Research article
UDC 34:004:341:57.087.1:316.642.4
EDN: https://elibrary.ru/joupzt
DOI: https://doi.org/10.21202/jdtl.2025.5

Behavioral Biometrics in the European Union: Legal Challenges and Technological Prospects

Baurzhan Rakhmetov
M. Narikbayev KAZGUU University, Astana, Kazakhstan

Kazbek Khaizabekov
University of Padova, Padova, Italy

Keywords

artificial intelligence,
behavioral biometrics,
data protection,
digital technologies,
European Union,
facial recognition,
law,
legal regulation,
legislation,
privacy

Abstract

Objective: to study the historical development of the European Union legislation on behavioral biometrics; to identify the features of the European approach to the regulation of behavioral biometrics, to assess its advantages and disadvantages.

Methods: general scientific methods of analysis and comparison, with an emphasis on the study of legal texts such as directives, regulations and conventions. To ensure a comprehensive understanding of the issue, the authors also consider the technical aspects of behavioral biometrics, which allows for a comprehensive analysis of both legal norms and the technological processes underlying them.

Results: the research demonstrates that the European Union regulatory legal framework on biometrics does not clearly distinguish between behavioral and physical biometrics technologies. This leads to ambiguity in understanding the risks and opportunities associated with the use of behavioral biometrics. The authors emphasize that the insufficiently specific legislation creates significant difficulties for regulators, technology developers, and end users.

Scientific novelty: the article is the first comprehensive study of the historical development of European Union legislation on behavioral biometrics. The work reveals the key characteristics of the European

✉ Corresponding author

approach, its strengths and weaknesses, and compares it with the United States' regulatory practice. The study reveals the key aspects that require further regulation: from a clear definition of behavioral biometrics to the development of comprehensive mechanisms to ensure transparency and accountability in the use of these technologies. Given that behavioral biometrics is a relatively new and rapidly developing technology, the research is important for understanding current challenges and prospects for its regulation.

Practical significance: the research is multifaceted and relevant for experts in digital technologies: legal scholars, law enforcement officers, legislators, and developers of artificial intelligence and biometrics technologies.

For citation

Rakhmetov, B., & Khaizabekov, K. (2025). Behavioral Biometrics in the European Union: Legal Challenges and Technological Prospects. *Journal of Digital Technologies and Law, 3*(1), 108–124. https://doi.org/10.21202/jdtl.2025.5

Contents

Introduction

The regulation of behavioral biometrics in the European Union (EU) highlights the importance of addressing data protection and privacy amid a rapidly evolving technological landscape. Biometrics, which includes physical, physiological, and behavioral characteristics used to identify individuals, has been receiving more attention as privacy concerns grow around the world. The EU has continuously updated its legislation to protect personal data since the adoption of the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). Key documents such as the Directive 95/46/EC and the General Data Protection Regulation (GDPR) have helped the EU set a global benchmark for the protection of personal data, particularly in the sensitive area of biometric data. Recent developments in the form of the 2024

European Union Artificial Intelligence Act (EU AI Act) have further expanded the scope of these regulations, particularly regarding the use of behavioral biometrics and artificial intelligence in sensitive areas such as security and privacy.

Despite these advances, the regulation of behavioral biometrics presents various challenges, especially concerning the distinctions between physical and behavioral data. The EU's approach to regulating biometric data has significantly influenced privacy laws globally, yet it has faced criticism for its lack of clarity and specificity in certain areas. This article examines the evolution of EU regulations on behavioral biometrics, analyzing key legislation, its influence on data protection, and existing challenges. It also compares the EU regulatory approach with the United States, where the lack of a national law has resulted in less comprehensive regulation on biometrics.

1. Evolution of Behavioral Biometrics Regulation in the European Union

To get a more comprehensive picture of how biometrics are regulated in the EU, it is essential to understand the context and conditions that contributed to the emergence and implementation of its legal framework (Carrigan & Coglianese, 2011). With the rapid advances in electronic data processing in the 1960s and 1970s, there was a severe necessity to strengthen privacy protection measures, especially in the automatic collection of personal data. This was echoed in the EU and led to the adoption of the Convention 108 and the Directive 95/46/EC (De Hert, 2013). These documents were the first legally binding international normative acts regulating data protection, including biometric data.

Convention 108, signed on January 28, 1981, obliged EU countries to introduce a series of specific changes in their domestic legislation by principles such as fair and lawful collection and automatic processing of data and the presence of concrete, explicit, and legitimate purposes for storing such data; it is not allowed to use data that is inconsistent with these objectives or where the storage process takes more time than needed. These principles also encompass the adequacy, relevance, and not excessiveness of the data. Generally, it is the responsibility of controllers, under the provisions of Convention 108, to manage the processing of personal data[1].

There is now in force a modernized version of the document, known as Convention 108+, Article 6 of which stipulates that the processing of biometric data for personal identification is permitted as long as appropriate guarantees are in place to guard against risks that endanger the individual's interests, rights, and fundamental freedoms, including the risk of discrimination. At the same time, biometric data used for unambiguous identification belong to the category of sensitive data, therefore their processing must

[1] Convention 108 and Protocols: Background. (n.d.). Council of Europe Portal. https://clck.ru/3Ge8xN

be accompanied by specific guarantees. It requires separate or joint consent of the data subject, a law defining the objectives, methods, and specific conditions under which data processing may be utilized, confidentiality, measures based on risk analysis, and security precautions[2].

Directive 95/46/EC, adopted on October 24, 1995, was also an important document in the regulation of biometrics that cannot be omitted. The primary focus was on the safeguarding of the individual's fundamental rights and freedoms during the processing of data within the EU and the free movement of such data. The key responsibility for data protection rested with the supervisory authorities established by each state that adopted Directive 95/46/EC. These are independent bodies that have the power to advise on administrative measures and regulations as well as to initiate legal proceedings if breaches of data protection requirements are found. Although Directive 95/46/EC does not specifically mention the processing of biometric data, Article 29 established a Working Party to provide consultations and opinions on the operation and regulation of biometrics[3]. For example, in 2003, a "Working Document on Biometrics," which examines how the provisions of Directive 95/46/EC apply to the use of biometric technologies, was issued[4]. In 2012, the Working Party also published an opinion on revised guidelines on principles and recommendations for enhancing privacy and data protection in biometric applications[5].

Notwithstanding, today, Directive 95/46/EC is considered no longer in force due to its replacement by the General Data Protection Regulation (GDPR), which has ushered in a new stage of development in the regulation of personal data. GDPR was adopted in 2016 and entered into force in 2018. GDPR, as well as Directive 95/94/EC, applies to all countries in the EU but does not require them to change their domestic laws. All organizations both inside and outside the EU must comply with the GDPR. Meanwhile, the GDPR requires organizations based outside the EU, which provide goods or services that track the behavior and process and store data of EU citizens, to identify their representatives in the EU. In turn, controllers and processors also have certain obligations. Controllers should always remember to follow the steps necessary for effective data protection; they should only process data that is within the scope of their duties and not allow access to it to anyone other than those who are obliged to process it (Nguyen, 2018).

2 Convention 108 +. (2018). Council of Europe. https://clck.ru/3Ge94r

3 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. (1995). Official Journal of the European Union. https://clck.ru/3Ge97y

4 Working Document on Biometrics. (2003). The Working Party. https://clck.ru/3Ge9AL

5 Opinion on Developments in Biometric Technologies. (2012). The Working Party. https://clck.ru/3Ge9D4

In the parlance of regulators, the term biometric data first appeared with the introduction of GDPR. Article 4 characterizes biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person"[6]. It is worth noting that the GDPR foresees a category of special data requiring a higher level of protection, which also comprises biometric data. In accordance with Article 9, the processing of biometric data – the objective of which is to determine identity, health, or sexual life and orientation – is strictly prohibited, except under certain conditions. For example, the explicit consent of the subject allows for circumventing the above prohibition[7] (Meden et al., 2021).

Finally, the EU AI Act, adopted in March 2024, is the most recent and highly relevant regulation to date that also applies to biometrics. Nowadays, AI has a tremendous impact on the advancement of biometrics technologies. In combination with biometrics, AI systems contribute to reducing human error and accelerating decision making (Rawat et al., 2023). Therefore, the EU AI Act incorporates several key considerations designed to regulate biometrics, including behavioral biometrics. Notably, this document covers the following aspects related to biometrics: biometric data, emotion recognition system, biometric categorization system, remote biometric identification system, real-time remote biometric identification system, and post-remote biometric identification system[8]. Among all of them, emotion recognition systems and real-time remote biometric identification systems refer to behavioral biometrics (Xefteris et al., 2016; Alsaadi, 2021; Revett, 2008). For example, an emotion recognition system aims to process characteristics such as gaze tracking, mood, facial movement and expression, gait, and heartbeat. In this regard, the EU AI Act imposes a ban on the use of emotion recognition technologies in the workplace and schools, on predictive policing if it is based on human profiling and personal characteristics assessment, and on AI that involves manipulation of people's behavior or vulnerabilities. As for real-time remote biometric identification systems, this technology can be used subject to strict safeguards and limitations[9].

---

6 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). (2016). Official Journal of the European Union. https://clck.ru/3Ge9Gn

7 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). (2016). Official Journal of the European Union. https://clck.ru/3Ge9Gn

8 Santalu, N. (2023). Biometrics Under the EU AI Act. The International Association of Privacy Professionals. https://clck.ru/3Ge9Jz

9 Holistic AI Team. (2024). Prohibited AI Practices Under the EU AI Act. https://clck.ru/3Ge9Lf

2. Specific Features of Behavioral Biometrics Regulation in the European Union

2.1. Characteristics of the European Union's Approach to Behavioral Biometrics Regulation

The approach that characterizes the regulation of biometrics in the EU can be considered as risk-oriented. Behavioral biometrics legislation is accompanied by strong restrictive measures intended to protect privacy and civil liberties and to combat bias and discriminatory technologies. Collecting, processing, and storing behavioral data is a riskier process, especially in comparison with other types of personal data (Rezaee, 2025). The point is that the accuracy of analyzing such data does not allow to fully determine a person's identity but only reveals specific patterns related to his or her character and habits. It is important to consider that factors such as high stress levels or physical condition do not make it possible for behavioral biometrics to accurately capture a person's behavior. In turn, more accurate profiling of characteristic behavior requires the collection of a significant amount of behavioral data. Furthermore, since behavioral data collection is always ongoing, it necessitates the storage of significant amounts of such information, which also poses additional risks to data privacy[10] (Sharma & Elmiligi, 2022).

Behavioral biometrics are a relatively emerging technology that is actively gaining momentum today but still accompanied by certain challenges and risks. To mitigate them, the GDPR makes it compulsory to obtain data subjects' consent to the handling and gathering of their biometric data, including behavioral ones. Previously, the GDPR had already classified biometric data as sensitive. However, the recently passed EU AI Act has expanded the categorization system by adding risk levels such as unacceptable risk, high risk, limited risk, low or minimal risk. To determine the level of risk, it is essential to ascertain the nature and the extent of AI application (Arcila, 2024). The category of unacceptable risk that prohibits use includes AI systems that imply social scoring based on behavior or personal traits and manipulation of people's behavior or vulnerabilities. The use of real-time remote biometric identification is also not allowed, unless this technology can contribute to locating missing individuals, preventing life-threatening situations, including a foreseeable terrorist attack, and identifying criminal suspects. The emotion recognition system falls into the limited risk category, but its application is not allowed in educational institutions or the workplace except for medical or safety reasons[11].

---

[10] Makhani, F. (2022). Beyond Fingerprints: Exploring Behavioral Biometrics For Secure Identity Verification. VikingCloud. https://clck.ru/3Ge9SS

[11] High-Level Summary of the AI Act. (2024). Future of Life Institute. https://clck.ru/3Ge9UK

2.2. Advantages and Disadvantages of the European Union's Approach to Behavioral Biometrics Regulation

One of the advantages of the EU's approach is that its regulatory experience has significantly influenced other countries that are creating and developing their own data protection and biometrics legislation. Greenleaf (2012) examined 39 countries outside Europe and found that there was a wide range of specific similarities with Convention 108 in the legislation of 33 countries. Some of the reasons for this phenomenon include the fact that countries are thereby demonstrating their commitment to become part of European privacy laws. Overall, Argentina, Cabo Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia, and Uruguay decided to accede to Convention 108[12].

Convention 108+, which replaced Convention 108 in 2018, has also succeeded in becoming an influential benchmark in global data protection regulation practices. In addition to EU member states, the updated protocol was signed by the United Kingdom (then a member of the EU), Uruguay, Cabo Verde, Mauritius, Mexico, Senegal, and Tunisia. Furthermore, Argentina, Burkina Faso, and Morocco were also welcomed to the Convention 108+[13]. Nonetheless, it is the GDPR that has served as the primary benchmark for data protection regulation around the world. As of 2020, countries such as Brazil, Canada, and South Korea have enacted laws similar to the GDPR (Chen et al., 2022). Many African countries including Tanzania, Eswatini, Rwanda, Uganda, and Nigeria have established several new data protection regulations that contain common principles with the GDPR[14]. It is worth noting that not only countries but also organizations around the world have been impacted by GDPR requirements. Since the European regulation mandates strict data protection safeguards, organizations whose activities extend to European citizens have had to make significant changes to comply with GDPR (Li et al., 2019; Chen et al., 2022).

The EU's approach to regulating biometrics, including behavioral biometrics, is distinguished by a robust degree of data protection and privacy. According to Article 9 of the GDPR, biometric data is classified as sensitive data requiring special protection and privacy requirements. This implies that, in general, the processing of such data is only permitted under strict compliance with certain conditions. For instance, it is imperative to acquire the explicit consent of the data subject – the individual whose data is being utilized. Furthermore, the GDPR has given data subjects the right to examine information held by organizations, and to withdraw consent for data collected by organizations. The obligations of an organization collecting and processing data from European citizens include expressing an interest in collecting personal information, justifying the reason

12 Chart of Signatures and Ratifications of Treaty 108. (n.d.). Council of Europe. https://clck.ru/3Ge9a5

13 Baker, J. (2018). What Does the Newly Signed 'Convention 108+' Mean for UK Adequacy? The International Association of Privacy Professionals. https://clck.ru/3Ge9ch

14 Wu, J., & Hayward, M. (2023). International Impact of the GDPR Felt Five Years on. Pinsent Masons. https://clck.ru/3Ge9gi

to possess this information, and presenting their identity to data subjects. Overall, the GDPR requires organizations to limit data processing, as well as possession and transfer of data between platforms, providing appropriate means of protecting and disposing of data after a set period. It is becoming clear that the GDPR approach can be considered user-centered, which has a positive effect on individual responsibility, reducing security risks and increasing privacy measures (Aseri, 2020).

There are severe sanctions for violating the above biometric data policies. Generally, there are two levels of administrative fines for non-compliance with the GDPR: 1) up to 10 million euros or 2 % of annual global turnover, whichever is greater; 2) up to 20 million euros or 4 % of annual global turnover, whichever is greater. The amount of the fine is determined depending on the specific provisions of the GDPR; it will be less if data security is breached and more if people's privacy rights are violated. For example, under the application of the GDPR, Meta[15] was fined €1.2 billion by the Irish Data Protection Commission in 2023 for sending European users' personal information to the US without proper data protection mechanisms. Before that, companies such as Amazon, TikTok, WhatsApp, Google, and others were also sanctioned[16].

The most significant drawback of the European approach is the failure to categorize and be specific in some aspects. In particular, European regulators do not consider the point that different types of biometrics use different types of data; only behavioral biometrics collects data such as keystroke dynamics, mouse movements, touchscreen inputs, eye movements, gesture, and gait (Eberz et al., 2017; Cheung & Vhaduri, 2020). Instead, the European legal framework contains only generic interpretations and guidelines pertaining to physical, psychological, and behavioral features. This shortcoming can be traced both in the past, meaning Convention 108 and Directive 95/46/EC, and up to the present, referring to Convention 108+, GDPR, and EU AI Act. The fact is that the dynamic nature of behavioral data, which does not allow it to be forecasted, modeled, or fabricated as easily, makes it non-adaptable and unsuitable for current EU regulations that cover only physical biometrics. Companies and financial institutions located in the EU, which have already started a consistent implementation of behavioral biometrics, are still guided by regulations for collecting people's physical data[17] (Kindt, 2018).

The problem of vagueness is also evident in other important provisions of regulations concerning the use of biometrics. For example, the GDPR does not make a significant distinction between the primary comparative functions of biometric technologies, specifically between 'verification' and 'identification.' Verification involves the use

[15] The organization is recognized as extremist, its functioning is prohibited in the territory of the Russian Federation.

[16] 20 Biggest GDPR Fines So Far. (2024). Data Privacy Manager. https://clck.ru/3Ge9me

[17] Özal, M. (2020). 'Behavioral Biometrics': A Brief Introduction from the Perspective of Data Protection Law. CiTiP Blog. https://clck.ru/3Ge9pA

of biometric data on a one-to-one (1:1) basis, while 'identification' involves a one-to-many (1:n) basis. It is worth noting that, according to the Council of Europe and national data protection supervisory authorities, the verification function is more secure than the identification method because it does not involve a database. In contrast, the use of biometric identification requires extensive collection and storage of biometric information in databases. Also, it should be noted that biometric identification introduces further risks due to probability-based matching, which adversely affects the level of accuracy. Accordingly, European regulators should objectively consider the relative risks of both verification and identification while introducing appropriate rules for the application of the two main functions of biometric technologies[18].

3. Comparative Analysis of the European Union's Approach to Regulating Behavioral Biometrics and the US Experience

To better comprehend the regulatory landscape for behavioral biometrics in the EU, it may be useful to examine the experience of the United States and compare it with the EU's approach. Most notably, the United States differs from the EU in the way that, instead of unified national legislation as in the EU, biometrics are regulated at the state level[19].

Numerous states, including Illinois, Texas, and Arkansas, have various laws aimed at regulating biometrics and biometric data. To begin with, it is worth noting Illinois, which introduced the Biometric Information Privacy Act (BIPA) in 2008, becoming the very first state to start regulating the collection, use, and storage of biometric data. Under BIPA, companies are obliged to acquire written consent from data subjects prior to collecting their biometric information and to limit scanning methods such as retinal or iris scanning, fingerprinting, voiceprints, or facial and hand geometry scanning. In other words, other biological and behavioral data are not considered biometric identifiers under this law (Illman, 2017). Texas provides similar definitions of biometric identifiers related to biometrics in its 2009 law under Section 503.001[20].

The State of Arkansas has enacted the Biometric Data Act, which focuses solely on biological parameters, thereby excluding behavioral data. This regulation defines biometric data as information about a person's biological characteristics, such as fingerprints, facial or eye scans, DNA, and other unique biological features utilized for identification purposes[21].

---

18 Kindt, E. (2020). A First Attempt at Regulating Biometric Data in the European Union. AI Now Institute. https://clck.ru/3Ge9ti

19 Biometric Data Protection (Privacy – EU, UK and US). (2021). https://clck.ru/3Ge9w2

20 2023 Texas Statutes Business and Commerce Code. https://clck.ru/3GePrv

21 Arkansas Personal Information Protection Act. https://clck.ru/3GeRBo

Among the various interpretations of biometric data in different United States laws, the California Consumer Privacy Act (CCPA) of 2018 notably broadens the understanding of biometric data. Under the CCPA, biometric information comprises "physiological, biological, or behavioral characteristics of an individual, including DNA, that can be used alone or in combination with other data to establish individual identity."[22] This encompasses not only traditional biometric identifiers but also behavioral patterns such as keystrokes, gait rhythms, sleep habits, health, or exercise data that can identify a person[23]. Distinctively, under the CCPA, citizens of the State have greater visibility and control over their biometric data, including the rights to general disclosure, requests for information, deletion of information, and "equal service and prices" (Ghelardi, 2020).

Additionally, The American Privacy Rights Act of 2024, successor to the American Data Privacy and Protection Act of 2021, aims to establish clear national data rights and protections. The legislation was introduced by lawmakers in both the House and Senate in April 2024, and was approved by the Subcommittee on Data, Innovation and Commerce a month later. Now, it will have to pass through a full committee and both houses of Congress prior to potentially gaining enactment into law. This legislation defines biometric information as data derived from the technological processing of unique biological, physical, or physiological characteristics, including fingerprints, facial scans, and gait, among others. Importantly, the bill was modeled on the GDPR operating within the EU[24].

In comparison with the EU legislation, the American one is less elaborated. Laws are not adopted at the federal level, but at the state level, which indicates the need for a more comprehensive approach (Neace, 2020). It also becomes apparent that these regulations, like those in the EU, do not clearly distinguish between physical and behavioral biometrics. While some laws mention behavioral characteristics, there is still no explicit legislative definition or regulation of behavioral biometrics within these frameworks. Consequently, issues related to behavioral biometrics remain inadequately addressed, requiring further legislative attention and development. Moreover, the need to focus closely on behavioral biometrics, including characteristics such as hand movements and gaze direction, has been clearly articulated by the executive branch under President Joe Biden's Executive Order on Artificial Intelligence[25].

---

22 California Consumer Privacy Act. https://clck.ru/3GeRFp

23 What is the California Consumer Privacy Act (CCPA)? (2024). TermsFeed. https://clck.ru/3GeAJh

24 Wright, V. (2024). The American Privacy Rights Act (APRA): Everything You Need to Know. BigID. https://clck.ru/3GeALE ; Pınarbaşı, A. T. (2024). The American Privacy Rights Act (APRA): Everything You Need to Know. Didomi. https://clck.ru/3GeANc

25 Brunetti, F. (2024). Behavioral Characteristics as a Biometric: Something to Keep an Eye (Scan) on. The International Association of Privacy Professionals. https://clck.ru/3GeATg

Conclusions

To sum up, the regulation of behavioral biometrics within the EU has evolved significantly, shaped by key legislative frameworks such as Convention 108, Directive 95/46/EC, and most recently the 2018 General Data Protection Regulation and the 2024 EU AI Act. These regulations have established a solid foundation for protecting personal data, especially biometric data categorized as sensitive information. The introduction of the GDPR's definition of biometric data and its strict rules for processing has set a global standard, influencing not only European countries but also legal practices across the world. However, certain challenges remain, for example, in distinguishing between physical and behavioral biometrics and in addressing the complexities of biometric technologies like verification and identification.

Comparing the EU's approach to the United States' approach highlights the EU's more comprehensive and unified regulatory framework, in contrast to the fragmented state-level laws in the US. Although the US has made progress through state regulations such as Illinois' Biometric Information Privacy Act (BIPA) and the more recent American Privacy Rights Act, the lack of the unified national approach raises concerns. For instance, behavioral biometrics are still inadequately addressed in the US. As technologies such as AI continue to evolve and become increasingly interconnected with biometric technologies, it is important to highlight that the EU and the US should continue to strengthen their regulations to safeguard personal data and promote the ethical use of biometrics. Yet given the novelty of behavior biometrics, further research of legal regulation of personal data is required.

References

Alsaadi, E. (2021). *Study on Most Popular Behavioral Biometrics, Advantages, Disadvantages and Recent Applications: A Review*. https://doi.org/10.13140/RG.2.2.28802.09926

Arcila, B. B. (2024). AI liability in Europe: How does it complement risk regulation and deal with the problem of human oversight? *Computer Law & Security Review*, *54*, 106012. https://doi.org/10.1016/j.clsr.2024.106012

Aseri, A. (2020). The Implication of the European Union's General Data Protection Regulation (GDPR) on the Global Data Privacy. *Journal of Theoretical and Applied Information Technology*, *98*(4), 692–702.

Carrigan, C., & Coglianese, C. (2011). The Politics of Regulation: From New Institutionalism to New Governance. *Annual Review of Political Science*, *14*(1), 107–129. https://doi.org/10.1146/annurev.polisci.032408.171344

Chen, C., Frey, C. B., & Presidente, G. (2022). Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally. *Oxford Martin School*.

Cheung, W., & Vhaduri, S. (2020). Continuous Authentication of Wearable Device Users from Heart Rate, Gait, and Breathing Data. *2020 8th IEEE RAS/EMBS International Conference for Biomedical Robotics and Biomechatronics (BioRob)*, 587–592. https://doi.org/10.1109/BioRob49111.2020.9224356

De Hert, P. (2013). Biometrics and the Challenge to Human Rights in Europe. Need for Regulation and Regulatory Distinctions. In: P. Campisi (Eds.), *Security and Privacy in Biometrics* (pp. 369–413). Springer London. https://doi.org/10.1007/978-1-4471-5230-9_15

Eberz, S., Rasmussen, K. B., Lenders, V., & Martinovic, I. (2017). Evaluating Behavioral Biometrics for Continuous Authentication: Challenges and Metrics. *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, 386–399. https://doi.org/10.1145/3052973.3053032

Ghelardi, E.-M. (2020). Closing the Data Gap: Protecting Biometric Information Under the Biometric Information Privacy Act and the California Consumer Protection Act. *St. John's Law Review*, *94*(3).

Greenleaf, G. (2012). The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108. *International Data Privacy Law*, *2*(2), 68–92. https://doi.org/10.1093/idpl/ips006

Illman, E. J. (2017). Data Privacy Laws Targeting Biometric and Geolocation Technologies. *The Business Lawyer*, *73*(1), 191–198.

Kindt, E. (2018). Having Yes, Using No? About the New Legal Regime for Biometric Data. *Computer Law & Security Review*, *34*(3), 523–538. https://doi.org/10.1016/j.clsr.2017.11.004

Li, H., Yu, L., & He, W. (2019). The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management*, *22*(1), 1–6. https://doi.org/10.1080/1097198X.2019.1569186

Meden, B., Rot, P., Terhorst, P., Damer, N., Kuijper, A., Scheirer, W. J., Ross, A., Peer, P., & Struc, V. (2021). Privacy–Enhancing Face Biometrics: A Comprehensive Survey. *IEEE Transactions on Information Forensics and Security*, *16*, 4147–4183. https://doi.org/10.1109/TIFS.2021.3096024

Neace, G. (2020). Biometric Privacy: Blending Employment Law with the Growth of Technology. *UIC Law Review*, *53*(1).

Nguyen, F. Q. (2018). The Standard for Biometric Data Protection. *Journal of Law & Cyber Warfare*, *7*(1), 61–84.

Rawat, Y., Gupta, Y., Khothari, G., Mittal, A., & Rautela, D. (2023). The Role of Artificial Intelligence in Biometrics. *2023 2nd International Conference on Edge Computing and Applications (ICECAA)*, 622–626. https://doi.org/10.1109/ICECAA58104.2023.10212224

Revett, K. (2008). *Behavioral Biometrics: A Remote Access Approach*. Wiley.

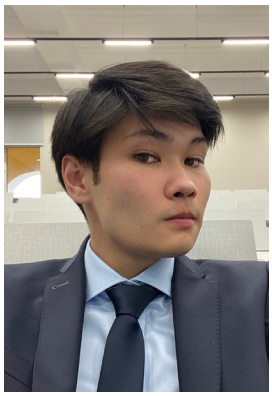
Rezaee, K. (2025). Machine Learning and Facial Recognition for Down Syndrome Detection: A Comprehensive review. *Computers in Human Behavior Reports*, *17*, 100600. https://doi.org/10.1016/j.chbr.2025.100600

Sharma, M., & Elmiligi, H. (2022). Behavioral Biometrics: Past, Present and Future. *Recent Advances in Biometrics*. IntechOpen. https://doi.org/10.5772/intechopen.102841

Xefteris, S., Doulamis, N., Andronikou, V., Varvarigou, T., & Cambourakis, G. (2016). Behavioral Biometrics in Assisted Living: A Methodology for Emotion Recognition. *Engineering, Technology & Applied Science Research*, *6*(4), 1035–1044. https://doi.org/10.48084/etasr.634

Authors information

Baurzhan Rakhmetov – PhD (Politics and International Relations), Assistant Professor, International School of Economics, M. Narikbayev KAZGUU University
Address: 8 Korgalzhyn street, 010000, Astana, Kazakhstan
E-mail: b_rakhmetov@kazguu.kz
ORCID ID: https://orcid.org/0000-0003-3948-9977
WoS Researcher ID: https://www.webofscience.com/wos/author/record/32537389
Google Scholar ID: https://scholar.google.com/citations?user=hanfRwoAAAAJ



Kazbek Khaizabekov – Master's Student, European and Global Studies, Department of Political Science, Law, and International Studies, University of Padova
Address: Via VIII Febbraio, 2, 35122 Padova PD, Italy
E-mail: khaizabekovk@gmail.com
ORCID ID: https://orcid.org/0009-0009-8241-8016
WoS Researcher ID: https://www.webofscience.com/wos/author/record/MIN-4357-2025

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interest

Baurzhan Rakhmetov is a member of the Editorial Board of the Journal; the article has been reviewed on general terms.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – September 19, 2024
Date of approval – October 23, 2024
Date of acceptance – March 25, 2025
Date of online placement – March 30, 2025

Научная статья
УДК 34:004:341:57.087.1:316.642.4
EDN: https://elibrary.ru/joupzt
DOI: https://doi.org/10.21202/jdtl.2025.5

Поведенческая биометрия в Европейском Союзе: правовые вызовы и технологические перспективы

Бауржан Рахметов ✉
Университет КАЗГЮУ имени М. С. Нарикбаева, Астана, Казахстан

Казбек Хайзабеков
Падуанский университет, Падуя, Италия

Ключевые слова

Европейский Союз,
законодательство,
защита данных,
искусственный интеллект,
конфиденциальность,
поведенческая биометрия,
право,
правовое регулирование,
распознавание лиц,
цифровые технологии

Аннотация

Цель: изучение исторического развития законодательства Европейского союза в области поведенческой биометрии, выявление особенностей европейского подхода к регулированию поведенческой биометрии, а также оценка его преимуществ и недостатков.

Методы: общенаучные методы анализа и сравнения с акцентом на изучение юридических текстов, таких как директивы, регламенты и конвенции. Для обеспечения всестороннего понимания проблемы авторы также рассматривают технические аспекты поведенческой биометрии, что позволяет провести комплексный анализ как правовых норм, так и технологических процессов, лежащих в их основе.

Результаты: нормативная правовая база Европейского союза в области биометрии недостаточно четко разграничивает технологии поведенческой и физической биометрии. Это приводит к неоднозначности в понимании рисков и возможностей, связанных с использованием поведенческой биометрии. Авторы подчеркивают, что отсутствие конкретики в законодательстве создает значительные трудности для регулирующих органов, разработчиков технологий и конечных пользователей.

Научная новизна: заключается в том, что она представляет собой первое комплексное исследование исторического развития законодательства Европейского союза в области поведенческой биометрии. В статье раскрываются ключевые характеристики европейского подхода, его сильные и слабые стороны, а также проводится сравнительный анализ с опытом регулирования в Соединенных Штатах. В исследовании детально раскрываются ключевые аспекты, требующие дальнейшего законодательного урегулирования: от четкой дефиниции

✉ Контактное лицо

поведенческой биометрии до разработки комплексных механизмов обеспечения прозрачности и подотчетности при использовании данных технологий. Учитывая, что поведенческая биометрия является относительно новой и быстро развивающейся технологией, такое исследование имеет важное значение для понимания современных вызовов и перспектив ее регулирования.

Практическая значимость: определяется его многогранным характером и актуальностью для широкого круга специалистов в сфере цифровых технологий: от ученых-правоведов, правоприменителей и законодателей до разработчиков технологий искусственного интеллекта и биометрии.

Для цитирования

Рахметов, Б., Хайзабеков, К. (2025). Поведенческая биометрия в Европейском союзе: правовые вызовы и технологические перспективы. *Journal of Digital Technologies and Law*, *3*(1), 108–124. https://doi.org/10.21202/jdtl.2025.5

Список литературы

Alsaadi, E. (2021). *Study on Most Popular Behavioral Biometrics, Advantages, Disadvantages and Recent Applications: A Review*. https://doi.org/10.13140/RG.2.2.28802.09926

Arcila, B. B. (2024). AI liability in Europe: How does it complement risk regulation and deal with the problem of human oversight? *Computer Law & Security Review*, *54*, 106012. https://doi.org/10.1016/j.clsr.2024.106012

Aseri, A. (2020). The Implication of the European Union's General Data Protection Regulation (GDPR) on the Global Data Privacy. *Journal of Theoretical and Applied Information Technology*, *98*(4), 692–702.

Carrigan, C., & Coglianese, C. (2011). The Politics of Regulation: From New Institutionalism to New Governance. *Annual Review of Political Science*, *14*(1), 107–129. https://doi.org/10.1146/annurev.polisci.032408.171344

Chen, C., Frey, C. B., & Presidente, G. (2022). Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally. *Oxford Martin School*.

Cheung, W., & Vhaduri, S. (2020). Continuous Authentication of Wearable Device Users from Heart Rate, Gait, and Breathing Data. *2020 8th IEEE RAS/EMBS International Conference for Biomedical Robotics and Biomechatronics (BioRob)*, 587–592. https://doi.org/10.1109/BioRob49111.2020.9224356

De Hert, P. (2013). Biometrics and the Challenge to Human Rights in Europe. Need for Regulation and Regulatory Distinctions. In: P. Campisi (Eds.), *Security and Privacy in Biometrics* (pp. 369–413). Springer London. https://doi.org/10.1007/978-1-4471-5230-9_15

Eberz, S., Rasmussen, K. B., Lenders, V., & Martinovic, I. (2017). Evaluating Behavioral Biometrics for Continuous Authentication: Challenges and Metrics. *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, 386–399. https://doi.org/10.1145/3052973.3053032

Ghelardi, E.-M. (2020). Closing the Data Gap: Protecting Biometric Information Under the Biometric Information Privacy Act and the California Consumer Protection Act. *St. John's Law Review*, *94*(3).

Greenleaf, G. (2012). The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108. *International Data Privacy Law*, *2*(2), 68–92. https://doi.org/10.1093/idpl/ips006

Illman, E. J. (2017). Data Privacy Laws Targeting Biometric and Geolocation Technologies. *The Business Lawyer*, *73*(1), 191–198.

Kindt, E. (2018). Having Yes, Using No? About the New Legal Regime for Biometric Data. *Computer Law & Security Review*, *34*(3), 523–538. https://doi.org/10.1016/j.clsr.2017.11.004

Li, H., Yu, L., & He, W. (2019). The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management*, *22*(1), 1–6. https://doi.org/10.1080/1097198X.2019.1569186

Meden, B., Rot, P., Terhorst, P., Damer, N., Kuijper, A., Scheirer, W. J., Ross, A., Peer, P., & Struc, V. (2021). Privacy–Enhancing Face Biometrics: A Comprehensive Survey. *IEEE Transactions on Information Forensics and Security*, *16*, 4147–4183. https://doi.org/10.1109/TIFS.2021.3096024

Neace, G. (2020). Biometric Privacy: Blending Employment Law with the Growth of Technology. *UIC Law Review*, *53*(1).

Nguyen, F. Q. (2018). The Standard for Biometric Data Protection. *Journal of Law & Cyber Warfare*, *7*(1), 61–84.

Rawat, Y., Gupta, Y., Khothari, G., Mittal, A., & Rautela, D. (2023). The Role of Artificial Intelligence in Biometrics. *2023 2nd International Conference on Edge Computing and Applications (ICECAA)*, 622–626. https://doi.org/10.1109/ICECAA58104.2023.10212224

Revett, K. (2008). *Behavioral Biometrics: A Remote Access Approach*. Wiley.

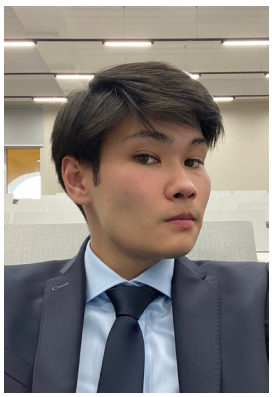
Rezaee, K. (2025). Machine Learning and Facial Recognition for Down Syndrome Detection: A Comprehensive review. *Computers in Human Behavior Reports*, *17*, 100600. https://doi.org/10.1016/j.chbr.2025.100600

Sharma, M., & Elmiligi, H. (2022). Behavioral Biometrics: Past, Present and Future. *Recent Advances in Biometrics*. IntechOpen. https://doi.org/10.5772/intechopen.102841

Xefteris, S., Doulamis, N., Andronikou, V., Varvarigou, T., & Cambourakis, G. (2016). Behavioral Biometrics in Assisted Living: A Methodology for Emotion Recognition. *Engineering, Technology & Applied Science Research*, *6*(4), 1035–1044. https://doi.org/10.48084/etasr.634

Сведения об авторах

Рахметов Бауржан – PhD в области политологии и международных отношений, ассистент-профессор, Международная школа экономики, Университет КАЗГЮУ имени М.С. Нарикбаева
Адрес: Казахстан, 010000, г. Астана, Коргалжинское шоссе, 8
E-mail: b_rakhmetov@kazguu.kz
ORCID ID: https://orcid.org/0000-0003-3948-9977
WoS Researcher ID: https://www.webofscience.com/wos/author/record/32537389
Google Scholar ID: https://scholar.google.com/citations?user=hanfRwoAAAAJ



Хайзабеков Казбек – магистрант в области европеистики и глобальных исследований, кафедра политологии, права и международных исследований, Падуанский университет
Адрес: Италия, 35122, г. Падуя, ул. 8 февраля, 2
E-mail: khaizabekovk@gmail.com
ORCID ID: https://orcid.org/0009-0009-8241-8016
WoS Researcher ID: https://www.webofscience.com/wos/author/record/MIN-4357-2025

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Бауржан Рахметов является членом редакционной коллегии данного журнала; статья прошла рецензирование на общих условиях.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.87 / Международное право
Специальность ВАК: 5.1.5 / Международно-правовые науки

История статьи

Дата поступления – 19 сентября 2024 г.
Дата одобрения после рецензирования – 23 октября 2024 г.
Дата принятия к опубликованию – 25 марта 2025 г.
Дата онлайн-размещения – 30 марта 2025 г.