DOI: 10.33270/01232502.94
UDC 341.1/.8

The Standpoint for the Legal Course Onward to the Protection of Deceased Biometric Data

BULGAKOVA Daria*
Ph.D. in International Law, Law School of the University of International Business and Economics (UIBE)
Beijing, People's Republic of China
ORCID: https://orcid.org/0000-0002-8640-3622;

BULGAKOVA Valentyna
Pedagogue-Methodist of the Highest Category, Supervisor of scientific manuscripts on history, sociology, and law in Dnipropetrovsk Oblast', Gymnasium No. 91
Kryvyi Rih, Ukraine
ORCID: https://orcid.org/0009-0009-6463-5228

Rather, what is shown to us is an imprint of light that requires a leap of faith for us to accept that these images depict something no one has in fact seen.
Nevertheless, if this is a theatre of devices, it is a poor form of it.
(Haldar, 2013, p. 150)

Abstract. The state of the art of technology shall plays a crucial role in promoting respect for fundamental rights, including data protection. It is important to govern individuals' personal data after their death to maintain dignity and ensure data protection as much as possible. From this perspective, the article describes the line between real-world of unique immortal characteristics, which gives eternal life, to the deceased represented in a digital form. An innovative and interdisciplinary approach with the legal reasoning applies in the research to encompasses a broader perspective, and to substantiate the theme assertion. The authors identify the problem in the General Data Protection Regulation (GDPR) that protect 'alive' biometric feature only, and, thus, escape to regulate biometric data of the deceased. It gives the possibility to business do not follow exact prohibition defined in Article 9 (1) concerning the processing of deceased biometric data since this provision disregard data after the death. While the GDPR does not apply to the personal data of deceased persons, there is a debate on whether it should. Considering this GDPR weakness, the research article seeks to propose solution through the need in a European Union (EU) law that will govern biometric data of the deceased according to the technological, philosophical, and biological grounds. Accordingly, the EU lawmakers shall take towards measures for the normative connection between 'life' data of the natural persons and biometric data of the deceased for the best personal data protection.

Keywords: individual; personality; life; dead; identification; biometrics; personal data; human dignity; General regulation of data protection; European Union.

Історія статті:
Отримано: 06.02.2023
Переглянуто: 03.04.2023
Прийнято: 01.05.2023

Рекомендоване посилання:
Bulgakova D., Bulgakova V. The Standpoint for the Legal Course Onward to the Protection of Deceased Biometric Data. *Філософські та методологічні проблеми права. 2023.* № 1 (25). С. 94–101. doi: 10.33270/01232502.94.

*Відповідальний автор

Introduction

The research considers a natural person – a legal person – the physical body, social presence, and a 'soul' of a personhood as intertwined through unique identification phenomenon. This resembles how an individual can be seen from a technological, philosophical, and biological aspects as a legally established unit in the digital area. Regardless, the research seeks to gain a deep understanding of the fundamental structures of identity within modern states by examining those complex connections.

Biometric information connects a person to alphanumerical data stored in an information technology (IT) system (FRA, Opinions Biometrics). The data ‘collection starts from birth and extends throughout the life of the holder’ (Tarchila, 2020, p. 5) when 'sensitive or private yet’ data 'relates' to nexus satisfied where the processing ‘is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, and ‘relates to the data subject’ (C-434/16, para 34) ‘because of its content, purpose or effect, is linked to a particular person’ (C-434/16, para 35). Regardless, the biometric identifier's quality is of paramount importance (FRA, Opinions Biometrics). If IT systems become interoperable, a person's biometric identifier will connect the person to the information contained in all IT systems, regardless of the quality standard according to which it was collected (FRA, Opinions Biometrics).

Given the stark differences in data profiling across differently situated social classes, and in particular the differences in profiling according to wealth, it would undoubtedly be the case that any algorithmically generated legal metric score will entail gaps in its dataset (Burk, 2021, p. 1185). The FRA research shows that European Union (EU) IT systems contain inaccurate alphanumeric data, such as names or dates of birth, due to various reasons (FRA, Opinions Biometrics). Thus, even if an individual is ‘correctly’ flagged as potentially negligent, reflexivity creates a strong likelihood that a data-matching score for negligence would tend to cement someone labelled with such a score into the category of ‘imprudent’ persons (Burk, 2021, p. 1185). On the converse, it would be rather naive to accept that new hardware will never be needed to process such data because the standard personal computer should be able to perform this task (Singh, 2013, p. 17). The requirement for sophisticated computer software for analysis opposes this notion (Singh, 2013, p. 17). Therefore, the software and, eventually, the hardware will need to be upgraded every two to three years or even more quickly, given the speed at which criminality and technology advances (Singh, 2013, p. 17). For instance, training tends to focus on the technical aspects of fingerprinting and less on treating the persons being fingerprinted (FRA, Opinions Biometrics).

Mistakes can occur when, for instance, a person’s fingerprints are mistakenly linked to another person’s alphanumeric data (FRA, Opinions Biometrics). Thus, we might, for example, expect that the individual with an unfavourable algorithmic negligence score could quickly find herself subject to higher insurance premiums (or perhaps stripped of insurance) or subject to higher civil or criminal liability for posing a social risk (Burk, 2021, p. 1185-1186). We have now established that the bias in algorithmic systems lies not so much in their fidelity or infidelity to some objective state of the world but instead in the feedback loop constituting the social shaping of algorithmic input and the corresponding shaping of social perceptions by algorithmic output (Burk, 2021, p. 1186). Therefore, if obtaining biometrics poses significant challenges that quality standards cannot meet, then alternative methods should be explored to avoid causing unnecessary stress or anxiety to the individual's unique characteristics.

Under the General Data Protection Regulation (GDPR), unique characteristics -biometric data - a special data category – are under Article 9 protection taking the course to prohibit the processing as per para 1. According to Article 52 (1) of Charter of Fundamental Rights of the EU, the authors standpoint about the interference with the right dignity and seek to the principle of proportionality application for the adequate balance of competing interests between business and a person to make sure that it does not pose any (potential) risk that outweighs the legitimate interests of individuals to data protection in the lifetime and after the death unless EU law provides specific rules for the processing deceased biometric data where, significantly, human dignity shall prevail.

Materials and methods

This article oriented to critique the GDPR weakness to provide appropriate legal protection of deceased biometric data. The authors of the work apply an innovative and interdisciplinary approach through technological, philosophical, and legal argumentation, which covers a broader perspective, going beyond the framework of traditional analytical jurisprudence.

For the purposes to protect deceased biometrics, the processing of personal data shall be carried out based on the technological and organisational measures in order to find out of overreaching unique identification. However, whether the EU law is ready to attribute deceased biometric data at first place is not clear; therefore, the authors operate reflections and submit thoughts about an issue of a clear position in the field of information law on how to protect the biometric data of a deceased person цршср the article designs to solve.

Research results

Human dignity

That is challenging with unique identification since the law cannot peer into the individual soul and plumb its piety (Byrnes, 2005, p. 1109). It means that biometric data processing links the representation of life to death and allows the spirit of the law to be communicated as living memory. It is the foundation for all fundamental rights in the Charter (FRA, Opinions Biometrics). Therefore, according to the authors view, the legal protection of biometric data is low if there is a lack of the respect for human dignity as per CFREU Article 1. Significantly, the FRA also emphasizes the importance of respecting human dignity and applying proportional determination.

In cases where fingerprinting is required, the duty to provide prints should be enforced in a reasonable amount of time. According to FRA findings, for instance, disproportionate force has been used when fingerprinting asylum seekers and migrants irregularly (FRA, Opinions Biometrics). In terms of law and law enforcement, technology has crept into the administrative side of legal practice (Singh, 2013, p. 14). Regardless, the consent shall be explicit but not implicit, and more than this approach is needed to address the risks the modern digital landscape poses. On the other hand, a person will not voluntarily give up her selfish interest (commit or remain committed) when that person is subject to the tyranny of a majority of which that person is not a part of (Fruehwald, 2010, p. 213). Furthermore, it has to be done measures to avoid fingerprinting when the authorizations have trouble in obtaining fingerprints that appear anchored quality standards. This is especially important in situations where behaviourally targeted advertising occurs in high-stress environments, as this raises the risk of an inappropriate response due to depletion or stress and undermining the individual's human dignity. Hence, the training of personnel should focus not only on the technical aspects of fingerprinting but also on treating individuals with respect and dignity during the process, and, at the same time, prioritizing the individual's privacy.

In order to mitigate the risk of interaction between machines and humans and to ensure that human dignity is respected, it is essential to consider both the risks according to the criteria of the principle of proportionality application. In the authors vision, these derived criteria from the principle examination, impose compliance conditions on behaviourally targeted processing that helps eliminate interference with dignity by addressing the sustained risk of connecting the human body to biometric technology. Since all humans are defined by the inner workings of their minds, and they share a similar genetic makeup (Fruehwald, 2010, p. 213), – the person is a desiring subject. Periodically, the subject experiences a lack-in-being (Milovanovic, 1994, p. 76). There is no escape from this lack of being; it is the price paid for the inauguration into the Symbolic Order (Milovanovic, 1994, p. 76). The subject is forever separated or castrated from the Real Order (ibid.). This lack-in-being mobilizes desire (ibid.). This suturing operation implicates all three Orders (ibid., p. 77). The Imaginary order provides certain illusions that are potential sources for filling gaps in being (manque d'etre) (ibid.). The Symbolic order provides a wealth of signifiers, or words, that can embody desire (ibid.). Finally, the Real order is implicated in the suturing process when the subject selects appropriate objects of desire and embodies them (ibid.). Consequently, the lack in recognition of being mobilizes desire, is addressed through Imaginary, Symbolic, and Real Orders: (i) the Imaginary order provides illusions that fill the gaps in being, and (ii) the Symbolic order provides words that embody desire; (iii) the Real order is implicated when the subject selects appropriate objects of desire and embodies them. In light of this philosophical context, the research emphasizes the representational evidence about legal subjectivity such as personhood.

Biometric data is defined by the GDPR Article 4 (14) as 'allowing or confirming the unique identification of a natural person' underlying the human nature. Despite its emergence through technological advancements, biometric data has established a new standard for defining personhood from legal standpoint. In this sense, personhood is not a fixed, inherent quality but rather a relational one, determined by the connections and disconnections between various data points and the technological and legal barriers that limit or enable these connections significantly effecting social dynamics, and the ideologies about identity.

Human body

There is a divergence between a human as a whole and, on the other side non-visible for eye distinct structure that makes a human differentiative from socium to a particular person. That person relies on technology for the best practice of its representation in the form of digital identity where both wax print and biometric portray are a state of a human being's existence. Likewise, personhood is recognized and realized through various modes of linkability (Hutton, 2019, p. 253) such as linkability based on the unique characteristics of a person. Modern philosophy has indeed attempts to accept the givenness and immediacy of sensible existence by approaching it through an analytical progression; it has adopted a taxonomical approach based upon the predominance of language; it has given priority, by embracing a post-Hegelian wave, to the totality of the spirit that would eventually lead to neutralisation of the (eschatological) 'subject/object' divide (Siliquini-Cinelli, 2014, p. 131). In other notes, the

research refers to biometrics in a sense of observed technology that not only reproduces a human by digitalization but also draws the life to the legality of biometric data subject. This matter interferes with a connection between the life of biometric data subject as the legal subject in relationships and the apparition of death. In this regard, the law provides a division between spirit and body, absence, and presence (Haldar, 2013, p. 136) which allowed for the spirit to capture the living subject (Haldar, 2013, p. 135). In this sense, biometric data processing retains to the idea of the imago.

The forensic apprehension of personality shifts to bio - representations due to a change in the perceived purpose of presenting evidence within social communication. Accordingly, biometric characteristics of the person are different at the time when the person is alive and when the person is dead. Part of what unique identification is addressed in legal vision as a capacity of perception and apprehension changes of the requirements for technological evidence. Indeed, for example, specific fingerprint characteristics serve a critical criterion for comparing prints and identifying any temporary modifications. It is common practice to obtain at least two images to monitor the changes within a few seconds in halo patterns. These prints are usually taken at the mechanical intervals where sweat does not occur on inactive fingers, and halos do not form on them. Therefore, the problem of distinguishing a ‘live’ biometric obtained from real carrier from non-living ones should be taken into account by layers because ‘in order to treat information as personal data, that information alone does not need to allow the data subject to be identified' (C-434/16, para 35).

Under the GDPR, Article 24, technical measures are implemented either at the level of the software or the reader. Reader-level is associated with modifying the scanning system and provides the ability to define additional parameters inherent only to 'live' biometric characteristics. This means biometrics lose its legal feature after the death, and a legitimate aim of unique identification cannot be achieved. Furthermore, the objective of identifying a deceased person through a system that utilizes a combination of biometric parameters and database matching is flawed. This is because the unique biometric characteristics of a deceased individual do not match the characteristics recorded during lifetime, rendering the identification process unreliable. Such processing can result the loss of legal identification of the deceased individual.

Hereinafter, biometrics plays a crucial role in the identity governance, and the law demands certainty in selecting appropriate questions and limitations within a given jurisdiction. At the same time, there is increasing conflict between the liberality of common law identity regimes and the demands of modern state governance within which citizens have a single identity that is stable and linkable across a range of domains (Hutton, 2019, p. 247).

The latest biometric technology provides the legal system with an unparalleled level of certainty. Prior to the advent of industrial reproduction methods, lawmakers relied on human observation and subsequent communication of technologies that were compatible with the market. In parallel, biometric digitization comes to the fore based on the scheme of biometric data when individuals seek to obtain it through the prism of human collection and processing by the controller. This rule necessitates a signifier's perception, tools for discursive reproduction, an embodiment of request, and bridging gaps-in-being. Therefore, the research spotlights the advantages of biometric technology in providing certainty in legal tag and the various turnover components, such as a combination of human perception, language, and physical requests, and overcoming barriers to effectively identify individuals through the unique identification.

Research discussion

Biometric data of the ‘alive’ and deceased person

Industry and the scientific research community can play an important role in developing technical solutions that promote respect for fundamental rights, including protecting personal data (FRA, Opinions Biometrics). They should continue to embed data protection by design and by default in the technical solutions they devise for IT systems (FRA, Opinions Biometrics). However, the state-of-the-art technology may lead to manipulation, which can be disguised through coding, and then the interpretation of data may be subjective. Considering these concerns, it is essential to contemplate the protection of naturals whose biometrics is being processed and the preservation of the processing when individuals pass away.

The characteristics of a person or a specimen are unique and have sacred descriptions of oneself. Fingerprinting may capture the digit, but a sample does not entirely represent the individual. Taken for an example a Roman history, the Populares continually asked for grants and gifts from the state and must have motivated the ‘empire’ to consider the needs of the underclass (Byrnes, 2005, p. 1049). Here, the research indicates a similarity with nowadays practice to the interpretations of Roman law in terms of legal personhood as follows. The Roman lex bestowed rights based on the wax impressions of deceased ancestors, establishing a human's existence and legal standing. These impressions are necessary to be recognized as a person with civic status. This presents a legal and

ethical challenge, especially when fusing the human material and/or sample to maintain origin and integrity. Regardless, the most marked way in which data protection may safeguard both legal person and deceased person data is through direct inclusion within the material scope of the law itself (Erdos, 2021, p. 2).

The idea of subjectivity in law is based on semiotics, which involves the condensation and displacement of meanings. From the forensic side, the research accumulates a connection between legal structures and an extra-existential realm that includes life and death. In Roman law, the legal rank of a living heir was established through the wax print of their dead ancestors. This print authors of this article see as a technological distinction between the deceased and the living features. Given the study, the existence of human beings is intricately linked to person's identification as legal subjects. Without proper documentation or legal recognition, their material, legislative, and civil status holds little weight unless it is bolstered by biometric technology. This raises questions about the separation of legal subjectivity from the biological or natural assumption of 'being' in the legal theory. However, the coalesce of biometric data to legal subjectivity inevitably overlooks the crucial nuances of the unique format and context a human to be a digital source. In this respect, the study investigates non-legal theories regarding legal personhood without recourse to a biological basis through technology. In that case, the presentation of the human being in a biometrically digitized format within the legal sphere must be evaluated in terms of how the legal subjectivity undergoes a genuine transformation. Therefore, authors propose a new legal standard of subjectivity based on a biometric representation reconciled through appropriate technology.

Hereinafter, this shift has arisen due to the gradual maturing of personal data protection management as a mass movement and functional attention given to the biometric data of deceased individuals. The push for the inclusion of data protection policies has originated from those who prioritize the core rationale of protecting the personal data of living individuals. This is because those one (such as business, research entities, etc.) distribute vital interest to 'alive' data and deceased data respectively. However, there is opposition to include these data of both (alive and deceased individual) in data protection policies, and, therefore, are with a limited protection. This attention has been spurred on by the large amounts of often shared intimate 'alive' data over the scope, and absence of a 'stop processing bottom' in the event of death.

The expansion of European data protection law, such as GDPR, provoke a controversy over whether this legal framework works for the biometric data of the deceased on the same way as it applicable to 'alive' person. Again, the formal scope of European data protection has referred throughout to either an 'individual' or a 'natural person' is a matter of interpretative dispute over many decades especially whether this inherently leads, or should lead, to the protection of data related to the deceased as well as the living one (Erdos, 2021, p. 3). Although the Court of Justice of the European Union (CJEU) has yet to rule on whether deceased person data are directly protected within primary EU data protection law, there is a shift away from seeing such data as inherently including the concept of individual or natural person data, and reflecting the need for harmonization within a directly applicable legal instrument, recitals in the GDPR now clarify that this instrument does not exist per se to 'apply to the personal data of deceased persons' (ibid.). The law remains ambiguous, especially when there is a different wording law, likewise, the GDPR Recital 27 vs. Recitals 156 and 158 have. Furthermore, the CJEU in Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen has ruled toward whether deceased data is undeviating protected by prime EU law. Indoors, there was a shift off examining such data as naively encompassed within the theory of individual or natural/ human person's data pondering the insufficiency and need for harmonization about an instantly applicable legal apparatus.

Measures for the appropriate data protection

Following the GDPR Articles 25 and 35, the conditions for the prevention of the possibility in accessing systems illegally, for example, using falsified cut-off fingers, authors initiate to be met based on the technological solution of patent biometric apparatus that can process biometric data only based on the unique characteristics of a living person. At the same time, notably, such protection methods have significant drawbacks, including the complexity and bulky nature of the required devices. In this scenario specialized technical equipment is necessary to measure biometric parameters to 'live' individuals, driving up equipment costs and complicating the recognition procedure.

Another measure is an application of a type of patent that functionally safeguards through verification about belongness of biometric characteristics to a living person, such as Amazon's feature that requires users to take selfies and perform specific actions to confirm their identity. Additional measure involves determining whether a person whose biometric data is presented for identification is captured from alive or dead person. This contrast achieves its decision through a sensor in the form of a scanner with installed a working surface of featuring electrodes system and the electrically conductive material. In this scenario,

when unique characteristics are placed on the scanner's surface, they cover the electrodes, and any changes in their electrical properties are detected by an external electrical sample connected to the external electrodes of the unique characteristics' application range. In the authors idea, the proposed innovation would incentivize companies to invest in research and promote the advancement of security systems. Essentially, in Europe, technical inventions can be protected through national patents granted by competent national authorities or European patents granted centrally. Companies are able to apply for patents and access the European Patent Register through the European Patent Office (EPO).

The authors also offer key to the problem in the event of organizational measures to enhance security and optimize the admission system. This involves simultaneously implementation of multi-biometric protection via several biometric technologies, such as fingerprints and facial recognition. Additionally, multi-form experience operates with multiple authentication methods, including biometric data and designed accessories such as smart cards.

In the view of the research, the technological measures are more effective since the Parliament and the Council have approved the legal bases for a European patent with unitary effect which is commonly referred to as the unitary patent. Besides, the package of measures to implement the unitary patent has been confirmed by the CJEU advocating about sufficient prevention divergences in patent protection among participating Member States and provides uniform resolution with respect to the Article 118 Treaty on the Functioning of the EU (C-146/13, para 51). Furthermore, as per Regulation (EU) No 1257/2012 Article 3(2), the regime coexisting with the EU patent system confirms a harmonized approach given the uniform enactment. Therefore, the research suggests for business to improve biometric inventions across through a single patent with reference to the Unified Patent Court because is the venue for legal disputes.

Conclusions

As information advances and its capabilities change, the line between the human body, technology, and the law becomes increasingly blurred. The differentiation of 'alive' and biometric data is challenging since the technological solutions need legally established aspects because the human body's capabilities are vastly unique; therefore, the expectation from the technological point of view is that innovations would do the best protection of data to prevent business overprocess and reprocess biometric after the death of individuals. At the same time, nevertheless of the fact that GDPR is out of the protection of the deceased biometric data, the legal anticipation relates to the strength of the technology-neutral regulation framework in the EU to eliminate risk of illegal use deceased biometric data, especially by business players, stressing the respect to human dignity. It is relevant especially under exceptions where unique identification could be permitted.

At the same time, it is recommended no to rely solely on the transparency because, in algorithms context, such approach could potentially result compromised scoring of people resulting exploit of the result of the desired protection. Hereinafter, biometric data processing may be regarded as inaccurate or biased due to the subject's intentional manipulation of data inputs. A scholar Hutton (2019, p. 253) concludes about a puzzle about the number or other identifier are linked to, that is, the precise entity that is identified. The explanation is the individual - physical body - so the identity in this basic sense is the linkage between a body and required (digital) registration regime. It would be odd to say that someone's body possessed a particular status, such as citizenship or being married. Citizenship does not reside in the body or the 'bare life' (Agamben, 1998); it is an expression of legal personality. The body itself may also be used as a part of the registration regime, for instance, in biometric forms to discern, such as eye-scans, DNA, fingerprints, etc. On the other hand, if the body is the entity that is to be referenced within a registration regime, then it does not make sense to say that such characteristics as DNA serve to identify a body because that would be the body identifying itself. Thus, the body is technologically integrated into a wider identity scheme and the biometric determination is the complexities of using identifiers to corelate an individual to a registration regime. Indeed, the body itself may be used as part of the tag process, but it is not the sole entity that is identified. Consequently, a human body and technological integration play an important role in identity schemes. And, therefore, taking into consideration broad range strategies of Member States to extent digital recognition, and weakness of GDPR application to deceased biometric data, authors advice to develop regulation in digital terms of identity and its unique identifiers protection after the death.

References

[1] Agamben, G. (1998). *Homo sacer: sovereign power and bare life*. Stanford University Press.
[2] Burk, D.L. (2021). Algorithmic Legal Metrics. *Notre Dame Law Review*, 96(3), 1147. Retrieved from https://scholarship.law.nd.edu/ndlr/vol96/iss3/6.
[3] Byrnes, W.H. (2005). Ancient Roman munificence: the development of the practice and law of charity. *Rutgers Law Review*, 57(3), 1043. Retrieved from https://ssrn.com/abstract=2314731.
[4] CJEU, Judgment of the Court (Grand Chamber), Case C-146/13, Kingdom of Spain v European Parliament and Council of the European Union, ECLI:EU:C:2015:298, 5 May 2015. Retrieved from https://curia.europa.eu/juris/document/document.jsf?text=&docid=164092&doclang=EN.
[5] CJEU, Judgment of the Court (Grand Chamber), Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen, ECLI:EU:C:2010:662, 9 November 2010. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62009CJ0092.
[6] CJEU, Judgment of the Court (Second Chamber), Case C-434/16, Peter Nowak v Data Protection Commissioner, ECLI:EU:C:2017:994, 20 December 2017. Retrieved from https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62016CJ0434.
[7] Erdos, D. (2021). Dead ringers? Legal persons and the deceased in European data protection law. *Computer Law and Security Report*, 40, 105495. doi: https://doi.org/10.1016/j.clsr.2020.105495.
[8] European Union Agency for Fundamental Rights (FRA), Opinions Biometrics. Retrieved from https://fra.europa.eu/en/content/fra-opinions-biometrics (last visited 18 March 2023).
[9] Fruehwald, E. (2010). A biological basis of rights. *Southern California Interdisciplinary Law Journal,* 19(2), 195-235. Retrieved from https://gould.usc.edu/why/students/orgs/ilj/assets/docs/19-2%20Fruehwald.pdf.
[10] Haldar, P. (2013). Forensic Representations of Identity: The Imago, the X-Ray and the Evidential Image. *Law and Humanities,* 7(2), 129-150. doi: https://doi.org/10.5235/17521483.7.2.129.
[11] Hutton, C. (2019). Linkability, Personhood and State Modernity: Understanding the Affordances of Personal Identity across Different Legal Regimes. *Law and Literature,* 31(2), 239-257. doi: https://doi.org/10.1080/1535685X.2018.1530840.
[12] Kayuni, S.W. (2016). Quis Custodiet Ipsos Custodes (Who is Guarding the Guardians)? - Decision Processes in the ICC's Offences Against the Administration of Justice. *The Law and Practice of International Courts and Tribunals,* 15(2), 345-384. doi: https://doi.org/10.1163/15718034-12341326.
[13] Milovanovic, D. (1994). The postmodernist turn: Lacan, psychoanalytic semiotics, and the construction of subjectivity in law. *Emory International Law Review,* 8(1), 67-98. Retrieved from https://heinonline.org/HOL/LandingPage?handle=hein.journals/emint8&div=9&id=&page=.
[14] 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 (General Data Protection Regulation), OJ L 119, 1-88 (4 May 2016).
[15] Regulation (EU) No 1257/2012 of the European Parliament and of the Council of 17 December 2012 implementing enhanced cooperation in creating unitary patent protection, OJ L 361 (31 December 2012).
[16] Siliquini-Cinelli, L. (2014). Imago veritas falsa : for a (post-) Schmittian decisionist theory of law, legal reasoning, and judging. *Australian Journal of Legal Philosophy,* 39(39), 118-141.
[17] Singh, C. (2013). Quis custodiet ipsos custodes? Should Justice Beware: A Review of Voice Identification Evidence in Light of Advances in Biometric Voice Identification Technology. *International Commentary on Evidence,* 11(1), 1-28. doi: https://doi.org/10.1515/ice-2014-0009.
[18] Tarchila, P. (2020). Respect for the Honor, Privacy, and Dignity of the Human Person*, Agora International Journal of Juridicial Sciences*, 1(34). Retrieved form 329082419.pdf (core.ac.uk).
[19] The Article 29 (A29), Opinion 4/2007 on the concept of personal data, 01248/07/ENWP 136.

Концептуальні погляди щодо правового курсу на захист біометричних даних померлих

БУЛГАКОВА Дар'я
доктор філософії з міжнародного права, факультет права Університету міжнародного бізнесу та економіки (UIBE)
м. Пекін, Китайська Народна Республіка
ORCID: https://orcid.org/0000-0002-8640-3622;

БУЛГАКОВА Валентина
педагог-методист вищої категорії, науковий керівник дослідницьких робіт з філософії, соціології та права в Дніпропетровській області, Криворізька гімназія № 91
м. Кривий Ріг, Україна
ORCID: https://orcid.org/0009-0009-6463-5228

Анотація. Дослідження спрямоване на побудову правової моделі для регулювання даних померлого з метою збереження людської гідності та забезпечення максимального захисту даних як за життя, так і після смерті людини. Ураховуючи те, що дія Загального регламенту захисту даних (GDPR) не поширюється на захист даних померлого, автори наголошують на проблемі щодо захисту біометричних характеристик, стверджуючи, що вказаний правовий дефіцит дає можливість бізнесу не дотримуватися чіткої заборони обробки біометричних даних, визначеної в статті 9 (1) GDPR, оскільки це положення ігнорує захист унікальних характеристик після смерті людини, адже догма заборони в обробці біометричних даних померлого відсутня. На думку авторів, це дозволяє бізнесу обробляти біометричні характеристики без конкретних обмежень. У статті окреслено правову модель шляхом виокремлення підстав для захисту, з огляду на інтерпретацію пов'язаних ризиків у контексті техно-біології та права. В інформаційному контексті таке рішення залежить від адаптованих систем сучасного рівня технологій, які з правового огляду повинні також ураховувати повагу до людської гідності. Однак існує занепокоєння щодо легкої доступності біометрії та суб'єктивного тлумачення даних, яке спричиняє дискусію з приводу того, чи слід взагалі диференціювати захист біометрики в контексті даних живої та померлої особи. Автори цієї роботи доходять висновків, що використання біометричних технологій є наслідком неоднозначності в праві Європейського Союзу. Доведено потребу в узгодженні юридичної суб'єктивності на підставі філософських тлумачень про існування людини, упровадження спеціальних технологічних засобів, які здатні підтвердити належність даних до померлої чи живої особи, що забезпечить мінімізацію ризиків у використанні унікальних даних

Ключові слова: фізична особа; особистість; життя; померлий; ідентифікація; біометрика; персональні дані; людська гідність; Загальний регламент захисту даних; Європейський Союз