Ius Novum
1/2020

THREATS TO THE INDIVIDUAL'S RIGHT TO PRIVACY IN RELATION TO PROCESSING OF PERSONAL DATA IN ORDER TO PREVENT AND COMBAT CRIME

KATARZYNA MRÓZ*

DOI: 10.26399/iusnovum.v14.1.2020.05/k.mroz

1. INTRODUCTION

In recent years, personal data protection authorities have faced major challenges in balancing the right to data protection with the responsibilities of the European Union and its member states to ensure the security of its citizens in the area of freedom, security and justice.[1] Maintaining a "just balance" between the fundamental rights and freedoms of individuals and the interests of public security and the national security of the member states has contributed to the discussion on the reform of the personal data protection system. Due to the fast pace of technological changes resulting in an increase in the amount of processed data, the need to ensure effective protection of the individual's rights has led to the development of legally binding mechanisms regulating the transfer and processing of data in a manner consistent with the law of the European Union, in particular allowing compliance with a high standard of protection of the rights of persons whose data are processed.[2]

The universality of personal data protection issues makes it possible for issues relating to this sphere of rights and interests of individuals to arise at the level of criminal proceedings.[3] The subject of the article is the analysis of legal grounds for

* MA, doctoral student at Lazarski University in Warsaw; e-mail: katarzyna.iwona.mroz@gmail.com; ORCID: 0000-0003-4775-7767

1 Cf. Article 3(2) of the Treaty on European Union, Dz.U. of 2004 No. 90, item 864/30; hereinafter TEU.

2 M. Rojszczak, *Prywatność w epoce Wielkiego Brata: podstawy prowadzenia programów masowej inwigilacji w systemie prawnym Stanów Zjednoczonych*, Ius Novum No. 1, 2019, pp. 238–239.

3 A. Wolska-Bagińska, *Ochrona danych osobowych a zasady procesu karnego*, Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury No. 3(31), 2018, p. 23.

processing personal data in criminal proceedings, which undoubtedly constitute one of the fundamental issues in the practice of applying the law. This study analyses the regulatory framework for the protection of personal data processed in connection with the prevention of and fight against crime from the perspective of Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences and the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA,[4] taking into account civil liberties. Evaluation of new assumptions ensuring transparency of data processing by the police and institutions combating crime requires undertaking discussion regarding the limits of data processing, making them available and their control by authorized bodies, including during the performance of operational and investigative activities by appropriately authorized services. Cases of processing information on persons in order to minimise threats to security and public order constitute a starting point for considerations on existing threats to the limitation of individual rights.

The admissibility of limiting the rights and freedoms of individuals in the course of criminal proceedings requires a precise defining in what situations and to what extent this is possible. As Joseph Cannataci, Special Rapporteur on Privacy, appointed by the UN Human Rights Council, rightly pointed out, effective protection of privacy implies "borderless safeguards and protection measures".[5] The adoption of common EU data protection rules is an important step towards more effective cooperation between law enforcement and judicial authorities, as well as trust-building and legal certainty. The strengthening of data subjects' rights and obligations of data subjects processing personal data, as well as their corresponding powers to monitor and enforce personal data protection rules in the member states, has prompted reflection on the legitimacy of the changes made to the legal grounds for personal data protection law in Europe.[6] The summary of the arguments will be concluded with an attempt to assess new assumptions ensuring transparency of data processing by the police and institutions fighting crime, from the point of view of confidentiality guarantees related to data processing in proceedings conducted by competent authorities in this area.

---

[4] OJ EU L of 2016, No. 119, p. 89; hereinafter referred to as Directive 2016/680.

[5] The UN Human Rights Council, Report of the Special Rapporteur on the Right to Privacy, Joseph A. Cannataci, 27.02.2017, A/HRC/34/60, p. 34.

[6] W. Wiewiórowski, *Nowe ramy ochrony danych osobowych w Unii Europejskiej jako wyzwanie dla polskiego sądownictwa*, Kwartalnik Krajowej Rady Sądownictwa No. 1, 2013, p. 14.

2. EU LEGISLATION ON THE PROTECTION OF PERSONAL DATA IN CRIMINAL MATTERS

Achieving a fair balance between the need to safeguard the process of obtaining evidence and the right to respect for the family life of the individual[7] has led to a more effective protection of individuals' data in view of the rapid pace of technological changes contributing to an increase in the volume of data processed. The legal instruments so far have not been sufficient, putting individuals' personal data at increasing risk.[8] As underlined in the Stockholm Programme,[9] technological developments not only present new challenges for the protection of personal data but also offer new opportunities for better data protection that should be exploited.[10] In response to the necessary developments in the area of personal data protection, the EU institutions have started to ensure a high and consistent level of protection of individuals, while removing obstacles to the movement of personal data.

More than 15 years after the introduction of the first regulations in this area,[11] The European Commission presented a communication entitled "A Comprehensive Approach on Personal Data Protection in the European Union"[12]. The 2010 document identified specific challenges, including responding to the impact of new technologies, improving the internal market dimension of data protection, responding to globalisation and improving international data transfers, ensuring better institutional arrangements for effective enforcement of data protection rules, and enhancing the coherence of the legal framework for data protection. The Commission also signalled the need for specific rules in the area of police and judicial cooperation in criminal matters, given the specificities of these areas and the potential differences in the exercise by individuals of certain data protection rights and the need to prevent, investigate, detect or prosecute criminal offences in the enforcement of sanctions in a specific case.[13]

---

[7] ECtHR judgments of: 19 May 2009 in *Kulikowski v. Poland*, Application no. 16831/07, point 77 *in fine*; 11 October 2005 in *Bagiński v. Poland*, Application no. 37444/97, point 94.

[8] See the Explanatory memorandum to the government's bill on the protection of personal data processed in connection with prevention and combating of crime, UC116, https://legislacja.rcl.gov.pl/projekt/12310605 (accessed 31.10.2019).

[9] The Stockholm Programme: An Open and Secure Europe Serving and Protecting Citizens, OJ 2010, C 115, p. 1.

[10] https://www.prawo.pl/prawnicy-sady/zmiany-w-ochronie-danych-osobowych-dotycza-tez-postepowan-karnych,185770.html (accessed 31.10.2019).

[11] See Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, OJ L 281 of 1995, p. 31.

[12] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union, COM/2010/0609 *final*.

[13] An important reason for adopting such a solution was, on the one hand, the need to ensure a consistent and high level of protection of personal data of natural persons and, on the other hand, to facilitate the exchange of personal data between competent authorities of the member states in order to ensure efficient judicial co-operation in criminal matters and police co-operation, as well as the possibility to transfer data to a third country provided that the

As a result, on 25 January 2012 the European Commission presented a draft legislative package containing a new framework for the protection of personal data in the EU.[14] The package consisted of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC[15] and Directive (EU) 2016/680 of the European Parliament and of the Council. The draft act was adopted in March 2014 and is addressed to the Council of the European Union.[16] On 4 May 2016, the official texts of the legal instruments making up the data protection reform,[17] which introduced binding requirements for the protection of privacy and personal data, not only in vertical but also in horizontal relations, were published in the Official Journal of the European Union.[18]

Ensuring a consistent standard of protection of the freedoms and rights of persons by introducing a uniform and effective system of personal data protection was essential to guarantee effective judicial cooperation in criminal matters and police cooperation. Indeed, separate from the general system of protection, regulations were developed relating exclusively to the processing of data in specific aspects of criminal cases.[19] President Jean-Claude Juncker stated in his political guidelines: "The fight against cross-border crime and terrorism is a shared European responsibility".[20] The prevention, investigation, detection and prosecution of criminal offences requires that competent authorities process personal data collected in the context of the prevention, investigation, detection or prosecution of specific criminal offences in order to improve the understanding of criminal activities and to establish links between the various criminal offences detected,[21] nevertheless,

---

purpose of such action is to prosecute criminal offences while ensuring an adequate level of data protection by the third country.

[14] http://eur–lex.europa.eu/legal–content/PL/TXT/?uri=CELEX:52012AR0625 (accessed 21.11.2017).

[15] OJ C 318, 30.12.2011, p. 1. OJ EU of 2016, L 119/1.

[16] http://orka.sejm.gov.pl/wydbas.nsf/0/aa1e06213f088c33c1257d0e00491563/$file/infos_173.pdf (accessed 31.10.2019).

[17] http://www.giodo.gov.pl/1520147/id_art/9278/j/pl/ (accessed 31.10.2019).

[18] For a more detailed discussion of the provisions of the general Regulation, see M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2016; D. Lubasz, E. Bielak-Jomaa (eds), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2017.

[19] The European legislator deliberately excluded from the scope of application of Regulation 2016/679 the processing of personal data by competent authorities for the purpose of preventing crime, investigation, detection and prosecution of criminal offences or executing criminal penalties, including the protection against and prevention of threats to public security, by regulating these issues – due to the specific nature of such activities – in a legal act of a different rank, i.e. Directive 2016/680. The directive, as a legal act obliging the member states to establish a given legal order – in contrast to a regulation whose provisions are directly applicable – allows taking into account differences in national regulations on preventing and combating crime in the provisions prepared on its basis.

[20] A New Start for Europe: My Agenda for Jobs, Growth, Justice and Democratic Change – Political Guidelines for the next term of the European Commission, J.-C. Juncker, Strasbourg, 15.07.2014.

[21] See recital 27 of Directive 2016/680.

in accordance with recital 29 of the Directive, personal data must be collected for specified, explicit and legitimate purposes falling within the scope of application of the Union legal instrument and not processed for purposes incompatible with the prevention, investigation, detection and prosecution of criminal offences and the execution of criminal penalties, including the protection against and prevention of threats to public security.

In accordance with Directive 2016/680, Member States shall: (a) protect the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data; and (b) ensure that, where provided for by Union or national law, the exchange of personal data by competent authorities within the Union is not restricted or prohibited on grounds relating to the protection of individuals with regard to the processing of personal data.[22] Although the member states have primary responsibility for safety, they cannot achieve this on their own. All relevant EU and national actors need to cooperate better in combating cross-border threats, while respecting national compliance obligations and safeguarding internal security.[23]

Law enforcement authorities, due to the nature of their activities, have a special access to the collection of data, the processing of which may involve the risk of infringement of rights and freedoms of individuals, such as economic and social harm, breach of professional secrecy or good name. This risk increases when data concerning, inter alia, racial origin, political opinions, beliefs, health, sexual orientation, genetic or biometric data are processed. As can be seen from recital 15 of Directive 2016/680, the basic objective of this instrument is to ensure an equivalent level of protection of individuals by ensuring effective data protection rights applicable throughout the Union, and to prevent divergences hampering the exchange of personal data between competent authorities. The approximation of member states' laws does not have the effect of weakening the protection of personal data they afford but, on the contrary, serves to ensure a high level of protection throughout the Union.[24] As a result, the European data protection model is now considered to be the most mature in the world and a model for the actions of other legislators.[25]

3. PROCESSING OF PERSONAL DATA IN ORDER TO PREVENT AND COMBAT CRIME IN THE LIGHT OF DIRECTIVE 2016/680/EU

The need to adopt a coherent, systemic solution at the national level, ensuring an efficient interaction of complementary elements of personal data protection stemming from the EU rules (Directive 2016/680 and Regulation 2016/679), while taking into account the multiplicity of public entities, has led to a broad definition of data

[22] See Article 1(2) of Directive 2016/680.

[23] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, European Security Agenda, European Commission, Strasbourg, 28.04.2015, COM(2015) 185 *final*.

[24] See recital 15 of Directive 2016/680.

[25] P. Schwartz, *The EU-U.S. Privacy Collision: a Turn to Institutions and Procedures*, Harvard Law Review Vol. 126, 2013, p. 1968.

processing consisting in the lack of a top-down definition of all activities falling within the scope of this concept. According to Article 4(2) of Regulation 2016/679, "processing" means the operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, adaptation or combination, restriction, erasure or destruction.[26]

Translating the meaning of the term processing of personal data into a criminal-processing context, it should be recognised that any action taken within the framework of a criminal process involving personal information should be classified as processing of data.[27] A particular intensity of activities performed on personal data occurs during the pre-trial phase. During this stage of the process, law enforcement agencies process the largest amount of data in connection with the collection of evidence for the purposes of conducting criminal proceedings. At the stage of jurisdiction proceedings, due to the type and frequency of operations performed during this stage, there is also a significant intensity of operations on personal data. Taking into account the above-mentioned remarks, it should be concluded that the provisions of the Criminal Procedure Code[28] stipulate a number of regulations relating to operations on personal data, i.e. their processing.[29] It is therefore not surprising that the prevention, investigation, detection and prosecution of criminal offences require that competent authorities process personal data collected in the context of the prevention, investigation, detection or prosecution of specific criminal offences in order to better understand criminal activities and to establish links between the different criminal offences detected.[30]

In order to ensure the security of processing and to prevent processing in breach of the Directive, member states must ensure that personal data are: (a) lawfully and fairly processed; (b) collected for specified, explicit and legitimate purposes and not processed in a way incompatible with those purposes; (c) adequate, relevant and not excessive in relation to the purposes for which they are processed; (d) adequate and, where necessary, kept up to date; (f) processed in a way ensuring adequate security of personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, by appropriate technical or organisational measures.[31] Any processing of personal data should include the protection of the vital interests of the data subject.

On the basis of Directive 2016/680, two levels of data categorisation were introduced, distinguishing between data by subject and data type. Categorisation by subject is linked to the introduction of categories of data subjects. Member states

---

[26] The concept of data processing regulated by Directive 2016/680 is covered in the same way as in Article 4(2) of Regulation 2016/679.

[27] A. Wolska-Bagińska, *Podstawy prawne przetwarzania danych osobowych w postępowaniu karnym*, Prokuratura i Prawo No. 6, 2018, p. 48.

[28] Act of 6 June 1997: Criminal Procedure Code, Dz.U. of 2018, item 1987.

[29] A. Wolska-Bagińska, *supra* n. 27, p. 49.

[30] See recital 27 of Directive 2016/680.

[31] Article 4(1) of Directive 2016/680.

therefore must ensure that the controller, where appropriate and possible, clearly distinguishes between personal data of different categories of data subjects, such as the following: (a) persons in respect of whom there are serious grounds for believing that they have committed or are about to commit an offence; (b) persons convicted of an offence; (c) victims of an offence, or persons whose specific facts indicate that they may be liable to become victims of an offence; and (d) persons other than those who, in relation to the criminal offence, such as persons who may be called upon to testify in criminal investigations or at further stages of criminal proceedings, persons who can provide information about the criminal offence or persons who have any contacts or connections with one of the persons referred to in points (a) and (b). This should not prevent the application of the principle of the presumption of innocence guaranteed by the Charter of Fundamental Rights of the European Union and by the Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted respectively by the case law of the Court of Justice and the European Court of Human Rights.[32]

The categorisation by type of data, on the other hand, involves the identification of data which, by their nature, are particularly sensitive in the light of fundamental rights and freedoms. Moreover, they require special protection since the context in which they are processed may give rise to a serious risk of infringing fundamental rights and freedoms. These data include information revealing: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data processed to identify a natural person unambiguously, health, sexuality and sexual orientation of a natural person.[33] In accordance with Article 29(1) of Directive 2016/680, these specific types of data should be covered by a higher standard of data security.

It should be borne in mind that, in any event, infringements of the rights or freedoms of natural persons with different degrees of probability and seriousness of threat can lead to physical, material or non-material damage, in particular: where processing may result in discrimination, identity theft or fraud, financial loss, damage to reputation, breach of confidentiality of data protected by professional secrecy, unauthorised reversal of pseudonymisation or any other substantial economic or social damage. The likelihood and seriousness of a breach is determined by taking into account the nature, extent, context and purposes of the processing. The risk of breach is assessed on the basis of an objective assessment of whether the processing operations present a serious risk.

In transposing these considerations into criminal law, it should be underlined that the nature of the processing of data in criminal matters is linked to the limitations of the right of access to these data. Member states may adopt legal instruments to limit in whole or in part the data subjects' right of access to the data to the extent and for the duration that such partial or total restriction is necessary and proportionate in a democratic society, with due regard for the fundamental rights and legitimate

---

[32] Done at Rome, 4 November 1950, amended by Protocols No. 3, 5 and 8 and supplemented by Protocol No. 2, Dz.U. of 1993, No. 61, item 284.

[33] See Article 10 of Directive 2016/680.

interests of the individual concerned, in order to: (a) prevent obstruction of official or judicial proceedings, investigations or procedures; (b) prevent interference with the prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties; (c) protect public security; (d) protect national security; (e) protect rights and freedoms.[34]

The obligation to inform the data subject of any refusal or restriction of access, together with the grounds for such refusal, shall lie with the controller.[35] Limitations, delays in the right of access or omission in providing of information to data subjects should be individually verified by the data controller in each case. However, the information may be omitted if its provision could undermine any of the purposes for which access to the data has been denied. In this case, however, the following requirements must be met: (a) the controller is required to document the factual and legal grounds on which that decision is based with a view to making them available to the supervisory authorities at a later stage; (b) the controller is obliged to inform the data subject of the possibility of filing a complaint to the supervisory authority or a judicial remedy.

4. TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Directive 2016/680 regulates the exchange of information involving personal data between law enforcement authorities of member states and third countries. The existing regulations in this area in the repealed Directive 95/46/EC of the European Parliament and of the Council were applicable to all processing of personal data within member states, both in the public and private sectors, but they did not apply to the processing of personal data within the framework of activities beyond the scope of the Community law, such as activities in the framework of judicial cooperation in criminal matters and police cooperation. Similarly, the repealed Council Framework Decision 2008/977/JHA applied to judicial cooperation in criminal matters and police cooperation limited to the processing of personal data transmitted or made available only between member states. These rules proved to be insufficient due to the dynamic development of cross-border and international crime, largely due to technological developments in the exchange of information. With this in mind, it has become necessary to prepare a new legal instrument which would comprehensively implement the arrangements for the transfer of personal data in criminal matters to third countries or international organisations. However, it should be noted that the new Directive 2016/680 does not apply to the processing of personal data in the course of activities which fall outside the scope of the Union law, therefore activities in the field of national security, activities of agencies or entities dealing with national security, processing of personal data by member states

[34] See Article 15(1) of Directive 2016/680.
[35] *Ibid.*

in the course of activities which fall within the scope of Title V, Chapter 2 TEU, are not covered by the scope of the Directive.

For the purpose of implementing Article 63 of Directive 2016/680, member states provide that the transfer of personal data by competent authorities, which are or are to be processed after their transfer to a third country or an international organisation, including onward transfer to another third country or an international organisation, may be subject to compliance with national law only if the following conditions are met: (a) the transfer is necessary for the purpose of preventing, investigating, detecting and prosecuting criminal offences and enforcing penalties, including the prevention and protection against threats to public security; (b) personal data are transferred to a controller in a third country or an international organisation that is competent for the aforementioned purposes;[36] (d) the Commission has taken a conformity decision pursuant to Article 36 of the Directive or, in the absence of such a decision, adequate safeguards are provided or exist pursuant to Article 37 or in the absence of a conformity decision pursuant to Article 36 or securities in accordance with Article 37, exceptions to the special situations in accordance with Article 38 shall apply;[37] and (e) in the event of onward transfer to another third country or international organisation, the competent authority that has carried out the initial transfer or another competent authority of the same member state shall authorise the onward transfer after due consideration of all relevant factors, including the gravity of the criminal offence, the purpose for which the personal data were originally transferred and the degree of protection of personal data in the third country or international organisation to which the personal data are onward transferred.

By way of exception to the principle of transfer of personal data to a controller in a third country or an international organisation which is competent for the purposes of preventing, investigating, detecting and prosecuting criminal offences and enforcing penalties, including the prevention and protection against threats to public security, the Union law or a member state law may, subject to international agreements, provide that, on a case-by-case basis, competent authorities may transfer personal data directly to recipients established in third countries only if all of the

---

[36] According to Article 35(2) of Directive 2016/680, member states should provide that the transfer of personal data without the prior authorization of another member state is only allowed if the transfer in question is necessary to prevent an immediate and serious threat to public security in a member state or a third country or to the important interests of a member state, and the prior consent cannot be obtained within a reasonable period of time.

[37] In the absence of a decision finding an adequate level of protection under Article 36 or of appropriate safeguards under Article 37, member states should provide that a transfer or a specific category of transfer of personal data to a third country or international organisation may take place only on condition that the transfer is necessary: (a) to protect the vital interests of the data subject or of another person; (b) in order to safeguard the legitimate interests of the data subject, if the law of the member state transmitting the personal data so provides; (c) to prevent an immediate and serious risk of a breach of public security of a member state or of a third country; (d) on a case-by-case basis, for the purposes of preventing, investigating, detecting and prosecuting criminal offences and enforcing penalties, including protecting against and preventing threats to public security; or (e) in an individual case, to identify, pursue or defend claims in relation to the above objectives.

following conditions are met: (a) the transfer is strictly necessary for the performance of the task of the competent transferring authority under the Union law or under the law of a member state for the purposes of the Directive; (b) the competent authority of the data exporter determines that the fundamental rights and freedoms of the data subject do not override the public interest served by the transfer in question; (c) the competent transferring authority considers that transmission to a competent authority for the purpose of preventing, investigating, detecting and prosecuting criminal offences and enforcing penalties, including protection against and preventing threats to public security, in a third country would be ineffective or inappropriate, in particular because the transmission cannot take place in a timely manner; (d) the authority which is competent for the aforementioned purposes in the third country is informed without undue delay, unless this would be ineffective or inappropriate; and (e) the communicating competent authority must inform the recipient of the specific purpose or purposes for which personal data are to be processed exclusively by the recipient, provided that such processing is necessary.[38]

The Commission and the member states take appropriate measures in favour of third countries and international organisations, i.e. they: (a) develop international cooperation mechanisms to facilitate effective enforcement of personal data protection rules; (b) ensure mutual international assistance in the enforcement of personal data protection rules, including through notification, complaint handling, investigative assistance and exchange of information, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms; (c) involve relevant stakeholders in discussions and activities aimed at promoting international cooperation in the field of personal data protection enforcement; (d) promote the exchange and documentation of personal data protection rules and practices, including on conflicts of jurisdiction with third countries.[39]

5. CONCLUSIONS

In the conditions of global crime and terrorism and organised crime crossing the borders, it is important to prevent threats whose occurrence may cause irreparable damage to legally protected rights.[40] It is not disputed that "the fight against serious crime, particularly organised crime and terrorism, is of paramount importance to guarantee public security and its effectiveness may depend to a large extent on the use of modern investigative techniques"[41]. In view of the above, it is necessary to facilitate the free movement of personal data between competent authorities for the purpose of preventing, investigating, detecting and prosecuting criminal offences and penalties, including for the purpose of preventing and protecting against

[38] Article 39 of Directive 2016/680.

[39] See Article 40 of Directive 2016/680.

[40] M. Zubik, J. Podkowik, R. Rybski, *Prywatność. Wolność u progu D-Day*, Gdańskie Studia Prawnicze Vol. XL, 2018, p. 395.

[41] See recital 51 of the CJEU judgment of 8 April 2014 in joined cases C-293/12 *Digital Rights Ireland Ltd* and C-594/12 *Kärntner Landesregierung and Others*.

threats to public security within the Union and transferring such personal data to third countries and international organisations, while ensuring a high level of protection of personal data. It is clear that the transfer of all data entrusted to public services, without any judicial control and without the possibility of supervising the correctness and legality of the measures taken, does not lead to an increase in confidence in the designated service providers. Protecting the rights of individuals against potential abuses by the police and secret services is becoming a problem.

For the protection of personal data in the member states to be effective, the rights of data subjects, the obligations of those who process personal data and the corresponding powers to monitor and enforce the rules on the protection of personal data in the member states need to be strengthened. Ensuring more effective protection of personal data requires a coordinated response at the European level. The assistance of the Union institutions to member states in further developing mutual trust, making full use of existing tools for exchanging information and strengthening cross-border operational cooperation between competent authorities has contributed to the development of certain standards and the adoption of new legal acts in the area of personal data protection and the right to privacy. The need to balance the right to data protection with the responsibilities of the European Union and the member states to ensure the security of citizens within an area of freedom, security and justice in order to maintain a "fair balance" between the fundamental rights and freedoms of individuals and the public security and national security interests of the member states has contributed to the reform of the system of protection of personal data. Directive 2016/680 is a novelty in the EU legal system, becoming a comprehensive regulation of personal data protection in the area of criminal law and cooperation between authorities whose task is to combat crime. Undoubtedly, the EU legal act has slightly revised the existing approach to the differentiation in the protection of individuals' privacy, strengthening the protection of fundamental rights and democratic control over the policy of the EU in the area of internal security.

The success of the tools put in place by the European Union in recent years is based primarily on shared responsibility, mutual trust and effective cooperation between all the actors involved: the EU institutions and agencies, the member states and national authorities. Such action leads to a stable and more coherent framework for the protection of personal data in the Union and to a strict enforcement of its rules. A good law covering both data protection and data security provisions is valuable not only for the individual citizen but also for the security of the whole country.[42] The protective function of the right must be connected with the possibility of its application.

[42] S. Gwoździewicz, K. Tomaszycki (eds), *Prawne i społeczne aspekty cyberbezpieczeństwa*, Warszawa 2017, p. 26.

BIBLIOGRAPHY

Gwoździewicz S., Tomaszycki K. (eds), *Prawne i społeczne aspekty cyberbezpieczeństwa*, Warszawa 2017.

Krzysztofek M., *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2016.

Lubasz D., Bielak-Jomaa E. (eds), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2017.

Rojszczak M., *Prywatność w epoce Wielkiego Brata: podstawy prowadzenia programów masowej inwigilacji w systemie prawnym Stanów Zjednoczonych*, Ius Novum No. 1, 2019.

Schwartz P., *The EU-U.S. Privacy Collision: a Turn to Institutions and Procedures*, Harvard Law Review Vol. 126, 2013.

Wiewiórowski W., *Nowe ramy ochrony danych osobowych w Unii Europejskiej jako wyzwanie dla polskiego sądownictwa*, Kwartalnik Krajowej Rady Sądownictwa No. 1, 2013.

Wolska-Bagińska A., *Ochrona danych osobowych a zasady procesu karnego*, Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury No. 3(31), 2018.

Wolska-Bagińska A., *Podstawy prawne przetwarzania danych osobowych w postępowaniu karnym*, Prokuratura i Prawo No. 6, 2018.

Zubik M., Podkowik J., Rybski R., *Prywatność. Wolność u progu D-Day*, Gdańskie Studia Prawnicze Vol. XL, 2018.

Documents

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: European Security Agenda, European Commission, Strasbourg, 28.04.2015, COM(2015) 185 *final*.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union, COM/2010/0609 *final*.

A New Start for Europe: My Agenda for Jobs, Growth, Justice and Democratic Change – Political Guidelines for the next term of the European Commission, J.-C. Juncker, Strasbourg, 15.07.2014.

The Stockholm Programme: An Open and Secure Europe Serving and Protecting Citizens, OJ EU Official Journal of 2010, C 115, p. 1.

The UN Human Rights Council, Report of the Special Rapporteur on the Right to Privacy, Joseph A. Cannataci, 27.02.2017, A/HRC/34/60.

Explanatory memorandum to the government's bill on the protection of personal data processed in connection with the prevention and combating of crime, UC116.

Online sources

http://eur–lex.europa.eu/legal–content/PL/TXT/?uri=CELEX:52012AR0625 (accessed 21.11.2017).

http://orka.sejm.gov.pl/wydbas.nsf/0/aa1e06213f088c33c1257d0e00491563/$file/infos_173.pdf (accessed 31.10.2019).

http://www.giodo.gov.pl/1520147/id_art/9278/j/pl/ (accessed 31.10.2019).

https://legislacja.rcl.gov.pl/projekt/12310605 (accessed 31.10.2019).

https://www.prawo.pl/prawnicy-sady/zmiany-w-ochronie-danych-osobowych-dotycza-tez-postepowan-karnych,185770.html (accessed 31.10.2019).

THREATS TO THE INDIVIDUAL'S RIGHT TO PRIVACY IN RELATION TO PROCESSING OF PERSONAL DATA IN ORDER TO PREVENT AND COMBAT CRIME

Summary

The article contains an analysis of the regulation concerning the protection of personal data processed in relation to the prevention and combating of crime from the perspective of solutions contained in Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, p. 89), taking into account civil liberties. The EU regulation of personal data protection in the area of police and judicial cooperation in criminal matters raises the question of the scope of permissible interference of state authorities in the right to privacy. In this article, the author assesses the new assumptions ensuring transparency of data processing by the police and institutions fighting crime from the point of view of confidentiality guarantees related to data processing in proceedings conducted by competent authorities in this area.

Keywords: right to privacy, personal data, crime, police and judicial cooperation

ZAGROŻENIA DLA PRAWA DO PRYWATNOŚCI JEDNOSTKI W ZWIĄZKU Z PRZETWARZANIEM DANYCH OSOBOWYCH W CELU ZAPOBIEGANIA I ZWALCZANIA PRZESTĘPCZOŚCI

Streszczenie

Artykuł zawiera analizę regulacji dotyczącej ochrony danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości z perspektywy rozwiązań zawartych w dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW (Dz.Urz. UE L 119, s. 89), z uwzględnieniem swobód obywatelskich. Unijna regulacja ochrony danych osobowych w obszarze współpracy policyjnej i sądowej w sprawach karnych rodzi pytanie o zakres dopuszczalnej ingerencji organów państwa w prawo do prywatności (*right to privacy*). W niniejszym artykule autorka dokonuje oceny nowych założeń zapewniających transparentność przetwarzania danych przez policję i instytucje zwalczające przestępczość z punktu widzenia gwarancji poufności związanych z przetwarzaniem danych w postępowaniach prowadzonych przez właściwe w tym zakresie organy.

Słowa kluczowe: prawo do prywatności, dane osobowe, przestępczość, współpraca policyjna i sądowa

AMENAZAS AL DERECHO DE PRIVACIDAD DE INDIVIDUO EN RELACIÓN CON EL TRATAMIENTO DE DATOS PERSONALES CON EL FIN DE PREVENCIÓN Y LUCHA CONTRA LA DELINCUENCIA

Resumen

El artículo presenta un análisis de regulación sobre la protección de datos personales tratados con el fin de prevención y lucha contra la delincuencia desde la perspectiva de soluciones previstas en la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (Diario Oficial de la Unión Europea L 119, p. 89), teniendo en cuenta libertades de los ciudadanos. La regulación comunitaria de la protección de datos personales en el ámbito de cooperación policial y judicial en asuntos penales causa que nace la pregunta sobre el ámbito de la intervención admisible de los órganos estatales en el derecho a la privacidad (*right to privacy*). El autor en el presente artículo hace una valoración de nuevos principios que aseguran la transparencia del tratamiento de datos por policía e instituciones que luchen contra la delincuencia desde el punto de vista de garantía de confidencialidad relacionada con el tratamiento de datos en los procesos llevados por los órganos competentes.

Palabras claves: derecho a la privacidad, datos personales, delincuencia, cooperación policial y judicial

УГРОЗА НАРУШЕНИЯ ПРАВА НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ В СВЯЗИ С ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЦЕЛЯХ ПРЕДУПРЕЖДЕНИЯ И БОРЬБЫ С ПРЕСТУПНОСТЬЮ

Резюме

В статье анализируются положения о защите персональных данных, обрабатываемых в связи с предупреждением и борьбой с преступностью, с точки зрения положений Директивы 2016/680 Европейского парламента и Совета (ЕС) от 27 апреля 2016 года о защите физических лиц в связи с обработкой персональных данных компетентными органами в целях предотвращения, расследования, выявления и преследования уголовных преступлений и исполнения наказаний и о свободном движении таких данных, отменившей Рамочное решение Совета 2008/977/JHA (OJEU L 119, стр. 89). Автор обращает особое внимание на проблему гражданских свобод. В связи с нормативными положениями ЕС, касающимися защиты персональных данных в ходе сотрудничества между полицией и судебными органами по расследованию уголовных дел, встает вопрос о границах допустимого нарушения государственными органами права на неприкосновенность частной жизни (*right to privacy*). В статье содержится оценка новых предложений по обеспечению транспарентности процесса обработки персональных данных полицией и другими правоохранительными институтами с точки зрения гарантий конфиденциальности при обработке персональных данных в ходе процессуальных действий, осуществляемых соответствующими органами.

Ключевые слова: право на неприкосновенность частной жизни, персональные данные, преступность, сотрудничество полиции и судебных органов

BEDROHUNG DES RECHTS DES EINZELNEN AUF PRIVATSPHÄRE IM ZUSAMMENHANG MIT DER VERARBEITUNG PERSONENBEZOGENER DATEN ZUR VERHÜTUNG UND BEKÄMPFUNG VON STRAFTATEN

Zusammenfassung

Der Artikel enthält eine Analyse der Vorschriften zum Schutz personenbezogener Daten, die im Zusammenhang mit der Verhütung und Bekämpfung von Straftaten verarbeitet werden, aus der Perspektive der Lösungen, die in der Richtlinie des Europäischen Parlaments und des Rates (EU) 2016/680 vom 27. April 2016 zum Schutz von Personen bei der Verarbeitung von Daten enthalten sind personenbezogene Daten von zuständigen Behörden zum Zwecke der Kriminalprävention, Ermittlung vor dem Prozess, Aufdeckung und Verfolgung verbotener Handlungen und Vollstreckung von Strafen, zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977 / JI des Rates (Amtsblatt EU L 119, S. 89) unter Berücksichtigung der bürgerlichen Freiheiten. Die EU-Verordnung zum Schutz personenbezogener Daten im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen wirft die Frage nach dem Ausmaß der zulässigen Eingriffe staatlicher Behörden in das Recht auf Privatsphäre auf (*right to privacy*). In diesem Artikel bewertet der Autor neue Annahmen, die die Transparenz der Datenverarbeitung durch die Polizei und die Anti-Kriminalitäts-Institutionen gewährleisten, unter dem Gesichtspunkt der Vertraulichkeitsgarantien im Zusammenhang mit der Datenverarbeitung in Verfahren, die von den zuständigen Behörden durchgeführt werden.

Schlüsselwörter: Recht auf Privatsphäre, personenbezogene Daten, Kriminalität, polizeiliche und justizielle Zusammenarbeit

MENACES CONTRE LE DROIT DE L'INDIVIDU À LA VIE PRIVÉE EN RELATION AVEC LE TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL AFIN DE PRÉVENIR ET DE COMBATTRE LA CRIMINALITÉ

Résumé

L'article contient une analyse de la réglementation relative à la protection des données à caractère personnel traitées dans le cadre de la prévention et de la lutte contre la criminalité, du point de vue des solutions contenues dans la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (Journal officiel UE L 119, p. 89), en tenant compte des libertés civiles. Le règlement de l'UE sur la protection des données à caractère personnel dans le domaine de la coopération policière et judiciaire en matière pénale soulève la question de l'étendue de l'ingérence autorisée des autorités de l'État dans le droit à la vie privée. Dans cet article, l'auteur évalue de nouvelles hypothèses garantissant la transparence du traitement des données par la police et les institutions anti-criminalité, du point de vue des garanties de confidentialité liées au traitement des données dans les procédures conduites par les autorités compétentes.

Mots-clés: droit à la vie privée, données personnelles, criminalité, coopération policière et judiciaire

RISCHI PER IL DIRITTO ALLA PRIVACY DEI SINGOLI IN RELAZIONE AL TRATTAMENTO DEI DATI PERSONALI PER LA PREVENZIONE E LA LOTTA AI REATI

Sintesi

L'articolo contiene un'analisi della disciplina riguardante la protezione dei dati personali trattati a fini di prevenzione e lotta ai reati, nella prospettiva delle soluzioni contenute nella direttiva 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (Gazzetta ufficiale dell'Unione europea L 119/89), tenendo presenti le libertà civili. La disciplina comunitaria di protezione dei dati personali nel settore della collaborazione della polizia e dei tribunali nei procedimenti penali genera la domanda sull'ambito dell'ingerenza ammissibile delle autorità statali nel diritto alla privacy (*right to privacy*). Nel presente articolo l'autore compie una valutazione dei nuovi approcci che assicurano la trasparenza del trattamento dei dati da parte della polizia e delle istituzioni incaricate della lotta contro la criminalità, dal punto di vista delle garanzie di riservatezza legate al trattamento dei dati nei procedimenti condotti dalle autorità competenti in tale ambito.

Parole chiave: diritto alla privacy, dati personali, criminalità, collaborazione della polizia e dei tribunali

Cytuj jako:

Mróz K., *Threats to the individual's right to privacy in relation to processing of personal data in order to prevent and combat crime [Zagrożenia dla prawa do prywatności jednostki w związku z przetwarzaniem danych osobowych w celu zapobiegania i zwalczania przestępczości]*, „Ius Novum" 2020 (14) nr 1, s. 82–97. DOI: 10.26399/iusnovum.v14.1.2020.05/k.mroz

Cite as:

Mróz, K. (2020) 'Threats to the individual's right to privacy in relation to processing of personal data in order to prevent and combat crime'. *Ius Novum* (Vol. 14) 1, 82–97. DOI: 10.26399/iusnovum.v14.1.2020.05/k.mroz