Articles

Studia Iuridica Lublinensia vol. XXVIII, 2, 2019
DOI: 10.17951/sil.2019.28.2.97-106

Sylwia Zaborska
Maria Curie-Skłodowska University in Lublin
ORCID: 0000-0002-9811-9995
sylwia.zaborska@poczta.umcs.lublin.pl

Legal Regulation of the Protection of Biometric Data under the GDPR

Regulacje prawne w zakresie ochrony danych biometrycznych na podstawie RODO

SUMMARY

The purpose of this article is to draw attention to the possibility of using new methods for the identification and verification of individuals, i.e. biometric techniques. Nowadays, the use of biometrics grows, which entails the adaptation of legal norms to current trends. The author points out the changes in the protection of biometric data in connection with the introduction of the GDPR, especially in the context of making biometric data as a special category.

Keywords: biometry; biometric data protection; sensitive personal information

The ongoing development of information technology has made unlocking a phone with fingerprint sensors or by face scanning a commonly used feature. Customers of banks can increasingly use ATMs or other devices by only authenticating their identity with one's physical characteristics. A technology most often used for ATM cash transactions is the technology based on the blood vessel system – palm vein[1]. With this solution, customers do not need to be concerned with the risk of losing their payment cards because they can use their own palms instead[2]. The Polish Ministry of Finance intends to implement similar technological solutions.

[1] R. Lewandowski, *Biometria – nowe zastosowania*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 17, p. 157.

[2] W. Boczoń, *Biometria w bankowości. Co za jej pomocą załatwimy dziś w banku?*, www.bankier.pl/wiadomosc/Biometria-w-bankowosci-Co-za-jej-pomoca-zalatwimy-dzis-w-banku-7542743.html [access: 6.12.2018].

It is planned to introduce the voice identification of taxable persons who call the National Tax Information. However, this idea faced many controversies, as well as an intervention by the Polish Ombudsman due to concerns about the breach of the callers' right to privacy[3].

The need to find an effective method of proof of identity appeared with the development of documents and the necessity to exchange them between people. In practice, one can find a number of methods of verification and identification[4] whether a person is the one who he claims to be. This most often entails checking whether an individual is able to produce a specific object, such as a key or magnetic card[5]. Another method of verification is based on knowledge and involves asking questions about the fact the authorised person should be aware of, e.g. the PIN or password[6]. As these traditional means of identification or verification of individuals are far from being perfect and reliable, they are increasingly replaced by state-of-the-art technologies, such as biometric systems. These systems consist of the digital measurement of certain anatomical or behavioural characteristics of a human body and then compare the results obtained with the reference characteristics. This means that biometric systems boil down to matching the set of characteristics of the observed object with a set of characteristics previously recorded. A positive match result affects the final decision on the decision regarding the recognition of a given person[7].

Biometrics is the scientific discipline aimed at establishing the identity of a human being using his or her unique features and skills. It is interdisciplinary in nature, because it uses achievements of such disciplines as biology, mathematics, engineering and probability theory[8]. The very term "biometrics" is derived from the Greek, where *bios* means 'life', while *metron* means 'to measure'[9].

Each person has unique characteristics of the external appearance, body or behaviour, which is referred to as biometric characteristics. The literature on the subject distinguishes between individual characteristics of a human being into biologi-

[3] For more details, see *Rzecznik w sprawie rozpoznawania głosu osób dzwoniących na Krajową Informację Podatkową*, www.rpo.gov.pl/pl/content/rzecznik-w-sprawie-rozpoznawania-glosu-osob-dzwoniacych-na-krajowa-informacje-podatkowa [access: 8.12.2018].

[4] The point of departure in the identification process is ignorance as to the identity of a given person, while the verification takes place by comparing the identifier of the person with a model pre-recorded in the database. See M. Tomaszewska-Michalak, *Prawne i kryminalistyczne aspekty wykorzystania technologii biometrycznej w Polsce*, Warszawa 2015, p. 14.

[5] D. Gutowska, *Techniki identyfikacji osób z wykorzystaniem indywidualnych cech biometrycznych*, „Zeszyty Naukowe Wydziału Elektroniki i Automatyki Politechniki Gdańskiej" 2004, nr 20, p. 69.

[6] W. Gutfeter, A. Pacut, *Człowiek w systemie biometrycznym*, [in:] *Dokumenty a prawo*, red. M. Tomaszewska-Michalak, T. Tomaszewski, Warszawa 2015, p. 79.

[7] D. Gutowska, *op. cit.*, pp. 69–70.

[8] R. Kaszubski, *Społeczne i prawne aspekty biometrii. Człowiek i dokument*, Warszawa 2009, p. 3.

[9] K. Krasowski, I. Sołtyszewski, *Biometria – zarys problematyki*, „Problemy Kryminalistyki" 2006, nr 252, p. 39.

cal-physical and behavioural[10]. First, they are closely related to the human organism, which means that man has no influence on them. The category of biological-physical biometrics includes fingerprints, structure of iris, facial image, DNA. Behavioural characteristics reflect how a particular activity is performed by a specific person. These may be learned, acquired and genetically conditioned behaviours. The category of behavioural biometrics covers, among other things, lips motion, manner of walking or manner of writing one's signature[11]. Currently, the ongoing development of so-called behavioural biometrics[12], which focuses on the activities which, under the influence of frequent repetition, are subject to the individualization process.

The use of biometric solutions on a large scale resulted in public opinion's concerns about interference with the right to privacy, human dignity or the right to the protection of personal data[13]. Hence, there is a strong need for special protection of biometric data. In the previously binding legislation, there were no regulations referring directly to biometric data. Determining the conditions for admissibility and legality of biometric data processing gave rise to a number of ambiguities, especially since the legislature failed to provide the definition of biometric data and to regulate their status[14]. The Directive 95/46/EC[15] did not refer to biometric data directly. A valuable source of knowledge regarding the relationship between law and biometrics were opinions developed by Article 29 Data Protection Working Party[16]. A document prepared by the Working Party on biometrics in most cases granted to biometric data the status of personal data and pointed to the essential role played by the principle of proportionality in biometric data processing[17]. On the other hand, in the opinion of 2012, Article 29 Data Protection Working Party warned about the risk related to the processing of biometric data, especially in large centralised databases, due to the possible negative effects to persons whose data is processed. Article 29 Data Protection Working Party argued that biometric data should be identified with human biological properties and physiological and

[10] A. Krasuski, *Ochrona danych osobowych na podstawie RODO*, Warszawa 2018, p. 118.

[11] A. Bodnar, J. Michalski, *Dokument biometryczny a prawa człowieka*, [in:] *Dokumenty we współczesnym prawie*, red. E. Gruza, Warszawa 2009, pp. 52–54.

[12] B. Hołtys, *Biometria w procesie identyfikacji*, [in:] *Funkcje procesu karnego. Księga jubileuszowa Profesora Janusza Tylmana*, red. T. Grzegorczyk, Warszawa 2011, p. 702.

[13] D. Jaroszewska-Choraś, *Biometria. Aspekty prawne*, Gdańsk 2016, p. 17.

[14] Biometric data in the legislation previously in force neither was classified as sensitive data nor regular data. See A. Krasuski, *op. cit.*, p. 118.

[15] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ EU L 281 of 23 November 1995), hereinafter: Directive 95/46/EC.

[16] More on the Working Party, see https://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358 [access: 10.06.2019].

[17] Data Protection Working Party, Opinion 5/2003 of 1 August 2003, p. 9.

behavioural characteristics[18]. Despite the non-binding nature of the information contained in the guidelines developed by the Working Party, it should be noted the important role that this information played in the process of analysing the legal basis for processing biometric data[19].

The law must follow the technological development, based on current trends and directions of change. The constant development of new technologies has also forced changes in the law on the protection of personal data. It was only 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[20] which introduced the term of biometric data, unknown to the legislation applicable before 25 May 2018. According to the legal definition provided in Article 4 (14) GDPR, biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

The linguistic interpretation of the provision indicates that the EU legislature has sought to formulate the broadest possible definition of biometric data. Examples of biometric modalities are a facial image[21] and dactyloscopic data. It should also be stressed that the legislature adopted a legal definition of biometrics in line with the guidelines of the Article 29 Working Party[22]. As a result, three premises must be met to be able to refer to a specific information or set of information as "biometric data".

Firstly, this information must meet the definition of personal data referred to in Article 4 (1) GDPR. As a result, it must be the information about an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name and surname, identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

---

[18] Data Protection Working Party, Opinion 3/2012 of 27 April 2012, pp. 8–13.

[19] It should be noted that within the Polish legal system, the term "biometric data" was only used by the Act of 13 July 2006 on Passport Documents (Journal of Laws 2006, No. 143, item 1027 as amended). Pursuant to Article 2 (1) of the Act on Passport Documents, the facial image and fingerprints placed in passport documents in electronic form shall be deemed biometric data. Also, Article 18 (1) (11) of the Act on Passport Documents lists biometric data as the data contained in a passport document.

[20] OJ EU L 2016, No. 119, hereinafter: GDPR.

[21] Referring to facial image, the EU legislature, in recital 51 of the GDPR, noted that photographs, which are to be understood as media containing image, are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. See A. Krasuski, *op. cit.*, p. 128.

[22] M. Koba, *Dane biometryczne*, [in:] *RODO – ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, p. 275.

Secondly, as this definition indicates, personal data must relate to one of the characteristics relating to a particular natural person. This may be one of the physical, physiological or behavioural characteristics. Among the physical characteristics, there is a distinction between morphological and anatomical features. Morphological features are all features that are visible to the naked eye in our appearance, e.g. eye colour. The anatomical features, on the other hand, refer to our internal body structure[23].

Thirdly, biometric data must result from special technical processing. Although the legislature did not explain what technical processing was supposed to be characterised by and what it was supposed to consist in, the literature emphasises that it is to be associated with the use of technical means, with particular emphasis on ICT resources operating under appropriate software[24]. Not all information concerning physical, physiological or behavioural features of a human being will be classified as biometric data. Only those which entail special technical processing[25].

An important novelty in relation to the previously applicable legislation is the inclusion of biometric data processing in a particular category of data, commonly referred to as the so-called sensitive data[26]. Under the previously applicable legislation, the use of biometric data could only imply the use of sensitive personal data. When analysing fingerprints or biometric facial recognition, the data concerning racial or ethnic origin can be disclosed, which, in contrast to biometric data, were classified as sensitive data[27].

As was the case before, the new rules also indicate that, in principle, the processing of special categories of data is prohibited[28]. Data covered by special protection by their nature are particularly sensitive in the context of fundamental rights and freedoms, as their processing may cause interference with the fundamental rights and freedoms of an individual[29]. Sensitive data concern the most intimate spheres of human life, hence the need for their exceptional protection[30]. Biometrics, on

[23] A. Krasuski, *op. cit.*, pp. 126–127.

[24] *Ibidem*, p. 127.

[25] M. Koba, *op. cit.*, p. 275.

[26] The classification of data as ordinary and sensitive data is of particular importance in the context of the obligations of data controllers, in particular when analysing the data risk assessment and the related security of processing, the recording of activities and the mandatory appointment of a Data Protection Officer. See D. Lubasz, *Dane zwykłe i szczególne kategorie danych*, [in:] *RODO w e-commerce*, red. D. Lubasz, Warszawa 2018.

[27] D. Jaroszewska-Choraś, *op. cit.*, p. 103.

[28] A. Dmochowska, *Przetwarzanie danych szczególnej kategorii*, [in:] *Unijna reforma ochrony danych osobowych – analiza zmian*, red. A. Dmochowska, M. Zadrożny, Warszawa 2016, p. 29.

[29] P. Litwiński, P. Barta, M. Kawecki, *Zasady RODO*, [in:] *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, red. P. Litwiński, P. Barta, M. Kawecki, Warszawa 2018, p. 331.

[30] D. Jaroszewska-Choraś, *op. cit.*, p. 102.

the other hand, examines everything that makes it possible to identify individual characteristics, so it should be considered as an appropriate solution to include biometric data in a specific category by the legislature.

The list of sensitive data specified in the GDPR is of a closed nature. Pursuant to the current wording of Article 9 (1) GDPR, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited[31].

Legal scholars note that the so-called "two-fold division" between ordinary and sensitive data is artificial and flawed. It is argued that it is very likely that in specific situations the processing of certain data falling within the category of ordinary data, e.g. data on the economic or social situation, will pose a higher risk to human privacy than the processing of certain so-called sensitive data[32].

The EU legislature, despite the general prohibition on the processing of so--called sensitive data, has defined in Article 9 (2) GDPR situations where this prohibition may be lifted. This means that this data may only be processed if at least one of the conditions mentioned in the above-mentioned law provision is met. Each of these circumstances is independent and autonomous, hence the literature points to the prohibition on interpreting this provision broadly[33].

The processing of data[34] covered by special protection, including biometric data, will be allowed provided that the data subject has given a clear consent to their processing for one or more specific purposes. *A contrario*, it cannot be an "ordinary consent". The literature points out that explicit consent cannot raise any doubt about the fact that it has been granted by the data subject and will have the form of a declaration of intent. It will therefore not be sufficient to only acknowledge it[35].

Another condition allowing for personal data processing is the fact that the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and

[31] The GDPR extended the list of special categories of data. The Directive 95/46/EC failed to distinguish genetic data and biometric data in the so-called sensitive data catalogue. See P. Fajgielski, *Przetwarzanie szczególnych kategorii danych w świetle RODO*, „Informacja w Administracji Publicznej" 2017, nr 2, p. 15.

[32] P. Litwiński, P. Barta, M. Kawecki, *op. cit.*, p. 331.

[33] *Ibidem*, p. 330.

[34] Under the GDPR, the definition of data processing is very broad. According to Article 4 (2) GDPR, personal data processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

[35] P. Litwiński, P. Barta, M. Kawecki, *op. cit.*, p. 334.

social security and social protection law in so far as it is authorised by European Union or Member State law[36].

Processing of the data concerned shall also be acceptable to the extent necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent (Article 9 (2) (c) GDPR). The regulation allows the possibility of waiving the prohibition on personal data processing in the context of the need to protect the vital interests of another person, not only the data subject. This waiver may be particularly important where there is a need to protect the third party's health, for the reasons related to the health condition of the data subject, related directly to e.g. an infectious disease[37].

Another condition authorising for the processing of specific categories of data is processing carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim (Article 9 (2) (d) GDPR). An important novelty in this respect is admitting the processing of personal data not only of the current members of the said organisations but also former members thereof[38].

The processing of a particular category will also be possible if the data subject makes the data manifestly public. Therefore, the two conditions must be met combined: 1) the publication of sensitive data, e.g. fingerprints by the data subject; and 2) these data must be manifestly made public, e.g. via the media such as radio, television, press or the Internet[39].

Another condition implying the possibility of processing personal data is the need to establish, exercise or defend legal claims or the processing whenever courts are acting in their judicial capacity[40].

Another circumstance conditioning the waiver of the general prohibition of processing of so-called sensitive personal data is reasons of substantial public interest. The legislature stressed that these interests should be proportionate to the aim pursued and should respect the essence of the right to data protection[41].

The next condition set out by the legislature concerns health protection. Sensitive data, including biometric data, may be processed if it is necessary for the purposes of preventive or occupational medicine. This concerns, first of all, the situation of assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care. Sensitive data may be processed for the purposes of

[36] A. Dmochowska, *op. cit.*, p. 31.
[37] P. Litwiński, P. Barta, M. Kawecki, *op. cit.*, p. 336.
[38] P. Fajgielski, *op. cit.*, p. 16.
[39] P. Litwiński, P. Barta, M. Kawecki, *op. cit.*, p. 337.
[40] A. Dmochowska, *op. cit.*, p. 32.
[41] *Ibidem*.

treatment or the management of health or social care systems and services on the basis of European Union or Member State national law (Article 9 (2) (h) GDPR).

Processing of such data is also allowed if necessary for reasons of public interest in the area of public health. This applies in particular to the protection against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of European Union or Member State national law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

The last condition, which implies the admissibility of processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Such processing should be based on national or European Union law[42].

It would seem that the above list is very broad, which may negatively affect the importance of the general prohibition of processing personal data of a special category[43]. Consequently, it is necessary to examine with due diligence and caution as to whether, in the case of biometric data processing, we have a legal condition to waive the general prohibition of the processing of so-called sensitive data. This problem concerns especially employers, who, along with technological progress, are increasingly willing to use new solutions. A particular interest in the use of biometrics covers the possibility of confirming the presence of employees at work and securing the property of special value located within the premises of the worksite[44].

It should also be noted that the EU legislature, in Article 9 (4) GDPR, left the possibility to establish further regulations, including the regulation of further restrictions on the processing of genetic, biometric and health-related data. Owing to this, a large scope of freedom is seen in the field of creating the principles of biometric data processing[45]. Taking into account the principle of adequacy, the controller should collect only necessary data, examining whether it is possible to achieve the required goal by using other, less sensitive data[46].

The use of biometric technologies is becoming more and more popular. The reasons for the growing interest in biometric methods relate to the fact that sometimes it is very difficult to remember access passwords or PINs, while it is very easy to lose access cards. As a result, traditional identification or verification is based on what the user knows or possesses. Biometric methods are different, as they are based on who the user is and what their individual characteristics are. However,

[42] P. Litwiński, P. Barta, M. Kawecki, *op. cit.*, p. 344.

[43] D. Jaroszewska-Choraś, *op. cit.*, p. 102.

[44] L. Mucha, *RODObiometria, czyli dane biometryczne w RODO*, www.rodokompas.ostrowski-legal.net/single-post/2018/09/19/RODObiometria-czyli-dane-biometryczne-w-RODO [access: 8.12.2018].

[45] R. Lewandowski, *op. cit.*, p. 164.

[46] L. Mucha, *op. cit*.

due to the complexity of the issue of biometrics and the possibility of using it in practice, it is important to first keep in mind its impact and its effects on the fundamental human rights[47]. It seems obvious that the use of biometric techniques, both in public administration and in the private sector, will depend on the approach to security considerations[48]. On the other hand, the increase in public awareness in the context of opportunities and risks related to the security of biometric systems could result in an increase in the overall efficiency level of these systems[49].

With this in mind, it should be firmly stated that modern biometric technologies pose numerous challenges to different scientific disciplines, including in particular legal sciences. It is therefore important that legal regulations, especially those regarding the protection of personal data, follow the development of the use of biometrics. These regulations should, on the one hand, allow for wider use of biometric techniques designed primarily to improve safety, but also to provide basic standards for the storage of biometric data and their processing. An instrument to ensure the basic security standards are the regulations for biometric data provided for in the GDPR. Therefore, the EU legislature's decision should be positively assessed as regards the introduction of the legal definition of biometric data and its classification as the category that requires special protection. The definition of biometric data will facilitate the process of determining the legal bases for processing.

REFERENCES

Act of 13 July 2006 on Passport Documents (Journal of Laws 2006, No. 143, item 1027 as amended).

Biometria w bankowości i administracji publicznej, Warszawa 2009.

Boczoń W., *Biometria w bankowości. Co za jej pomocą załatwimy dziś w banku?*, www.bankier.pl/wiadomosc/Biometria-w-bankowosci-Co-za-jej-pomoca-zalatwimy-dzis-w-banku-7542743.html [access: 6.12.2018].

Bodnar A., Michalski J., *Dokument biometryczny a prawa człowieka*, [in:] *Dokumenty we współczesnym prawie*, red. E. Gruza, Warszawa 2009.

Data Protection Working Party, Opinion 5/2003 of 1 August 2003.

Data Protection Working Party, Opinion 3/2012 of 27 April 2012.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ EU L 281 of 23 November 1995).

Dmochowska A., *Przetwarzanie danych szczególnej kategorii*, [in:] *Unijna reforma ochrony danych osobowych – analiza zmian*, red. A. Dmochowska, M. Zadrożny, Warszawa 2016.

[47] D. Jaroszewska-Choraś, *op. cit.*, p. 26.

[48] Security in this meaning is defined as preventing from acquisition and free use of sensitive information by unauthorised persons. See *Biometria w bankowości i administracji publicznej*, Warszawa 2009, p. 103.

[49] W. Gutfeter, A. Pacut, *op. cit.*, p. 81.

Fajgielski P., *Przetwarzanie szczególnych kategorii danych w świetle RODO*, „Informacja w Administracji Publicznej" 2017, nr 2.
Gutfeter W., Pacut A., *Człowiek w systemie biometrycznym*, [in:] *Dokumenty a prawo*, red. M. Tomaszewska-Michalak, T. Tomaszewski, Warszawa 2015.
Gutowska D., *Techniki identyfikacji osób z wykorzystaniem indywidualnych cech biometrycznych*, „Zeszyty Naukowe Wydziału Elektroniki i Automatyki Politechniki Gdańskiej" 2004, nr 20.
Hołtys B., *Biometria w procesie identyfikacji*, [in:] *Funkcje procesu karnego. Księga jubileuszowa Profesora Janusza Tylmana*, red. T. Grzegorczyk, Warszawa 2011.
https://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358 [access: 10.06.2019].
Jaroszewska-Choraś D., *Biometria aspekty prawne*, Gdańsk 2016.
Kaszubski R., *Społeczne i prawne aspekty biometrii. Człowiek i dokument*, Warszawa 2009.
Koba M., *Dane biometryczne*, [in:] *RODO – ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018.
Krasowski K., Sołtyszewski I., *Biometria – zarys problematyki*, „Problemy Kryminalistyki" 2006, nr 252.
Krasuski A., *Ochrona danych osobowych na podstawie RODO*, Warszawa 2018.
Lewandowski R., *Biometria – nowe zastosowania*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 17.
Litwiński P., Barta P., Kawecki M., *Zasady RODO*, [in:] *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, red. P. Litwiński, P. Barta, M. Kawecki, Warszawa 2018.
Lubasz D., *Dane zwykłe i szczególne kategorie danych*, [in:] *RODO w e-commerce*, red. D. Lubasz, Warszawa 2018.
Mucha L., *RODObiometria, czyli dane biometryczne w RODO*, www.rodokompas.ostrowski-legal.net/single-post/2018/09/19/RODObiometria-czyli-dane-biometryczne-w-RODO [access: 8.12.2018].
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 (OJ EU L 2016, No. 119).
Rzecznik w sprawie rozpoznawania głosu osób dzwoniących na Krajową Informację Podatkową, www.rpo.gov.pl/pl/content/rzecznik-w-sprawie-rozpoznawania-glosu-osob-dzwoniacych-na-krajowa-informacje-podatkowa [access: 8.12.2018].
Tomaszewska-Michalak M., *Prawne i kryminalistyczne aspekty wykorzystania technologii biometrycznej w Polsce*, Warszawa 2015.

STRESZCZENIE

Celem niniejszego artykułu jest zwrócenie uwagi na możliwość wykorzystywania nowych metod służących identyfikacji i weryfikacji osób fizycznych, tj. technik biometrycznych. Współcześnie wykorzystanie biometrii staje się zjawiskiem coraz częstszym, przez co wymagane jest dostosowanie norm prawnych do aktualnych trendów. Autorka wskazuje na zmiany, jakie zaszły w kwestii ochrony danych biometrycznych w związku z wprowadzeniem RODO, zwłaszcza w kontekście uwzględnienia danych biometrycznych jako danych szczególnej kategorii.

Słowa kluczowe: biometria; ochrona danych biometrycznych; dane wrażliwe