provides so many opportunities for communication between many people, including random people, that it is impossible to list them all.[50] Accordingly, access to them by the services is limited.[51] However, it does not change the fact of conducting conversations between at least two people, other people and random people. For example, exceptionally from the third circle of interests of a potential figurehead that joined discussion or conversation.

This state of affairs does not require a revolution in the regulations, but simply the amendment of several of them. We mean the change, respectively: Article 19 para. 1, Article 19 para. 7 point 4 and Article 19 para. 15 P.A. In the request for the application of operational control cannot be, as it is currently the case, mentioned only the data of the person or other data, allowing for an unambiguous identification of the entity or object to which the operational control will be applied, with an indication of the place or method of its application. There should certainly be the data of the person to whom the operational control will be applied, and the term "other data" should be used in the application but supplemented with many interlocutors and interviews. Hence the legal norm of Article 19 para. 7 point 4 P.A. could read as follows: "The application of the Police authority referred to in para. 1, for an order by the district court of operational control, should contain, in particular: details of conversations and interlocutors of the person or other data allowing for an unambiguous definition of the entity or object to which the operational control will be applied, with an indication of the place or method of its application".[52] The name and surname of the person to whom we apply operational control, as a rule, should be included in the application. However, today the authors encourage to make appropriate additions to the applications, for example "…operational control will be applied to: Jan Kowalski, his conversations and interlocutors…". The first part of the sentence in the application is of a detailed nature, where the given person is mentioned by name and surname. The second part has a general meaning and consists in introducing such notions as: "…his conversations and interlocutors…". This ensures the legal possibility of applying operational control in a modern information system without violating warranty standards.

The application for the application of operational control contains a justification, as well as attachments to it, in the form of materials justifying the need to apply operational control. Details and other data from the operational case, irrelevant

[49] A. Staszak, *Refleksje na temat procesowego wykorzystania materiałów…*, p. 117.

[50] Cf. W. Filipkowski, *Wybrane obszary zastosowania technologii data mining w kryminalistyce*, [in:] *Meandry prawa karnego i kryminalistyki. Księga jubileuszowa Prof. zw. dra hab. Stanisława Pikulskiego*, eds. W. Cieślak, J. Kasprzak, I. Nowicka, Szczytno 2015, pp. 513–523.

[51] Services have limited access to a lot of data due to the fact that data servers are located in different parts of the world.

[52] The authors' proposal of the new legal norm under Article 19 para. 7 point 4 P.A.

to the justification of the application of operational control (as previously stated), should not be presented to the prosecutor and the court. It is not, therefore, a matter of the prosecutor and the court conducting an operational case together with the Police, which they are fully acquainted with. As follows from the provisions of law, these authorities have separate jurisdiction and statutory powers in this respect. The essence, however, is to create real legal possibilities for the prosecutor to become acquainted with such materials to the extent that they justify the admissibility of the use of operational wiretapping.

Another important legal issue that needs to be addressed is the issue of the prosecutor getting acquainted with all the materials from the operational control. Further, at a later stage, the adjudicating court and the controlling court,[53] respectively, familiarize themselves with the materials of the operational work methods used, i.e. the results of some operational and exploratory activities for which evidence was taken. Accordingly, in the case of the prosecutor, he is currently unable to familiarize himself with all the materials from the operational control. These are primarily those referred to in Article 19 para. 15f point 1 P.A. That is, containing information on the secrecy of confession and defence secrecy. These materials, in accordance with Article 19 para. 15f *in fine* P.A., are – upon the order of the Police Commander in Chief, Central Police Investigation Bureau Commander, Police Internal Affairs Office Commander or the Voivodeship Police Commander – immediately, collectively and officially destroyed. They are completely deprived of prosecutorial and court control. The secrecy of confession and the secrecy of a defence constitutes an absolute prohibition of evidence, consisting in the fact that it is forbidden to interrogate as witnesses: a defence counsel or an advocate or legal adviser acting pursuant to Article 245 § 1 CPC with regard to facts of which he became aware while giving legal advice or conducting a case and a clergyman with regard to facts of which he became aware while giving a confession. Therefore, the legislator decided to adopt such a regulation, taking into account in the legislative process the rationale of the Supreme Bar Council regarding the immediate destruction of such materials collected during operational control. An acquaintance of such materials by the court is not even possible, pursuant to Article 19 para. 15h P.A., because the provision only mentions materials from Article 19 para. 15g point 2 P.A. Hence, rightly so, the materials referred to in Article 19 para. 15f point 1 P.A., are completely excluded from prosecution and judicial control. It remains, therefore, necessary to require the Police to thoroughly evaluate such materials. In the remaining scope *de lege ferenda*, after the operational control is completed, all materials should be submitted to the prosecutor's "desk" for evaluation. Both those which, in the opinion of the Police, constitute evidence allowing for the initiation of criminal proceedings or significant

[53] D. Świecki, *Konstrukcja apelacji jako środka odwoławczego w procesie karnym*, Warszawa 2018, p. 229.

for the pending proceedings, as well as those which do not contain such evidence (of course, except for those immediately destroyed under Article 19 para. 15f point 1 P.A.). This is due to the necessity of their reliable assessment, which today rests, in principle, solely with the Police (it naturally concerns materials that do not contain evidence and are destroyed by the Police). It should be remembered, however, that in the case of the operational control applied in the information system, there will be many more materials which do not contain evidence concerning information, as regards so-called random persons – that is to say, those from distant circles of the figure's connections. Hence, it seems that the final decision on the destruction of such materials should be made by the prosecutor, and not the Police, as before. Currently, the legislator has specified in Article 19 para. 17 P.A. that the materials collected during the application of operational control, not containing evidence allowing the initiation of criminal proceedings or evidence relevant to the criminal proceedings in progress, are subject to immediate, protocol and commission destruction. The destruction of the material shall be ordered by the Police authority that requested the order of operational control.[54]

In the case of court proceedings, as a result of which evidence from operational and exploratory activities was carried out, the court is obliged to assess it, based on criminal-procedural regulations. However, in justified cases, it should inspect them with regard to their collection, on the basis of the provisions of the Police acts.[55]

CONCLUSION

The authors are convinced that all the above arguments will constitute important guidelines for future changes that seem essential or even necessary. A thorough overhaul of the system for the application of call control and recording, in the short or long term, seems essential and necessary. It must be based on a thorough understanding of modern Internet communicators, of the technological solutions which form the basis of their functioning and, above all, on a change in the approach to the model that only one person is eavesdropped in a complex communication process. For these reasons, the authors are convinced that these changes are necessary, and the new look at the communication process with the use of information systems will allow for breaking away from the archaic legal system in this respect while ensuring the procedural rights of all participants in the communication process.

Translation Anna Babar

[54] See judgement of the Constitutional Tribunal of 30 July 2014, K 23/11, LEX no. 1491305.

[55] Cf. J. Kudła, *Glosa do wyroku Sądu Apelacyjnego w Warszawie z dnia 29.01.2020 r., sygn. akt 219/19*, LEX no. 2834474.

REFERENCES

Literature

Filipkowski W., *The use of data mining technology for fighting cyber crimes – selected forensic aspects*, [in:] *Current Problems of the Penal Law and Criminology*, eds. E. Guzik-Makaruk, E.W. Pływaczewski, vol. 7, Warszawa 2017.

Filipkowski W., *Wybrane obszary zastosowania technologii data mining w kryminalistyce*, [in:] *Meandry prawa karnego i kryminalistyki. Księga jubileuszowa Prof. zw. dra hab. Stanisława Pikulskiego*, eds. W. Cieślak, J. Kasprzak, I. Nowicka, Szczytno 2015.

Grzelak A., *Data Retention Saga Continues: Decision of the Polish Constitutional Tribunal of 30 July 2014 in Case K 23/11*, "European Public Law" 2016, vol. 22(3).

Guzik-Makaruk E., Laskowska K., *Poczucie bezpieczeństwa oraz zagrożenie cyberterroryzmem w świetle wyników badań empirycznych*, [in:] *Przestępczość w XXI wieku – zapobieganie i zwalczanie. Problemy technologiczno-informatyczne*, eds. E.W. Pływaczewski, W. Filipkowski, Z. Rau, Warszawa 2015.

Hoc S., Kudła J., *Zgoda następcza z art. 168b Kodeksu postępowania karnego. Komentarz praktyczny*, LEX/el. 2016.

Hofmański P., Zabłocki S., *Elementy metodyki pracy sędziego w sprawach karnych*, Warszawa 2011.

Hołyst B., *Podsłuchiwanie i inwigilacja użytkowników mediów elektronicznych w kontekście bezpieczeństwa informacyjnego*, „Prokuratura i Prawo" 2015, no. 3.

Kosmaty P., *Podsłuch procesowy – zamierająca instytucja walki z przestępczością*, „Prokurator" 2009, no. 2.

Krasuski A., *Chmura obliczeniowa. Prawne aspekty zastosowania*, Warszawa 2018.

Kudła J., *Glosa do wyroku SA w Warszawie z 29.01.2020 r., sygn. akt II AKa 219/19*, LEX/el. 2020.

Kudła J., *Glosa do wyroku Sądu Apelacyjnego w Warszawie z dnia 29.01.2020 r., sygn. akt 219/19*, LEX no. 2834474.

Kudła J., Staszak A., *Procesowa i operacyjna kontrola korespondencji przechowywanej w tzw. chmurze*, „Prokuratura i Prawo" 2017, no. 7–8.

Morawski L., *Zasady wykładni prawa*, Toruń 2010.

Ochrona danych osobowych w ściganiu przestępstw. Standardy krajowe i unijne, eds. M. Kusak, P. Wiliński, Warszawa 2020.

Ożóg-Wróbel K., *Katalog metod prowadzenia czynności operacyjno-rozpoznawczych*, „Roczniki Nauk Prawnych" 2012, vol. 4.

Ożóg-Wróbel K., *Przestępstwo kradzieży sygnału telewizyjnego w świetle ustawy o ochronie niektórych usług świadczonych drogą elektroniczną, opartych lub polegających na dostępie warunkowym. Sharing internetowy*, [in:] *Własność intelektualna w sieci*, ed. D. Żak, Lublin 2014.

Patkowski E., *Big Data w służbie służb – sięganie po owoc zakazany (?)*, [in:] *Przestępczość teleinformatyczna 2017*, ed. J. Kosiński, Szczytno 2018.

Ponikwia K., *Uwagi krytyczne do art. 239 k.p.k.*, „Prokuratura i Prawo" 2002, no. 10.

Skorupka J., *Kodeks postępowania karnego. Komentarz*, Warszawa 2020.

Staszak A., *Ewolucja przepisów dotyczących podsłuchu procesowego – niewielkie zmiany o istotnym znaczeniu*, [in:] *Zmiany w prawie karnym materialnym i procesowym w latach 2013–2017. Zagadnienia wybrane*, ed. H. Paluszkiewicz, „Acta Iuridica Lebusana" 2017, no. 7.

Staszak A., *Refleksje na temat procesowego wykorzystania materiałów zgromadzonych podczas stosowania kontroli operacyjnej (w świetle uchwały SN z 28 czerwca 2018r., I KZP 4/18)*, [in:] *Zmiany w prawie karnym materialnym i procesowym w latach 2013–2017. Zagadnienia wybrane*, ed. H. Paluszkiewicz, „Acta Iuridica Lebusana" 2019, no. 11.

Szumiło-Kulczycka D., *Dalsze wykorzystywanie materiałów z kontroli operacyjnej (uwagi na tle art. 168b k.p.k.)*, „Państwo i Prawo" 2018, no. 10.
Świecki D., *Konstrukcja apelacji jako środka odwoławczego w procesie karnym*, Warszawa 2018.

Netography

Regulamin Radiokomunikacyjny. Artykuły, 2016, www.il-pib.pl/images/stories/rozne/Regulamin_Radiokomunikacyjny/pdf/Regulamin_Radiokomunikacyjny_2016-2019-Tom1.pdf [access: 10.02.2021].

Legal acts

Act of 6 April 1990 on the Police (consolidated text Journal of Laws 2020, item 360).
Act of 6 June 1997 – Penal Code (consolidated text Journal of Laws 2019, item 1950).
Act of 6 June 1997 – Criminal Procedure Code (consolidated text Journal of Laws 2021, item 534).
Act of 16 July 2004 – Telecommunications Law (Journal of Laws 2019, item 2460).
Act of 5 July 2018 on the National Cybersecurity System (consolidated text Journal of Laws 2020, item 1369 as amended).
Commission Implementing Decision 2020/167 on harmonised standards for radio equipment, drawn up for the purposes of Directive 2014/53/EU of the European Parliament and of the Council of 5 February 2020 (OJ EU L L 34/46, 2020).
Commission Implementing Regulation (EU) 2020/911 of 30 June 2020 specifying the characteristics of small-area wireless access points pursuant to Article 57(2) of Directive (EU) 2018/1972 of the European Parliament and the Council establishing the European Electronic Communications Code (Text with EEA relevance) (OJ EU L 208/48, 2020).
Communication from the Commission to the European Parliament and the Council, the European Economic and Social Committee and the Committee of the Regions – Safe deployment of the 5G network in the EU – Implementation of the EU Toolkit, Brussels, 29.01.2020, COM(2020) 50 final.
Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions – A New Industrial Strategy for Europe – Brussels, 10.03.2020, COM(2020) 102 final.
Decision no. 676/2002/EC of the European Parliament and of the Council of 7 March 2002 on a regulatory framework for radio spectrum policy in the European Community (Radio Spectrum Decision) (OJ EU L 108/1, 2002).
Decision (EU) 2017/899 of the European Parliament and of the Council of 17 May 2017 on the use of the 470–790 MHz frequency band in the Union (OJ EU L 138/131, 2017).
Directive 2014/53/EU of the European Parliament and of the Council on the harmonization of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/WE of 16 April 2014 (OJ EU L 153/62, 2014).
Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of network and information systems in the territory of the Union (OJ EU L 194/1, 2016).
Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)Text with EEA relevance (OJ EU L 321/36, 2018).
Regulation 2015/2120 of the European Parliament and of the Council, establishing measures relating to open internet access and retail charges for regulated intra-EU communications services and amending Directive 2002/22/WE, as well as Regulation (EU) no. 531/2012 of 25 November 2015 (OJ EU L 310/1, 2015).

Case law

Judgement of the Court of Appeal in Katowice of 11 October 2012, II AKa 368/12, LEX no. 1236427.
Judgement of the Court of Appeal in Bialystok of 16 January 2014, II AKa 260/13, LEX no. 1422328.
Judgement of the Constitutional Tribunal of 30 July 2014, K 23/11, LEX no. 1491305.

ABSTRAKT

W artykule przedstawiono propozycję zmian w przepisach dotyczących szeroko rozumianego podsłuchu. Dynamika rozwoju przestępczości posługującej się nowymi technologiami, a w szczególności przestępczości cybernetycznej, stawia przed wymiarem sprawiedliwości, organami ścigania i służbami specjalnymi coraz większe wyzwania, którym można sprostać, jedynie wprowadzając nowe rozwiązania prawne pozwalające na stosowanie najnowszych osiągnięć technicznych. Jednocześnie orzecznictwo sądowe nakłada na ustawodawcę obowiązek poszukiwania i tworzenia nowych rozwiązań prawnych, które potrafiłyby pogodzić interesy i prawa jednostki z dobrem ogólnospołecznym. Powstaje zatem pytanie, czy konieczna jest kolejna nowelizacja przepisów w tym zakresie czy też niezbędne jest całkowicie nowe spojrzenie na sposób unormowań prawnych dotyczących zagadnień związanych z podsłuchem procesowym i operacyjnym. W niniejszym artykule podjęto próbę przedstawienia tej problematyki, biorąc pod uwagę przede wszystkim zmiany przepisów inwigilacyjnych w związku z ciągłym i progresywnym rozwojem sieci 5G i planowaniem stopniowego wdrażania sieci 6G. Przedstawione konstruktywne uwagi *de lege ferenda* w ocenie autorów powinny stać się pomocne do ustanowienia nowego prawa dotyczącego kontroli operacyjnej. Prawa, które czyniłoby zadość normom gwarantowanym konstytucyjnie w zakresie praw obywatelskich i jednocześnie wyposażałoby państwo i jego organy ścigania oraz służby specjalne w skuteczne narzędzia walki z nowymi formami i przejawami przestępczości. Intencją autorów jest przedstawienie problematyki dotyczącej podsłuchu *sensu largo* na tle współczesnych technologii i nowych propozycji rozwiązań prawnych przy jednoczesnym poszanowaniu zasad polskiego procesu karnego oraz oczekiwań praktyki w skutecznym zwalczaniu najpoważniejszych przestępstw.

Słowa kluczowe: system informacyjny; przestępczość cybernetyczna; kontrola operacyjna; przepisy inwigilacyjne; prawa obywatelskie; współczesne technologie; podsłuch procesowy i operacyjny