

МІЖНАРОДНЕ ПРАВО

DOI: 10.34015/2523-4552.2023.1.03

УДК 341.1

Daria A. Bulgakova

*Doctor of Laws, Ph.D. in International
Law, Lawyer (Kryvyi Rih, Ukraine)
ORCID: 0000-0002-8640-3622*

Valentyna A. Bulgakova

*Pedagogue-Methodist of the
Highest Category, Supervisor of
scientific manuscripts
On history, sociology, and law in
Dnipropetrovsk Oblast',
Gymnasium № 91
ORCID: 0009-0009-6463-5228*

THE RECOGNITION OF THE DECEASED BIOMETRIC DATA UNDER PERSONAL NON-PROPERTY RIGHTS IN TERMS OF THE GENERAL DATA PROTECTION REGULATION

The authors of this work claim that the legislation of the European Union does not adequately protect biometric data, due to the actuality that the protection of biometric data after the death of a person is unresolved within the legal field of personal data protection. The General Data Protection Regulation (GDPR) does not apply to deceased individuals, meaning that biometric data that was processed under the GDPR during the individual's lifetime continues to be at risk of re-processing after the individual's death, meaning that businesses can potentially avoid GDPR when the person has died, and decide the fate of the deceased's biometrics at their own discretion.

Taking into account the above, the authors of the work consider it necessary to orient special legislation to overcome the specified legal gap, and since the regulation on the protection of personal data is vague to solve the problem, the research proposal of the authors consists in the application of legal guarantees not only under the GDPR but also in conformity with civil law. Therefore, the authors aim to initiate provisions for potential legislation, including the consolidation of the processing of biometric data of the deceased as part of a person's last will. The development of legal norms that would protect the biometric data of deceased persons by classifying them as non-property rights is especially recommended for countries with a civil law system.

The research paper also warns that privileges that belong to the non-property rights of an individual do not, as a rule, automatically pass to heirs. In this regard, in the absence of a person's will to decide the future fate of biometric data that is

continuously processed at the time or after death, the authors offer to allow family members and other close persons to exercise the right to the protection of personal data, such as the right to be forgotten, on behalf of the deceased, and to demand the condition of appropriate technical and organizational guarantees in the event of such performance. In this matter, according to the authors, it is expedient to conclude agreements between interested parties and family members to determine the fate of biometric data. However, in order to avoid the realization of the right to the protection of personal data, which the deceased did not have time to realize during his lifetime, and if during the life of the person Article, 9 (2, a) GDPR confirmed as the basis for the permitted biometric data processing because it is subject to the consent of the person, then following the human-centric approach of the European Union, it is proposed to design and indicate in such consent a clause where the individual could specifically determine and decide the fate of the biometric data upon death, for example, to (i) delete, (ii) transfer for the research purposes.

Consequently, the authors predict the development of legal regulation of biometric data by assigning it to the category of non-property rights. Hence, the adoption of special provisions for the protection of the deceased biometric data and ensuring the realization of the right to personal data protection is expected not only during life but also after death.

Keywords: *GDPR, biometric data processing, the right to personal data protection, human dignity, consent, personal non-property rights.*

Introduction

Historically, individuals who have passed away do not have a right to data protection, and any privacy-alike interests they had while alive are null and void after death. However, in today's world where digital acquisitions contain vast amounts of personal data including biometrics that are stored on third-party servers, the EU, state legislatures, courts, and the public demand to rethink the efficacy of posthumous data protection right. Hence, the article submits the initiative and further argument for reconsideration as follows.

There are several issues to consider when it comes to biometric data (BD) of deceased individuals. Firstly, due to the gap in information law at the European Union (EU) level, the research defines controversies in relation to the argument that deceased bio-

metric data cannot be considered personal data as a deceased person cannot be considered an individual due to incapacity. Secondly, there is a necessity for distinct protection of data about deceased individuals, but such protection is not currently provided by any specific legislation at the European Union level. However, some Member-States countries extend the protection of personal data to information about deceased persons.

For instance, European countries have practiced two approaches to restrain biometric data of the deceased. The first approach is negative that directly excludes the relationship regarding the information about the deceased due to the restricted scope of the General Data Protection Regulation (GDPR) [13] in terms of application to the deceased data. The second approach is

positive, which is followed by countries that extend legislation on personal data protection due to the not applicability of the GDPR to data of deceased persons and where Member States may provide for rules regarding the processing of personal data of deceased persons. This approach founded with reference to the GDPR Recital 27 and proposed by the authors. Accordingly, the authors confer the idea to way forward to solve the lack of norms matter concerning deceased biometric data which consult to be solved regardless the relationships with the statutory personal non-property rights, recognized by legal science, the tradition of consolidation at the level of civil law, and with respect to the GDPR model. Some countries have already established special provisions for the BDP of the deceased. For example, the Bulgarian Law on Personal Data Protection [11] stipulates that the heirs of a deceased individual have rights over their data, while the French law on the protection of individuals concerning the processing of personal data [14] gives the heirs of a deceased person the right to require the controller to update personal data relating to the deceased. The Slovenian Law on Personal Data Protection [15] is the most refined, establishing rules that permit the processing of personal data of the deceased based on the law, and allowing heirs and anyone relevant to request access to the personal data of the deceased for historical, statistical, and scientific research purposes unless the deceased had previously denied such access in writing at the lifetime. Therefore, the **study scope** is the second approach. Notable, the research is not comprehensive and excludes the contrast with the first stressed approach.

Analysis of the recent publications

The problematic theme of this research article has been developed with respect to the work of Bulgakova [3, pp. 132, 134] stating that human characteristics factors and the ultimate recognition result are precisely and overcome used in biometric systems. Since biometric data is vital information, and its processing belongs to the main types of information activities, biometrics' relationship includes a person subjected to act as an informative element because the biometric characteristic is a source taken from the human body. Thus, an individual receives the subject data status within its unique identification procedure when a person's status differs in two ways. First, since biometric processing provides unique information, the person is a mandatory participant in such legal links, without whom biometric processing outcome – unique identification – cannot occur. Secondly, a biometric data subject is endowed with personal non-property rights. Therefore, in the view of the study, biometric data processing could endow a person's credentials similar to the subject of civil ties with personality and legal capacities.

Furthermore, as per the research of Caplova et al. [5, p. 669], in principle, many of the methods that have been used and tested on the living may aid the personal identification of the deceased, hence, Kaplan [6, p. 313] points out that ethical and policy analysis should assess data uses and users, as some are more compatible with societal norms and values than others. Accordingly, Khomenko et al. [7, pp. 797, 799] come to the results that everyone has the right to respect his dignity and honor; the dignity and honor of an individ-

ual are inviolable; an individual has the right to apply to a court with a claim to protect dignity and honor. In addition, however, in the context of the analysis of judicial practice in cases on the protection of violated personal non-property rights, both parties of civil legal relations and courts do not always use all the potential rules of the current legislation. Consequently, Banta [1, p. 931] explores how digital asset accounts should be treated if an individual has not made her intentions known. In this scenario, succession principles should apply, and living family members should have a claim in controlling or accessing a decedent's digital assets.

The processing claim to deceased biometrics is an emergence for the regulation especially when the processed data is the source of commercial gain and commodification of users' identities in e-platforms [4, p. 209], and when there are already patents on apparatus for tracking deceased users' body and process system solutions. According to Francisco Ray Kingston [8], the apparatus includes a processor and at least one remote computer system adapted to read and store a unique biometric input from a deceased body. The biometric input is cataloged with a unique identifier. Prior to the cremation of a deceased body at a crematorium, the biometric input is scanned and matched to stored data to verify the identity of the deceased body. Also, according to the patent of Blan et al. [2] a personal, biometric authentication system is disclosed. The system can be used for controlling access to equipment or physical facilities. The system employs the combination of a unique, inherently specific biometric parameter recognized and compared with stored data and at least one non-specific biometric parameter of

a physiological characteristic recognized and compared with physiological norms. Positive comparison results in the authentication of an individual that is not incapacitated, dismembered, or deceased.

Methodology

The research refers to Krebs's [9, pp. 88-90] alike methodology in terms of establishing the legal facts by preventing violations of a human right to personal data protection given by birth and affecting human dignity the study seeks to minimize the risk of taking it in null after the death. Lacking compulsory jurisdiction, the fundamental goal of this mission is to persuade relevant audiences to accept findings and adopt their recommendations. The assumptions underlying these efforts are that legal fact-finding bodies are well-suited to settle disputes over 'what happened,' and by producing credible facts, their findings, and conclusions will mobilize domestic accountability measures. Hence, the authors believe that since the GDPR is out of the scope to protect deceased biometrics processed by businesses during a person's lifetime and nevertheless constantly stored and over again under the risk of processing for other purposes that initially settled just because the person is passed away which means companies could escape from the GDPR because the processing is no longer being of GDPR control. It shall not happen, therefore the system of 'checks and balances' cited in the work of Shetreet [10, p. 202] is important to guarantee the right to personal data protection including deceased biometrics. Accordingly, the authors regard that demonstrated below research reflections would be relevant to lawmakers and estimated by them.

Statement of the problem

The legal status of biometric data after a person's death is currently unresolved within the personal data protection framework. The data protection law does not contain provisions that would determine the procedure for biometric data processing of the deceased. The matter is clear, the GDPR does not apply to the deceased persons as per Recital 27. However, biometric data, including a collection of biometric information that has been processed during a person's lifetime, continues to exist in electronic or file form within biometric databases. As an individual, a person's legal capacity ceases at the moment of death. This presents a risk of potential disproportionate processing and a lack of a legal basis for such actions. To address this dilemma, the principle of proportionality is a crucial tool contributing to finding a solution to assess that the processing 'does not involve an undue intrusion into the data subject's personal integrity' [16].

Finally, the rights of the deceased related to their personal, non-property rights do not pass on to their heirs, unlike other inheritance rights linked to the testator's person. This means that the deceased's personal rights, such as the right to privacy or the right to control the use of their biometric data, do not transfer to their heirs upon their passing. This is an important distinction because many inheritance rights pass on to the heirs, such as property, assets, and intellectual property rights. However, personal rights are generally viewed as inalienable and cannot be transferred to another person, even after death. In summary, the rights of the deceased related to their personal, non-property rights are not inheritable by their heirs. This is because personal

rights are viewed as inalienable and cannot be transferred to another person, even after death. Therefore, regarding the importance of upholding human dignity in research, appropriate safeguards must be implemented under data protection laws. Since GDPR does not provide adequate provisions, a specific law at the EU level of sources must be put in place to address these concerns.

Purpose

The authors forecast that countries with civil law systems could supplement their provisions with stipulations that would protect the deceased biometric data. Therefore, the research seeks to deliver inputs for such provisions in relation to those whose biometric data is still continuously processed after the death and targets (i) to consolidate the biometric data processing (BDP) of the deceased as an auxiliary ground to realize the last 'will'; (ii) to propose in the event of lack clearness in the deceased 'will' a solution to refer to the decision about further happening with biometrics designed in the form of agreement between interested party and family members or relatives or other reasonably close people; (iii) to allow family members, relatives, and other reasonably close people to exercise personal data protection rights (alike defined in the GDPR) over such data; and (iiii) to allow the BDP of the deceased for historical, and scientific purposes with a further guarantee that proper safeguards are in place.

Research results

The GDPR Recital 27, 158, and 160 accentuate that the regulation does not apply to the data of deceased persons. This repetition highlights the importance of understanding the bounda-

ry of the legislation. To address this issue, the European Data Protection Supervisor Guidelines on Assessing the Proportionality Measures recommended being devoted. This affects assessing (i) the legitimacy of the purpose, (ii) purpose determination, (iii) balance of interests, and (iiii) limitations for parties' rights in legal relationships concerning BDP.

The legitimacy of the purpose must be considered by both the natural person and the controller or processor involved. At the same time, the GDPR prescribes that the scope of the regulation does not cover the processing of biometric data of a deceased person. Therefore, individuals must take care of the fate of their BDP during their lifetime. However, this point is controversial as it raises questions about how the legislator would view situations where a person is on the verge of death and needs help in deciding the fate of BDP clearance. Despite this, individuals must be legally aware of their BDP, not only while alive but also in preparation for its disposal after death means of giving information to relatives about the outcome of BDP after the death of a particular person. The legitimacy of BDP concerning the deceased offered for governance according to three validities: 1) BDP is prohibited; 2) BDP is allowed if the person before the death explicitly agrees to its processing after the death, taking into account all legal and technical measures to guarantee the protection of the right to personal data protection and associated consequences; 3) a person cannot rely on the protection of own BD after death but would like to contribute to the science of medicine, etc. It is important to decide in the form of notary authorization consent with one of and disagree with the two fol-

lowing left options during the lifetime since a deceased person is no longer part of legal relationships on BDP. Therefore, it is noteworthy to comprehend the constraints and responsibilities of both individuals and controllers or processors in the legal affinity of BDP.

It is important to remember the criterion of proportionality for the precise characterization of the purpose determination and the balance of interests involved especially in the context of the GDPR biometric regime. The objective of unique identification of a person is stated in Article 9 (1) as to identify a natural person uniquely but it does not set that this processing shall be appropriately focus on tagging the same person whose BD was collected. This lack of clarity allows companies to store a person's BD, including data on deceased persons, in the system with the intent to identify other individuals by technical means, for instance, to match. In such cases, a legitimate drive is not violated, as the law only states the objective of the unique identification of the natural person and not the identification of the straightforward person who provided BD for processing. Furthermore, the controller or processor will not be held responsible and could process the biometrics of the deceased over and over for achieving the legitimate objective as per the GDPR Article 9 (2). Thus, it is critical to remark that the involvement of a deceased BD in the unique identification technique of another individual raises ethical concerns and may impact the privacy rights of both parties affected. Therefore, companies should ensure that they do not process the data of the deceased without a reasonable extent.

According to GDPR Recital 42, consent to the processing of BD is man-

datory and has a higher burden of proof than other types of grounds. The legislation prohibits the processing of BD in Article 9 (1) while guaranteeing individual freedom and democratic legitimacy in Article 9 (2) subject to conditions. Therefore, it may be reasonable for fundamental rights to regulate the use of BD by, again, applying the principle of proportionality, to limit the power of controllers and processors by blocking processing and removing data from the system upon the death of the consenting individual. However, the controller or processor may not always know if a person has died, creating a dilemma desecrating fundamental rights. In Spain, heirs have the right to access and request deletion or rectification of relevant data from data controllers and processors, except in circumstances where the deceased individual or applicable law prohibits such actions. The authors present a solution to secure the rights of players entangled when parties may agree to end biometric data processing upon the death of the person, once the controller or processor is made aware of the death. This idea has already been implemented in France through the Digital Republic Act, Article 40-1, which authorizes users to establish instructions for managing their biometric data after death. The examination also advises that relatives of the deceased be informed of the situation, as in Slovakia where a close person may give consent under certain conditions.

Nevertheless, the breakdown states that there is a legal gap in the regulation of biometric data processing between the shapes of being alive and deceased, which can negatively impact the achievement of lawful purposes. It is crucial to respect the prohibition of

BDP and to carefully consider the legal and ethical implications of providing consent since by providing adequate legal protection for biometric data, the interests and wishes of individuals can be respected even after their death. After stressing the fact that the GDPR does not apply to BDP after death, the legislator has provided legal protection for a person's biometric data by enforcing a balance of interests and familiarizing the right to be forgotten. In the view of the authors, the right to be forgotten under GDPR Article 17 is particularly relevant to the studied issue. This means that a user can request the erasure and cessation of the redistribution of BD without undue delay if the BD is no longer necessary due to death, withdrawal of consent, or lack of legal grounds for processing. Data controllers are also required to inform downstream processors of such a request. The applicable technical and organizational measures for the realization of this right are crucial, and the use of a personal information management system (PIMS) can be immensely useful, especially if a person is unable to appear at the institution controlling his BD due to proximity to death. A recent case about Google's fine of 75 million Swedish kronor, approximately € 7 million, by the Swedish Data Protection Authority (SDPA) on 10 March 2020 for failing to fulfill its obligation in respect of the right to be forgotten under Article 17 GDPR shows the force of the mentioned right. The SDPA found that Google had not complied with a previous order to remove search links sufficiently and within a reasonable time and had also processed data in violation of GDPR Articles 5(1) (b) and 6. Additionally, the notice given to data subjects was misleading in a manner con-

trary to Article 5 (1) (a) GDPR. Thus, the BD of a deceased person could be prevented from overuse and reprocessing with the benefit of the actualization of the right to be forgotten - a mechanism to confirm that person's data is not compromised after death.

On the other hand, the right to be forgotten only partially applies to BD as it is not an absolute right. A user may not request the erasure of BD if the processing is still necessary under Article 17(3)(c) of the GDPR for reasons of public interest in the area of public health under points (h) and (i) of Article 9(2) as well as Article 9(3), or if there is a legitimate interest. For instance, a 2014 complaint was lodged with the Bulgarian Data Protection Authority (BDPA) by an individual who alleged that a telephone service provider had disclosed personal information from a customer file to a debt collection agency without consent, in violation of national data protection law. The BDPA conducted an investigation and discovered a clause in the contract between the complainant and the service provider that authorized the disclosure of personal data to a third party for debt collection purposes. The BDPA found that the service provider had a legitimate interest in collecting the money owed by the complainant under the contract. Therefore, the BDPA concluded [12] that the telephone service provider lawfully disclosed the complainant's personal information to the debt collector, as the revelation had two lawful grounds for processing: (a) the necessity for the performance of a contract and (b) the legitimate interest of the controller. Also, the right to erasure may not be exercised if the BD pertains to archiving purposes in the public interest, scientific or historical research

purposes, or statistical purposes. This means that the right to erasure is likely to render the achievement of the objectives of GDPR outlandish or seriously impair them. This matter is highly controversial, as it can lead to conflicts in interpretation and requires a separate argumentation, and therefore guided for further research.

Research discussion

The research proposes a back-and-forth view of the peculiarities of biometric data protection in conformity with personal non-property rights. According to the purpose provided for by civil law to assure the natural existence of an individual, the social being of an individual, and to benefit on the satisfaction of spiritual, moral, and cultural needs of individuals, the following definition of personal non-property rights is the most complete and, according to authors, reflect the essence of the evaluated phenomenon the best; because the personal non-property rights of individuals are subjective civil rights that are closely linked to an individual, belong to from birth or provided by law, have no economic content, where the object is personal non-property or other intangible benefits, aiming to shadow the natural existence, social existence of individuals, or to find the way into the fulfillment of moral, cultural, spiritual needs of individuals.

A study approximates that from the civil point of view, the right to dispose of the biometrics of a natural person who has died belongs to him or her in terms of other information. However, this wording is debatable, as unique characteristic is considered an element of the heritage, causing objections. Therefore, the national legislation of Member States shall contain a national rule on the protection of information

about the deceased regarding the GDPR, Recital 27. The research shows that in Austria, Belgium, Czech Republic, Finland, Germany, Ireland, Netherlands, Poland, Spain, and Sweden, the implemented Data Protection Act does not provide any special provisions for the protection of deceased biometrics. But, in Denmark, the biometrics of the deceased appears to be protected after ten years of a death fact. Nevertheless, in the view of the authors, the protection of deceased biometric data shall be secure and remain confidential, hence, the weakness of information law due to doubtful naïve GDPR scope regardless of its application for the deceased biometrics as it was found in the previous results section, calls to adopt provisions forward recognition of data relevantly to personal non-property rights. These rights arise at the time of death and can be specifically defined by law or established by the individual before passing away. This solution should be granted when a person expresses 'will' regardless of what to do with biometrics (previously processed in means of the GDPR Article 4 (2)) in terms of when individuals specify how their biometric data is used after passing. In cases where the deceased person has not expressed a specific 'will,' data protection laws must, concerning the dignity, shield biometrics that even once have been processed, especially by the commercial sector. The appropriate stipulations should be implemented to accomplish research initiatives such as conditions that limit businesses processing activities in terms that do not let escape from the GDPR Article 9(1) simply because the person has passed away.

Therefore, recognizing the personal non-property rights of the deceased is crucial for protecting dignity.

The development of a legal framework for categorizing biometric data as a non-property right can assure that these rights are upheld, and the data protection law shall be extended as specified above. The research idea of protecting unique data (like biometrics) after the death of its subject, and whose biometric data still continues to be under the processing techniques in biometric technologies, deserves attention from the lawmakers with overweight of the person's 'will' in the event of contradictions. Likewise, by analogy, courts shall enforce a decedent's wishes regarding the treatment of her remains even over objections from her family [1, p. 951]. For example, where a decedent had stated his desire for his body to be cremated, but his next of kin opposed the cremation, the court found that the testamentary wishes of the decedent were 'paramount to all other considerations' and, thus, enforced the cremation [ibid.].

Conclusions

This article argues that the current approach to digital asset biometric data protection after death, which lets businesses dictate the terms in commercial interests, is defective because consent-alike solutions do not allow individual choice or testamentary intent to govern the benefit of biometrics after death.

Notably, the prohibition on processing biometric data was not implemented without careful consideration from experts who were consulted during the design of the GDPR. The primary objective of this ban was to minimize problematic BDP and eliminate it and to assign users to make an informed decision about whether or not to agree with the BDP. In cases where consent is given, the user bears the sole responsibility.

ity for such an exception as per GDPR Article 9 (2, a).

A multifaceted course is vital to preach this issue. While consensuses can be useful for protecting deceased biometrics, they are not without drawbacks. To this end, the authors prospect to provide individuals with the right to express their wishes regarding the BDP after death. This **recommendation** would allow a person to stop, deny, or refuse, the processing of their data either wholly or partially. With respect to the GDPR not materiality to deceased data, the study suggests that the form of consent regardless of BDP should be designed in such a way as to include a clause that addresses the handling of the person's data after death. In the scenarios when during the lifetime of a person concerned biometrics are processed based on another exception as per GDPR Article 9 (2), and where consent was not given but biometrics was anyway undertaking on the grounds provided by law, then the further outcome with BDP shall be resolved regarding non-personal rights and appropriate 'will' of a person concerned that shall be executed after as a person passed away. It means, if individuals have not made intent for their digital assets known, the default rule should be created by state legislatures rather than private companies. This default rule should be consistent with personal data protection law. This would also boost us to go along with a human-

centric approach when an individual could participate in legal relationships and prevent further re-processing of data or processing for other purposes. the processing of their data while they are still alive.

Therefore, the law must guarantee that not-property rights principles honoring testamentary intent apply to data protection. This means that individuals should be empowered to make testamentary data protection decisions about biometrics continuously in the setting of the 'processing' (in terms alike to GDPR Article 4 (2)), and it secures that the decedent's intent concerning the fate of digital asset is esteemed based on the respect to human dignity.

Moreover, it is essential to determine who is legally responsible for notifying the biometric data processing service about a person's death or providing a means for the service to obtain such information. With the establishment of clear guidelines in this regard, people can have greater control over their biometric data not only during their lifetime but also after they pass away. At the last, the authors remind, that personal data protection laws were initially created in response to technological advancements, and as technology continues to evolve, consequently, the law must keep pace with digital advances to shield personal data protection interests consistently to death adequately protected too.

References

1. Banta, N. M. (2016). Death and privacy in the digital age. *North Carolina Law Review*, 94(3), 928–990.
2. Blan, B. L., Osten, D. W., Carim, H. M., & Arneson, M. R. (2007). *Biometric, Personal Authentication System*.

3. Bulgakova, D. (2023). Unique Human Identification under the GDPR Article 9 (1) (2). *Philosophy of Law and General Theory of Law*, 1 (2022), 130-159. <https://doi.org/10.21564/2707-7039.1.275645>
4. Bulgakova, D. (2022). The Protection of Commodified Data in E-Platforms. *Analytical and Comparative Jurisprudence*, 1 (2022), 208-212. <https://doi.org/10.24144/2788-6018.2022.01.39>
5. Caplova, Z., Obertova, Z., Gibelli, D. M., De Angelis, D., Mazzarelli, D., Sforza, C., & Cattaneo, C. (2018). Personal Identification of Deceased Persons: An Overview of the Current Methods Based on Physical Appearance. *Journal of Forensic Sciences*, 63(3), 662-671. <https://doi.org/10.1111/1556-4029.13643>
6. Kaplan, B. (2016). How Should Health Data Be Used?: Privacy, Secondary Use, and Big Data Sales. *Cambridge Quarterly of Healthcare Ethics*, 25(2), 312-329. <https://doi.org/10.1017/S0963180115000614>
7. Khomenko, M. M., Kostruba, A. V., & Kot, O. O. (2019). Protection of Non-Property Right. *Journal of Advanced Research in Law and Economics*, 10 (3(41)), 794-801.
8. Kingston, F. R. (2015). *System And Method For Creating A Unique Keepsake Representing A Deceased Body*.
9. Krebs, S. (2017). The legalization of truth in international fact-finding. *Chicago Journal of International Law*, 18 (1), 83-163.
10. Shetreet, S. (2013). The Duties of Fairness and Impartiality in Non-Judicial Justice. *Asia Pacific Law Review*, 21(2), 197-222. <https://doi.org/10.1080/10192557.2013.11788273>
11. Bulgarian Personal Data Protection Act. Available at: <https://www.moew.government.bg/bg/zakon-za-zastita-na-lichnite-danni/>
12. Bulgarian Personal Data Protection Authority. Decision on appeal No. Ж-830/21.07.2014. Available at: https://www.cdpd.bg/index.php?p=element_view&aid=1486
13. European Parliament and the Council (2016) Regulation (EU) 2016/679 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 (General Data Protection Regulation), *OJ L 119*, 1-88.
14. French Law n° 2018-493 of June 20, 2018, relating to the protection of personal data. Available at: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037085952>
15. Slovenian Law on Protection of Personal Data. Available at: <https://www.gov.si/assets/ministrstva/MP/ZVOP-2-14.8.19.pdf>
16. Swedish Act (2018:218) with supplementary provisions to the EU's data protection regulation protection, section 3. Available at: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218.

Булгакова Д. А., доктор права, доктор філософії з міжнародного права, юрист

ORCID: 0000-0002-8640-3622

Булгакова В. А., педагог-методист вищої категорії, науковий керівник дослідницьких робіт з філософії, соціології та права в Дніпропетровській області, Криворізька гімназія № 91.

ORCID: 0009-0009-6463-5228

Визнання біометричних даних померлого за особистими немайновими правами з урахуванням загального регулювання захисту даних

Автори даної роботи стверджують, що законодавство Європейського Союзу не захищає належним чином біометричні дані через те, що захист біометричних даних після смерті особи є невирішеним у рамках правового поля захисту персональних даних. Загальне Регулювання Захисту Даних (GDPR) не поширюється на померлих осіб, а отже значить, що біометричні дані, які оброблювалися в рамках GDPR за життя особи, продовжуючи зберігатися й після смерті людини піддаються ризику повторної обробки, а тому бізнес потенційно має змогу уникнути GDPR коли людина померла, та вирішувати долю біометрики померлого на власний розсуд.

Ураховуючи зазначене, автори роботи вважають за необхідне впровадити спеціальне законодавство для подолання вказаної правової прогалини, і оскільки регулювання про захист персональних даних є недостатнім для вирішення проблематики, то дослідницька пропозиція авторів полягає в застосуванні правових гарантій не лише відповідно до GDPR, а й згідно цивільного права. Тому, автори ставлять за мету ініціювати положення для потенційного законодавства, включаючи консолідацію обробки біометричних даних померлих як частину останньої волі особи. Розробка правових норм, які б захищали біометричні дані померлих осіб через віднесення до немайнових прав, особливо рекомендується для країн із системою цивільного права.

Дослідницька стаття також зауважує, що права, які належать до немайнових прав фізичної особи, як правило, не переходять автоматично до спадкоємців. У зв'язку з цим, у разі відсутності волі особи щодо вирішення питання про подальшу долю біометричних даних, які на момент та після смерті продовжують піддаватися обробці, автори пропонують надати можливість членам сім'ї та іншим близьким особам реалізувати право на захист персональних даних, як то право на забуття (the right to be forgotten), від імені померлого та висувати вимогу про надання відповідних технічних і організаційних гарантій у разі такої реалізації. У такому разі, на думку авторів, є за доцільним укладання угод між зацікавленими сторонами та членами родини для визначення долі біометричних даних. Однак, для уникнення реалізації права на захист персональних даних, яке за життя померлий не встиг реалізувати, та якщо за життя особи стаття 9 (2, а) GDPR слугувала підставою для винятку з правила про заборону обробки біометричних даних, тому що є згода особи, то з урахуванням людиноцентричної доктрини у праві Європейського Союзу, пропонується розробити спеціальний дизайн такої згоди з вио-

кремленням застереження (clause), де б особа могла конкретно визначити та вирішити долю біометричних даних у разі смерті, наприклад, як то (i) видалити, (ii) передати для дослідницьких цілей тощо.

Таким чином, автори прогнозують розвиток правового регулювання біометричних даних шляхом їх віднесення до категорії немайнових прав. Тому очікується ухвалення спеціальних положень щодо захисту біометричних даних померлих і забезпечення реалізації права на захист персональних даних не лише протягом життя, а й після смерті.

Ключові слова: *GDPR, обробка біометричних даних, право на захист персональних даних, згода, особисті немайнові права, людська гідність.*