UDC 341.1/.8

DOI: 10.18523/2617-2607.2023.11.64-76

Daria Bulgakova
ORCID: https://orcid.org/0000-0002-8640-3622

Valentyna Bulgakova
ORCID: https://orcid.org/0009-0009-6463-5228

THE COMPLIANCE OF FACIAL PROCESSING IN FRANCE WITH THE ARTICLE 9 PARAGRAPH 2 (a) (g) OF (EU) GENERAL DATA PROTECTION REGULATION*

The legal identity of individuals is critical in digital ecosystems, and biometric systems play a vital role in verifying identities throughout their lives. However, these systems also pose significant risks and require responsible use. The European Union has established a digital strategy to create a trusted and secure digital identity, setting a global standard for technological development in identification. In line with the General Data Protection Regulation Article 9(1), member countries must justify any exceptions to the rule provided. France has taken a leading role in using unique identification legally, implementing digitally processed attributes such as facial recognition through the Alicem application on smartphones to identify individuals in a digital environment, and improving e-services uniquely. Specifically, the article analyses the General Data Protection Regulation Article 9, paragraph 1, and the exceptional conditions outlined in paragraph 2 (a) (g) along with scrutinized legislation in France of Decree n°2019-452 of 13 May 2019, which authorized the use of unique identification known as 'Certified Online Authentication on Mobile.' The research recommends that EU member countries taking approaches to introduce GDPR Article 9 into national legislation should consider their citizens' specific needs and concerns while aligning with the European Union law because it is critical to balance the benefits of biometric systems with the risks posed to personal data protection, ensuring that their responsible use contributes to a secure and trustworthy digital ecosystem.

Keywords: biometric data, human recognition, digital legal identity, unique identification, Alicem application.

Introduction

Governments, international organizations, and the private sector have come together to advocate the recognition of a person's identity through the efforts of the European Digital Rights (EDRi) association, which includes non-European and international members who share a commitment to digitalisation in the European Union (EU). The United Nations, through the Alliance Partners ID2020, also promotes the importance of human recognition, as digital identity is considered a fundamental human right that should be under everyone's control. The goal is to provide everyone with a trusted and viable technological form of sustainable legal identity. The biometric nature of digital identity recognition has sparked an ongoing debate around the development of technology that can provide secure human identity without infringing on fundamental rights and freedoms. An article further defends this viewpoint, emphasizing that the digitization of legal identity is grounded in human rights instruments, such as Article 6 of the Universal Declaration of Human Rights and Article 16 of the International Covenant on Civil and Political Rights, which guarantee everyone's right to recognition before the law. As a result, many countries are increasingly adopting policies to digitize and streamline their national identity systems, which enhance human recognition by creating a foundational registry for a digital identity ecosystem. A unique identifier can answer an individual's official e-existence, thereby necessitating the legalization of recognition techniques to fulfill personality in the digital space.

* The related to this manuscript research on "The Case Study about Facial ALICEM Identification under GDPR Article 9(2, g)" was presented for the 9th International Ph.D. and Young Researchers Conference "Everything You Always Wanted to Know About Law (But Afraid to Ask)" at Vilnius University, Faculty of Law, Vilnius, Lithuania, 2-3 June 2022.

However, it is essential to note that the General Data Protection Regulation (GDPR)[1] deems biometrics a particular category of data requiring a higher level of protection to safeguard individuals against any negative impacts from its use. Legal challenges must be addressed to establish appropriate governance for cyber identity authentication, preventing human bodies from being read, profiled, and acted upon by machinery. Thus, it is crucial to have appropriate data protection laws and legal safeguards at both the EU and Member State levels when adopting biometric-based national digital identity rules. This is particularly relevant as the GDPR has a direct implementation for Member States and requires them to take necessary steps to adapt legislation by repealing or amending outdated national provisions to ensure uniform application across the Union. To avoid conflicts between EU and national law, Member States can maintain supplementary data protection rules in specific areas, such as the public and municipal sector, employment and social security, preventive and professional medicine, processing for scientific, historical research, statistical purposes, public access to official documents, and the processing of genetic and biometric data. The implementation of EU norms in Member States' legislation is a critical legal consideration, as any degree of deviation could affect its practice. Moreover, for compliance with EU law, Member States must consider national measures that align with the Lisbon Treaties and are consistent with EU law. Additionally, the reproduction of the GDPR text verbatim in special rules must be exclusive and justified. The repetition of EU regulations in national law is prohibited unless strictly necessary to ensure consistency and make national laws understandable for those to whom they apply.

Analysis of recent research and publications. The antecedent novel theoretical doctrine of biometric data processing has been articulated through a vital transformation of the digital compass of individuals. It is mainly due to the widespread use of big data. The advantages of automotive processing allow users to independently create content and manage the connection between their own and other people's footprints through machine governance and even biological footprints.[2] As a result, it led to the coordination and inclusion of users not only in the procedure of creating personal data content but also within the algorithmic processing following public e-service matter in hand while providing the required information about him/her.[3] Cloud computing technologies increase production capacity available for storing and processing information by private and public organisations and individuals while retaining technologies that effectively process large amounts of data.[4] A scholar Hildebrandt[5] in his research assumes that personal data has been finally transferred to the electronic environment. Accordingly, it is exposed to new legal risks associated with the negative consequences of the impact on data protection regulation. It is non-tech neutral compared to the growing functionality of modern biotechnologies. With the help of big data, it became possible to analyze and integrate data generated via websites, weblogs, videos, text documents, services, and other sources. Nevertheless, this processing format needs aid with processing new types of personal data as biometrics. Specific biocharacteristics do not correspond to the standard automotive processing format.[6] Hence, the development of tech-neutral regulation of the legal relations concerning biometric data processing has been a long process.

The Council of Europe (CE) formulated a system of legal standards. The research highlights the promising activity of the CE as well as the activity of the European Parliament and the Council in the era of interplay law and biometric data processing. Regardless of that, the study includes a quantitative theoretical discussion about Convention 108,[7] Directive 95/46/EC,[8] and GDPR. The qualitative review has a place impact on the convergence of legal protection of the non-property interests of individuals within Europe. Adoption of the first international act in the field of data protection – Convention for the Protection of Individuals regarding Automatic Processing of Personal

[1] European Parliament and the Council, Regulation (EU) 2016/679 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), *Official Journal of the European Union. Law* 119/1 (4 May 2016).

[2] Aaron Opoku Amankwaa, "Trends in Forensic DNA Database: Transnational Exchange of DNA Data," *Forensic Sciences Research* 5, no. 1 (2020): 8–14.

[3] Mireille Hildebrandt, "Law as Information in the Era of Data-Driven Agency: Law as Information," *Modern Law Review* 79, no. 1 (2016): 1–30.

[4] *Ibid.*

[5] *Ibid.*

[6] EU, Report on Artificial Intelligence, 5 (2018).

[7] Convention for the Protection of Individuals with Regard to Automatic Processing of personal Data, CETS No. 108 (1981); Modernised Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (2018). Council of Europe, 128th Session of the Committee of Ministers, CM/Inf (2018)15-final; Council of Europe, Progress Report on the Application of the Principles Convention 108 to the Collection and Processing of Biometric Data (January 2014).

[8] 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 the Free Movement of Such Data.

Data – scholars regard the reason for actual contradiction between breakdown interpretations of automated data processing and its distribution in telecommunication networks, and further abuse in the proper use of personal data. The significance of this document is to unify relations concerning problematic processing by automated means. Thus, Schneider concludes,[9] through the adoption of several legal acts, European Union Law makes it possible to govern the protection of personal data. Additionally, to the position of scholar, the study is a view that Directive 95/46/EC has led to the layout of modern data protection leading to the crucial changes in the level of national legislation of the Members-States of the EU. From now on, to harmonize EU law and national law, each state started to coordinate rules for personal data processing in multi-layered sources.

Despite the legislation, legal sources nowadays are concerned with the problem of the rapid use of personal information by state bodies, commercial organizations, and individuals; that has come to be the issue number one and could not be governed by those legal acts. The problem arose with a regulatory framework, specifically with the start-up of technologies that processed the biometrics of individuals. Although another scholar Hermstrüwer Yoan[10] actively defended the situation calling to encourage rules governing the use of personal data by institutions, bodies, and institutions of a supranational organization, as well as by any other officials of such groups. The researcher viewed that if there is a shortage in the rules, then that legal lack notably may solve applying the principle of proportionality. Therefore, while this principle will eliminate these shortcomings, it is worth paying attention to improving the legal regulation of personal data protection in the European Union, especially in the sphere where the type of data is such characteristics that carry human origin.

Continuing the researcher's insights, indeed, the studied material written by Kamarinou[11] forms the following understanding of the topic being stated in the following opinion. The author distinguished the processing operation into several phases where the principle of proportionality must be spread to the collections, storage, modification, and transfer. The necessity of a specific application instead of a standard way is explained by the reason for the formation of new perception as machine learning. That means the law interacts with another field of knowledge. Therefore, there is a risk to the availability of robust legal protection of operations because certain regulative standards have yet to be developed since the threat of biometric data processing is faster than the laws adopted. This means, the biometric trend is risky because it needs to have a sufficient enough legal framework. The problem of uncontrolled biometric identification has also arisen in the work of Krausova.[12] The author highlighted that the problem that needs to be eliminated is not the neutrality of biometric technology and legal regulation. In this regard, the legal relationships concerning biometrics are not balanced; therefore, applying the principle of proportionality is needed. The study deliberates that the proportionality principle should regulate the relationship so that the processing would obtain its scope that must be directly proportional to the technology involved and the user's awareness of the processing techniques conducted by the biometric machine.

According to the scientists of legal studies, big data has influenced modern legal needs to meet the requirements of automotive processing. An example of such an opinion is the work of Krivogin.[13] In contrast to previous researchers, his analysis is traced to Regulation No. 45/2001.[14] A scholar states that there is no procedure for the principle to be applicable since appointed regulation is already devoted to data being mandatory for all institutions and bodies of the Union insofar as the processing is carried out in the course of activities that partially or entirely fall under data protection legislation of the EU. At the same time, the author also presumes many of the provisions of the discussed document were subsequently adapted and incorporated into GDPR. Therefore, although the GDPR indicates in Recital 4 that the principle of proportionality should be applied, at the same time, the legislator should have included an explanation of how such an

[9] Giulia Schneider, "Health Data Pools under European Policy and Data Protection Law: Research as a New Efficiency Defence?," *Journal of Intellectual Property, Information Technology, and Electronic Commerce Law* 11 (2020): 49.

[10] Yoan Hermstrüwer, "Contracting around Privacy: The (Behavioral) Law and Economics of Consent and Big Data," *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 8 (2017): 9.

[11] Dimitra Kamarinou, Christopher Millard, and Jatinder Singh, "Machine Learning with Personal Data," Queen Mary School of Law Legal Studies Research Paper 247/2016, November 7, 2016.

[12] Alžběta Krausová, "Online Behavior Recognition: Can We Consider It Biometric Data Under GDPR?," *Masaryk University Journal of Law and Technology* 12, no. 2 (2018): 161–78, https://doi.org/10.5817/MUJLT2018-2-3.

[13] Maxim Krivogin, "Peculiarities of Legal Regulating Biometric Personal Data," *Law. Journal of the Higher School of Economics* no. 2 (2017): 80–89.

[14] Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and On the Free Movement of Such Data.

application can be practiced, and hence the manual experience is needed. Especially denying practice, such an interpretation is impossible due to innovations and the boom of biometric technologies, when a legislator without technical knowledge and trial is unable to adopt highly qualitative and appropriate regulation. Respectively, Also, the scholar Milaj in academic work[15] emphasised proportionality by perceiving it to be a legal tool for evaluating the standards for technologies manufactured according to the criteria developed through the particular characteristics of this principle.

Scholars Wang Han[16] and Zhao Bo[17] based on their works, both doubted the problem of restraining processing by electronic aptitude. According to Zhao Bo, European Union law aims to harmonize the e-law over the world and globally to build a certain level of protection of fundamental rights and freedoms whether typically personal data or specifically sensitive data are processed. In particular, the requirements specify the transparency and confidentiality of data processing, data accuracy, sufficiency and purpose legitimacy, data safety, and the possibility for data deletion, as well as the free circulation of such data, equipment, and electronic communications services in the Union. However, Wang Han assumes European regulation in a contrary way. He believes European Union Law is eye-catching and has missed specific criteria for sensitive personal data. The writer is mannered that the more sensitive the piece of data, the stricter rules must be applied. The paper supports the researchers' opinion and also delivers the readers' attention to the statement that the specific data characteristics and biometric attributes are crucial for the processing prerequisite and entail competent legal norms.

Concerning risk mitigation, Macenaite's work[18] provides some valuable insights: (1) The protection system of the European Union is primarily designed to penalize misuse of personal data; (2) While Member States can establish specific requirements, these must not contradict EU primary sources; (3) Controllers are responsible for ensuring compliance with data protection laws, not the individuals themselves; (4) National laws determine the controllers' power, but the EU's hierarchical structure ultimately limits these; (5) Discretion should be exercised in identifying risks proportionally to the rights and freedoms of data subjects. However, there may be areas for improvement in the specific implementation of national legislation. For example, a provision that only allows biometric data processing necessary for personal legality may lead to misinterpretation of the grounds for processing. Therefore, in cases of ambiguity, the GDPR requires proportionality to be applied.

Statement of the problem. France has been at the forefront of biometric data processing among the Member-States with specific regulations in place before the introduction of GDPR. The new law was authorised by a Decree n° 2019-452 of 13 May 2019 of the Council of State adopted after a substantiated, not supportive vision of the French data regulatory authority Commission on Informatics and Liberty/ Commission Nationale de l'Informatique et des Libertés (CNIL) in Deliberation n° 2018-342.[19] The changes were incorporated into the former French data protection regulation by Law No. 2018-493 on 20 June 2018 and by Decree No. 2018-687 on 1 August 2018. Under GDPR Article 9(4), the French legislature has added additional conditions for biometric data processing, including the requirement that the processing is permitted on the state's behalf. Except for that essential, CNIL may prescribe additional legal, technical, and organizational measures for handling biometric data and provide legal guarantees for individuals. In non-ordinary cases, biometric data processing for the objective of the state's security, defense, or public safety may be permitted.

Facial recognition technology has revolutionized how people prove their digital legal identity and gain authorized access to e-services. In a significant move, France has recognized facial identification as a reasonable means of verifying legal identity, considering the exception provided under GDPR Article 9(2, a & g). To facilitate this, under Decree n° 2019-452, the Alicem smartphone application uses facial recognition technology to authenticate users accessing the e-service of Alicem through the FranceConnect platform, which provides free software solutions. Furthermore,

[15] Jonida Milaj, "Privacy, Surveillance, and the Proportionality Principle: The Need for a Method of Assessing Privacy Implications of Technologies Used for Surveillance," *International Review of Law, Computers & Technology* 30, no. 3 (2016): 115–30.

[16] Sarah Wang Han and Abu Bakar Munir, "Practitioner's Corner · Information Security Technology – Personal Information Security Specification: China's Version of the GDPR?," *European Data Protection Law Review* 4, no. 4 (2018): 535–41, https://doi.org/10.21552/edpl/2018/4/19.

[17] Bo Zhao and Jeanne Mifsud Bonnici, "Protecting EU Citizens' Personal Data in China: a Reality or a Fantasy?," *International Journal of Law and Information Technology* 24, no. 2 (2016): 128–50, https://doi.org/10.1093/ijlit/eaw001.

[18] Milda Macenaite, "The 'Riskification' of European Data Protection Law through a Two-Fold Shift," *European Journal of Risk Regulation* 8, no. 3 (2017): 506–40, https://doi.org/10.1017/err.2017.40.

[19] France, National Commission for Informatics and Liberty, Deliberation n° 2018-342 of 18 October 2018, *Authenticated Electronic Official Journal* no. 0113 (16 May 2019).

the French Minister of the Interior Affairs has ensured that electronic identification is safeguarded through the certification of Alicem online authentication on mobile devices, and its issuance pursues GDPR Article 9(4). In contrast, the Regulation allows Member-States to introduce additional biometric conditions under national law. Nevertheless, the French government has implemented a standardized biometric authentication system for various government and public service websites. However, the study has raised a statement of the problem regarding the system's legal basis, arguing that it lacks lawful consent and facial processing is disproportionate to the Alicem unique technique's intended purpose.

Research Questions. Considering the matter, two critical questions the research addresses. Firstly, Does the Alicem system obtain valid consent from its users to process their biometric data? Is the employment of facial recognition technology to process biometric data for public services a reasonable means of achieving the intended purpose? These questions have significant implications for the system's compliance with GDPR Article 9 para 2 (a) (g), which outlines conditions for employing biometric data for identification purposes.

Methodology. To interpret the underlying subject and toil towards advance, the breakdown is founded on the 'black-letter law' method and devotes tools of perceptive European Union law and France's national data protection decree that recognized Alicem as an official smartphone application that employs facial recognition process. Remarkably, the study justifies the Decree n° 2019-452 of 13 May 2019, authorizing unique identification 'Certified Online Authentication on Mobile' together with the national dispute of Council of State, 10th–9th chambers combined, Case No. 432656; ECLI:FR:CECHR:2020:432656.20201104, the Decision of 4 November 2020 to the GDPR Article 9 para (1) and the exceptional conditions under para 2 (a) (g) accordingly.

Problem Assessment. The GDPR Article 9(1)(2) is being developed to mandate alternative techniques to verify people's identity to address situations where an individual chooses not to provide biometric data for identification. The European Parliamentary Assembly has also imposed limitations on biometric technology, stating that it should only be utilised when there is an obvious necessity and its benefits outweigh the potential impact on human rights. Furthermore, alternative identification and verification methods must be unrestricted to individuals unable or unwilling to provide biometric data. Harmonization is also a key objective, with national laws being able to impose additional restrictions on biometric data processing under GDPR Article 9(4). These provisions enable Member-States to introduce supplementary prerequisites for processing, including biometric data. Although such opening clauses are not obligatory in EU secondary law, they facilitate cooperation among the Member-States. This study examines the intersection between European Union Law and Member-States' Law regarding personal data protection legislation in the model of France, which has enacted national legislation allowing facial identification while safeguarding the interests of its citizens for their digital identity.

France has officially recognized facial identification as a means of proving legal identity, using the Alicem smartphone application developed under the Ministry of the Interior and the National Agency for Secured Titles / Agence Nationale des Titres Sécurisés (ANTS). The French Minister of the Interior has been authorised to implement automated processing of personal data for certified online authentication on mobile, which aims to simplify users' lives as they increasingly use digital biometric technology to access public and private services. Under the ANTS, the application provides a secure way for users to create an account and authenticate themselves with online service providers. It has been in the test phase on the FranceConnect platform since June 2019. The technology is accessible to foreign nationals with an electronic chip. It is endorsed for use under Decree n° 2019-452 of 13 May 2019, 'Certified online authentication on mobile,' entitling the output of electronic identification means. The National Supervisory Board for the Protection of Personal Data / Nationale de contrôle de la protection des Données à caractère Personnel notes that the application does not necessarily involve the processing of personal data unless it is instructed for access to a service with a high level of security.

Prior to that, CNIL in Deliberation n° 2018-342 stated that the Alicem processing did not hold a sufficient impact appraisal and that the use of biometric data for identity verification through facial recognition is a substantial change that needs further scrutiny. The CNIL acknowledged that the purpose of the Alicem system was legitimate and explicit but questioned the credibility of consent as a legal basis for the processing of biometric data citing Article 9 para 1 of the GDPR, which prohibits the processing of biometric data except under specific circumstances, such as stated in para 2 (a) when the data subject has given explicit consent and/or when the processing is necessary for reasons of substantial public interest as per para 2 (g). The argument for an interpretation of para 2 (a) is that

the consent must be free, specific, informed, and unambiguous and that the refusal to carry out facial recognition would prevent the creation of the digital identity, making the consent not genuinely voluntary. The CNIL also, with respect to para 2 (g), stated that the necessity for using biometric data must be demonstrated and that alternative solutions must be developed to ensure practical freedom of consent. Therefore, the provisions of (a) and (g) in para 2 of Article 9 GDPR failed to demonstrate the proportionality principle as per Recital 4 of the GDPR. Similarly, the potential intrusiveness on the dignity of individuals, coupled with a risk of adverse negative impact on human rights and fundamental freedoms, underscores the importance of the proportionality canon under the Charter of Fundamental Rights of the European Union Article 52.

Research Results. The study highlights the contradiction in visions stipulated in the Deliberation n° 2018-342 and Decree n° 2019-452 about the exceptions approach of the GDPR Article para 2 (a) (g). According to Decree n° 2019-452 Article 1, the static and dynamic facial recognition system, live facial recognition technologies in uncontrolled environments should be subject to a democratic debate on its use and the possibility of a moratorium pending complete analysis. A declared association La Quadrature du Net (LQDN), fostering and protecting fundamental freedoms in the digital globe, believes that Decree n° 2019-452 also violates GDPR Article 4 para 11 and Article 7 para 4 by noncompliance in the obtaining of lawful consent for the use of biometric data and that facial recognition is disproportionate to the purpose of the processing. Therefore, there are two imbalances in the situation. Firstly, there is a conflict between the legitimate interest in providing efficient access to e-Government services through secure facial identification and the user's right to consent to the creation of a digital legal identity avoiding the use of individual biometrics. Secondly, suppose a person declines to use unique facial data for online recognition. In that case, it prevents the account activation for digitized identity satisfaction and violates initial consent to create the account.

In 2020, the Council of State held a hearing (case details in the methodology section) about (a) whether the validity of consent for the Alicem authentication system should be assessed at the level of each data processing or for all equivalent services, and (b) whether processing of biometric facial data by the Alicem for authentication purposes with certain public services and partners is sufficient, consistent, and reasonable under GDPR Article 5. In other means, the research targets to determine whether the Alicem processing is proportional to the scope of the unique identification. To dig it, the manuscript delves into Decree n° 2019-452, paying attention to Convention 108, Guidelines on Facial Recognition[20] which recognizes the challenges posed by the proliferation of facial recognition technology in Europe and underscores the importance of assessing the necessity and proportionality of its users about its impact on the rights of data subjects under the Quick-Guide to Necessity and Proportionality.[21] To this extent, the applicable framework refers to the robust and tailored to the specific use situation of the biometric technology addressing key elements of compliance such as (a) the purpose of the processing, (b) the minimum reliability and accuracy of the algorithm used, (c) the traceability of the process, and (d) the measure to link to the collected facial data additional personal information in order afterward pinpoint the person concerned back, otherwise anonymous biometric identification is out of the GDPR' scope.

People who use their smartphones for digital identity exercise their own will and decision-making abilities. The phone usually comes with a biometric tool installed, which the person can choose to use or not. This approach is called human-centric or user-centric because the person controls their biometric data and can make decisions based on their preferences and needs. In the European Union, this approach is thought safe and respectful of individuals' autonomy. Decree n° 2019-452 Article 7 specifies the processing categories of data flow, which, notably to the human-centric course, are kept on the user's mobile equipment and processed under their exclusive control. Those protected data consist of (a.1) data to allow the identification of the user, (b.2) data to allow the identification of the title held by the user, (c.3) data to record the history of transactions done via the Alicem account, and (d.4) the unique identifier of the notification service to identify the mobile device. Also, the Decree regulates the retention duration of the photos used, the possibility to audit, and safeguards to protect data subjects' rights. On the one hand, the user must be legally aware of these conditions if they wish to access the service. The user must be legally aware of these conditions to access the service, and the service

[20] Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Directorate General of Human Rights and Rule of Law, Guidelines on Facial Recognition (28 January 2021).

[21] European Data Protection Supervisor, Assessing the Necessity of Measures that Limit the Fundamental Right to the Protection of Personal Data: A TOOLKIT (11 April 2017); European Data Protection Supervisor, Guidelines on Assessing the Proportionality Measures that Limit the Fundamental Rights to Privacy and the Protection of Personal Data (19 December 2019).

requires the user to deliver biometric characteristics as the basis of its economic model. Thus, at each time of the account operation, ANTS informs the user about the activity of the facial recognition technique, automatically proposing a consent policy ensuring transparency and informed decision-making.

A study advocates that the 'will' is problematic because if a user does not consent to process facial recognition, he/she cannot create an Alicem account with its mandatory facial functionality. Consequently, access to the digital legal identity is guaranteed without it respect to data protection. So, the denial to be facially identified impact negative consequences to nationals and affects a person's freedom of decision-making as the consent would be given under pressure. Personal data processing must have the data subject's consent, under the conditions mentioned in GDPR Article 4 (11) and Article 7, as well as Recital 42 states: 'Consent should not be regarded as having been freely given if the data subject does not have a genuine freedom of choice or is not able to refuse or withdraw consent without suffering prejudice.' In comparison, Recital 43 states: 'Consent shall be presumed not to have been freely given if separate consent cannot be given to different personal data processing operations although this is appropriate in the particular case, or if the performance of a contract, including the provision of a service, – it is subject to a consent even though consent is not necessary for such performance.' Given the manuscript, to ensure compliance with processing requirements in technological innovation, it is necessary to establish general conditions of service within the concrete framework of an application that incorporates biometric functionality. This confirms the lawfulness of biometric data processing. The analysis of the validity of these conditions goes beyond the user's interest alone and affects the legal certainty of the digital economy. Besides, biometric advertising relies on biometric technologies controlled and managed by the user. When people purchase a biometric product, they essentially consent to process their biometric data. However, it is unfair to assume that the user is responsible for any performance loss resulting from the tool settings' configuration, especially if they cannot refuse the offered advertising. The study emphasizes that this plainly exhibits an individual's right to privacy and security through automated means designed for identity protection. This understanding is consistent with the GDPR's legal framework, which recognizes the potential for solely automated decision-making processes that do not involve human intervention.

It is evident that facial data use a unique criterion that allows the designation of a title holder to be certified and confirm the secure way to relevant, adequate, and not bloated creation of the digital identity. Facial recognition could accurately verify the alleged identity using a contraption. Subjecting to the purpose, Alicem is determined explicit, legitimate, and going along with the conditions of Article 5 (1, b) of the GDPR. The consent in France is practiced under (the first in the view of the study) legal basis, which is a necessity – a secure solution for the digital existence of individuals and their performance in the governmental e-services system. However, a law should distinguish between the creation of digital identity and the step of verifying the identity alleged by the person in Alicem. This activation is subjected to the processing of biometric data. Indeed, it seeks to achieve unique characteristics while implementing Alicem identification. On the other hand, a manuscript offers the mobilization of trust – (the second in the view of the study) legal basis for biometric experience. It is because, per Guidelines on Facial Recognition, a license – a certified mobile application – should not, as a power, be the lawful basis operated for facial recognition perpetrated by public authorities, viewing the imbalance of powers between data subjects and public authorities**.** For the same reason, as a rule, it should apply to similar tasks targeted by public authorities in France. Consent in the dispute seems to be a safeguard from the perspective of organisational and technical measures, but it is not fulfilled from the side of the proportionate way to the user's trust in Alicem's execution. The public interest recalls the conviction in Alicem serves. A study admits a conviction can only constitute a legitimate facial enactment if an individual has control and a natural choice concerning the step forward in accepting or refusing the Alicem solution without suffering prejudice. In demand to ensure smooth communication and proper recognition of human identity in the digital society of France, individuals shall be questioned to participate in forming their digital identity during the processing stage. This entangles undergoing a facial recognition process to design an Alicem digital legal identity, as no other alternatives are available to issue secure digital identity welfare in the network.

On the positive tab**,** under Decree n° 2019-452 Article 1, the pursuit of facial processing is to deliver proposals for French and foreign nationals' holders of a biometric ID the issuance of electronic identification on a digital scale, letting them to identify and authenticate themselves electronically with public or private bodies**,** and to attest it by employing electronic transmissions of terminal supplies furnished with a device lessening the contactless task of the electronic feature according to the provisions of Regulation

(EU) No 910/2014[22] relating to the teleservice concerned. Also, Decree n° 2019-452 Article 2 gives rise to opening an account for enrolment. Article 4 established the usefulness of a static and dynamic facial recognition system to ensure a trusted way. Article 10 stipulates that the data collected by the facial recognition system are collected for the sole purpose of and erased as soon as recognition is completed. Under the terms of Article 13, ANTS shall inform the user about the benefit of a static and dynamic facial recognition device at the time of opening an account and obtain consent to the processing of his/her biometric data.

Therefore, a study confirms that the ANTS implements the processing of data accordingly to provisions requirements in 'm' & 'n' of para 1, and the data conditions specified in 'o', 'p', 'q' of para 1, and para 3 of Article 7 Decree n° 2019-452. The processing uses both static and dynamic facial recognition systems and does not include a search device for identification from already scanned facial images. The personal data linked to facial identification includes name, date of birth, country of birth, nationality, gender, eye color, user's photograph for the title, user's photograph for facial recognition, video for dynamic facial recognition, telephone number of the electronic communications terminal, and a technical identifier associated with the user's account. The data is stored on the user's electronic communications terminal equipment and is encrypted, inaccessible once the user deletes their account, and is deleted after a period of inactivity or six years. Accordingly, the personal data linked to facial ID is relevant, adequate, and reasonable concerning the sense of producing a digital identity. This processing falls under the GDPR also because ANTS handles access, rectification, erasure, and data portability rights and aligns with Article 9(4) when the national law of France may introduce additional conditions about the processing of unique features. For example, facial recognition through the Alicem application (app) accurately verifies the alleged identity of the person that uses a particular device, creating a digital identity that individuals can use to identify and authenticate themselves for online services. During enrolment, the data comes from the electronic component's contactable reader, qualifying the title holder's identity to be certified.

In the view of the study, GDPR Article 9(4) equips a prospect to execute ordinances for biometric data processing on behalf of the State. It acts to exercise its prerogatives as a public authority necessary to authenticate and drive the digital legal identity. The service in the form of an application mobile operating system provides users a high level of guarantee and bid enhanced protection against data misuse or usurpation of identity in the context of digital procedures. Important to note that the user provides consent to the processing of biometric data collected through a designed system by recording a facial recognition algorithm that verifies an individual to be the legitimate holder of the biometric title and that reaches the identity claimed and ascertained determination of its validity according to an authoritative source as per Directive (EU) 2018/1972.[23] Electronic identifiers are associated with the user's account and enable a connection of digital identity with procedures on partner teleservices. Digital identity has a biometric identifier recognized by the Member-State, France, for lodged electronic exactness when an identifier is equal to the alleged identity. To confirm the authenticity of an element, an authoritative applicant is responsible for verifying its validity. The applicant is able to identify the person in question by comparing their physical characteristics with a reliable source. This comparison serves as a means of confirming the person's identity.

The examination suggests a unique tag can be a reliable way to secure electronic designations in an app network. However, this measure cannot override the prohibition stated in Article 9(1) of the GDPR. To determine whether employing such an extent is necessary, further evidence of its security benefits is needed, as outlined in Article 9(2, g) of the GDPR. Based on the study's findings, limitations can be placed on using biometric recognition technology to balance individual data protection and public interest. Specifically, biometric recognition should only be used if it is strictly necessary for the service requested by the individual or if the data controller provides an alternative to biometric recognition for the data subject to benefit. A verification function can be enforced to affirm trust in the Alicem networking system, providing a high level of cybersecurity to ensure accurate identity recognition. This is achievable through the app system because the Decree mandates that biometric data collected during account creation is promptly deleted after recognition. This deletion is in accordance with Decree n° 2019-452 Article 10, which requires erasure as soon as recognition is completed to

[22] European Parliament and the Council, 23 July 2014, Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, *Official Journal of the European Union. Law* 257/73 (28 August 2014).

[23] European Parliament and the Council, 11 December 2018, Directive (EU) 2018/1972 establishing the European Electronic Communications Code (Recast), *Official Journal of the European Union. Law* 321/36 (17 December 2018).

provide users with a high level of protection under Regulation (EU) No 910/2014. This guarantees that the data is inaccessible once the user deletes their account. It is kept only for the performance duration before being deleted within 24 hours or after six years of account inactivity, as specified in Article 11 of Decree n° 2019-452.

The mechanism utilised for the Alicem design must broadcast to the user whether static or dynamic facial recognition is being used when the account is forthright. Yet, this tool is limited only to reporting on facial recognition and does not comprise any actual facial data. The CNIL has stated in Deliberation n° 2018-342 that the data used for facial recognition come directly from the contactless reading of the electronic component of the ticket during the enrolment phase. This complies with Article 12 of the GDPR, which requires concise, transparent, understandable, and easily accessible information in clear and straightforward terms to be provided to the data subject about data processing at each request for identification and authentication by a service provider. The Decree also specifies that biometric data processing involves four components: (1) the user's tag, (2) the identification of the biometric designation, (3) the digital communications terminal equipment used by the person, (4) the history of transactions associated with an account. Nonetheless, facial data is not intercommunicated to e-providers under GDPR Article 9(1).

The documents in the case file demonstrate that FranceConnect, accessible through the Alicem application, does not mandate facial recognition processing. Users who do not consent to facial recognition processing in the context of Alicem can still access all e-services offered through FranceConnect. Therefore, users do not experience any prejudice due to the Alicem application. Consequently, the contested questions cannot argue that the consent of Alicem users is not willingly given or that the Decree infringes on the provisions of GDPR Article 9(2, a & g). Facial identification is proportionate to its purpose and is an acceptable means of identifying a person's digital identity in a cybersecurity context. The applicant's identity is confirmed by approximating one or more physical facets of the person from an authoritative source implementing Regulation (EU) 2015/1502.[24] Consent given for processing is voluntarily given and proportionate to that intent, as it is necessary to fulfill the digital identity and its management in the cybersecurity context.[25] Additionally, facial identification enables the certification of the identity of a title holder, which is pertinent, satisfactory, and not excessive regarding the objective of assembling a person's digital identity. In this case, the Decree of the Council of State authorized facial recognition technology, and the CNIL provided a reasoned and published (negative) opinion. It is prohibited to process biometric data to uniquely identify a natural person, except if the processing is justified by the public interest and authorized under the conditions provided by consent. Under the study view, the processing is carried out on behalf of the State, exercising its public authority prerogatives related to biometric data processing. The necessity for authentication in the digital environment justifies it. Facial recognition technologies must be lawful and based on the purposes of biometric processing provided by the law, together with safeguards complementing Modernised Convention 108.[26] As a result, in November 2020 State Council dismissed a conflicting request of the CNIL and substantiated that novel facial recognition through Alicem is compliant.

However, the study agrees with the CNIL position that alternative identification measures should be provided if biometric recognition is not desired. Biometric technology should safely and accurately identify a person who owns a personal e-cabinet of digitised identity. The study believes that a person's consent should not be based on whether they agree to facial recognition but rather on whether they want to use it as a protective measure for their digitised legal identity. Refusing facial recognition will lead to the rejection of a pass to the electronic service and one's digitized identity. However, biometric identification is considered a protective measure of digitised legal identity. In that case, it should be optional, and a person should have the freedom to choose whether they want it or not. This approach confirms that the goal of securing a digitised identity is committed and directly proportional to the purpose and interests concerned.

Conclusions

For the effective functioning of digitised legal identity in the context of legalised identification, it is necessary to have reliable legal mechanisms to ensure

[24] European Commission, 8 September 2015, Commission Implementing Regulation (EU) 2015/1502 On setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8 (3) of Regulation (EU) No 910/2014 of the European Parliament and the Council on electronic identification and trust services for electronic transactions in the internal market, *Official Journal of the European Union. Law* 235/7 (9 September 2015).

[25] *See* European Parliament and the Council, 20 June 2019, Regulation (EU) 2019/1157 on strengthening the security of identity cards of Union citizens and residence documents issued to Union citizens and their family members exercising their right of free movement, *Official Journal of the European Union. Law* 188/67 (12 July 2019).

[26] Modernised Convention, Article 19.

biometric protection. The Member-States must implement appropriate technical and organizational measures to safeguard the identity ecosystem effectively, especially when determining facial data. Under the Alicem case, the purpose of the unique identification is to offer the issuance of electronic titles, allowing users to identify a personality in digital means and to authenticate themselves by employing terminal equipment fitted with a contactable reading device of a static and dynamic facial recognition system. Constantly peering on a French stipulation on employing facial recognition as a tendency to maintain admittance to digitized legal identity consecutive by application Alicem, the manuscript ascertained that the government's Decree n° 2019-452 prominently commissioned the invention of unique automatic identification. Based on that, France reconsidered how to prove a person's credentials by fulfilling legal identity through facial recognition, which is authorised because the processing is necessary for a substantial public interest, which is commensurate to drive disposition of the right to data conserving, and delivers expedient and thorough dimensions to fend this fundamental right and the interests of the data subject under GDPR Article 9 para 2 (a) (g).

The study identified five key elements of Alicem's practice in France:

1. Satisfaction of the public interests: The biometric data processing by Alicem is for the public, which means it is intended to supply a service that is in the public interest. In this case, the service is the issuance of electronic titles, which enables users to identify themselves digitally and authenticate themselves by operating a terminal supply equipped with a contactable reading device of a static and dynamic facial recognition system.

2. Free consent: A person gives a license for processing biometric data. This means that users are not required to use Alicem, and they can choose whether to agree or not to provide their biometric data for the service. This approach is consistent with the GDPR's requirement that consent must be freely given, specific, informed, and unambiguous.

3. Respect for human dignity: The study found that Alicem respects human dignity because of the minimum reliability and accuracy of the algorithm used. This denotes that the technology is designed to minimize the risk of errors or false identifications, potentially harming an individual's reputation or dignity.

4. User control: Alicem is recorded on the user's mobile equipment using the ANTS leading technology-driven integrated programmatic advertising platform, allowing a person exclusive storage control. This indicates that users have complete control over their biometric data and can delete it anytime.

5. Necessity and proportionality: The study found that biometric data processing by Alicem is necessary and proportionate to the purpose of the service. The purpose of the service is to enable French and foreign nationals to identify themselves electronically, which is a legitimate public interest. The study concludes that facial distinction is a proportionate means of achieving this purpose.

Recommendations for national law of EU Member-States. Biometric data differs from access codes because it cannot be changed once disclosed and uniquely identifies a person. As a result, someone could be recalled without their knowledge based solely on their biometric characteristics. This poses a significant risk to data protection because biometric data is repeatedly used to authenticate online activities, such as accessing applications or services. Moreover, if someone's biometric data is disclosed, they could lose control over their identity, leading to negative consequences. Therefore, France has taken a case-by-case regulation approach to anticipate and address these risks. The examination suggests that authenticating the user's identity via unique facial characteristics offers distinct guaranteed security and reliability system levels to achieve a reliable digital legal identity. Therefore, the processing of biometric data authorized by the contested Decree n° 2019-452 must be seen as being given with consent, as it is necessary for the digital ecosystem and maintained for the intended purpose of proving who the user is.

The manuscript concludes that the French government has established a trustworthy official national approach to perpetrating digital identity by implementing regulatory measures for processing techniques. France has taken steps to implement provisions concerning the processing of exceptional personal data, explicitly stressing facial recognition technology. The technology has been beneficial in providing secure and efficient access to e-services, but France must guarantee compliance with legal requirements and the protection of individuals' unique data through necessary technical and organizational measures. The study identifies several conditions that must be met for the responsible use of biometric data processing. First, there must be an assessment of the necessity for biometric data processing while considering the principle of proportionality, particularly concerning biometrics. Second, national legislation should further restrict the processing of biometric characteristics due to their impact on human dignity. Third, national regulations should prohibit commercialising human body elements, as biometric technology can be exploited

for financial gain. Finally, biometric technology for identification should only be used as a last resort when other identification methods are ineffective.

Recommendations for organisational and technical experts. When people use a phone with a biometric tool, they process their unique attributes to ensure their safety through strong-willed decisions. This approach is called user-centric or human-centric in the European Union, where the person feels in control of their data. To minimise the data collected in biometrics, the study suggests using a two-fold math-substantiated description of the unique data based on an investigation of the minutiae, which habitually ends and produces bifurcations of elevations. To complete the storage limitation prerequisites, the template cannot be backside masterminded into a design concerning a fingerprint, and the hardware-based perception conformity is used where the details are deposited on a definite theme of the tool and run with the held device to admit the data without caching the data approaching single device itself. This grants the attached rejoinder throughout user authentication since the biometric templates remain to be stored sectional, and thus the recognition scheme does not demand unspecified outer response. A portable token system uses a fob or a smart card to store biometric data.[27] The person's data is seized and stored inside the token for future need.

To comply with GDPR Article 9 para 2 (a) (g) when processing facial data, it is advised to operate biometric templates that cannot stand reverse-engineered into a hardware perception. This confirms reliable user authentication since the biometric templates are stored separately. A portable token system, such as a fob or a thoughtful card, can store biometric data that was one-time captured, eliminating the need to convey the data over a network. This method reduces the risks of network-related vulnerabilities. To attest to the user, biometric data is presented as a two-step authentication process commonly used on smartphones. The biometric data is stored on-device through a chip separate from the device's shape. This approach guarantees user biometric data protection, privacy, and security while complying with GDPR.

Recommendations for law practitioners. The use of biometric data for processing must be lawful and under the user's control. However, the current conditions of biometric services often involve data collection and intensive use, which goes against GDPR Article 9(1). The user should be the main element in determining the lawfulness of the treatment of their data. It is disingenuous to force users to accept the processing of their biometric data by default, as it violates their right to privacy and security. Users should have the ability to configure their settings and reject unwanted advertising. This is essential for protecting a person's liberty and right to be secure in a digital environment encircled by the GDPR's framework for automatic processing. The manuscript argues that there is a risk of confusion when it comes to a person's rights regarding biometrically digitized tools. Specifically, the GDPR Article 9(1) does not apply to the protection of a person using a personal device with biometric functionality for two reasons. Firstly, when people exercise their rights under Article 6, Charter of the Fundamental Rights of the European Union, they make decisions related to purely personal activity. Secondly, a biometric is not involved in processing such a device. Therefore, the legal regime applicable to biometric identification is confined by the mode of storage used.

The research identifies two different legal protections that may apply depending on the storage of the device where biometric data is processed. Firstly, suppose the biometric tool is integrated into a smartphone and operates autonomously in an enclave that is not accessible from the outside. In that case, it may fall outside the scope of the GDPR as it applies to the automated processing of personal data. However, for this exemption to apply, the biometric data must remain in the control of the person concerned and meet certain criteria, such as being used for private purposes, being encrypted, and transmitted to indicate the success or failure of biometric authentication. Secondly, suppose the biometric device of the smartphone interacts with remote servers where the biometric template is stored. In that case, authorization from the CNIL or else body respectively is necessary to set up this type of device. This type of biometric device does not benefit from the exemption since the control of the biometric template is delegated to a third party. As the risks for the data subject are higher, authorization from the CNIL or another body is also necessary to ensure appropriate technical measures are taken to protect the confidentiality of the biometric templates. However, it is important to document that both types of biometric devices in smartphones present significant risks to the privacy of the persons concerned, as biometric data is not immune to hacking, whether it is stowed on a smartphone or a remote server.

[27] Ashish Dabas, Shalini Bhadola, and Kirti Bhatia, "Storage of Biometric Data in Database," *International Journal of Trend in Scientific Research and Development* 3, no. 3 (2019): 1001, http://dx.doi.org/10.31142/ijtsrd23146.

Acknowledgement. The authors would like to express their deepest gratitude for the fact that the related to this manuscript research on "The Case Study about Facial ALICEM Identification under GDPR Article 9(2, g)" was presented for the 9th International Ph.D. and Young Researchers Conference "Everything You Always Wanted to Know About Law (But Afraid to Ask)" at Vilnius University, Faculty of Law, Vilnius, Lithuania, 2-3 June 2022.

Bibliography

Law

European Parliament and the Council. "Regulation (EU) 2016/679 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)." *Official Journal of the European Union. Law* 119/1 (4 May 2016).

France. Council of State. Decree n° 2019-452 of 13 May 2019, authorizing the creation of electronic identification means called "Certified online authentication on mobile." *Authenticated Official Electronic Journal* 0113 (16 May 2019).

France. Council of State. 10th - 9th chambers combined, Case No. 432656; ECLI:FR:CECHR:2020:432656.20201104, 4 November 2020.

France. National Commission for Informatics and Liberty. Deliberation n° 2018-342 of 18 October 2018. *Authenticated Electronic Official Journal* 0113 (16 May 2019).

Special literature

Amankwaa, Aaron Opoku. "Trends in Forensic DNA Database: Transnational Exchange of DNA Data." *Forensic Sciences Research* 5, no. 1 (2020): 8–14. https://doi.org/10.1080/20961790.2019.1565651.

Dabas, Ashish, Shalini Bhadola, and Kirti Bhatia. "Storage of Biometric Data in Database." *International Journal of Trend in Scientific Research and Development* 3, no. 3 (2019): 1001–4. https://doi.org/10.31142/ijtsrd23146.

Hermstrüwer, Yoan. "Contracting around Privacy: The (Behavioral) Law and Economics of Consent and Big Data." *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 8 (2017): 9–26. https://www.jipitec.eu/issues/jipitec-8-1-2017/4529/JIPITEC_8_1_2017_Hermstruewer.pdf.

Hildebrandt, Mireille. "Law as Information in the Era of Data-Driven Agency: Law as Information." *Modern Law Review* 79, no. 1 (2016): 1–30. https://doi.org/10.1111/1468-2230.12165.

Kamarinou, Dimitra, Christopher Millard, and Jatinder Singh. "Machine Learning with Personal Data." Queen Mary School of Law Legal Studies Research Paper 247/2016, November 7, 2016.

Krausová, Alžběta. "Online Behavior Recognition: Can We Consider It Biometric Data Under GDPR?" *Masaryk University Journal of Law and Technology* 12, no. 2 (2018): 161–78. https://doi.org/10.5817/MUJLT2018-2-3.

Krivogin, Maxim. "Peculiarities of Legal Regulating Biometric Personal Data." *Law. Journal of the Higher School of Economics* no. 2 (2017): 80–89.

Macenaite, Milda. "The 'Riskification' of European Data Protection Law through a Two-Fold Shift." *European Journal of Risk Regulation* 8, no. 3 (2017): 506–40. https://doi.org/10.1017/err.2017.40.

Milaj, Jonida. "Privacy, Surveillance, and the Proportionality Principle: The Need for a Method of Assessing Privacy Implications of Technologies Used for Surveillance." *International Review of Law, Computers & Technology* 30, no. 3 (2016): 115–30. https://doi.org/10.1080/13600869.2015.1076993.

Schneider, Giulia. "Health Data Pools under European Policy and Data Protection Law: Research as a New Efficiency Defence?" *Journal of Intellectual Property, Information Technology, and Electronic Commerce Law* 11 (2020): 49–67.

Wang Han, Sarah, and Abu Bakar Munir. "Practitioner's Corner · Information Security Technology – Personal Information Security Specification: China's Version of the GDPR?" *European Data Protection Law Review* 4, no. 4 (2018): 535–41. https://doi.org/10.21552/edpl/2018/4/19.

Zhao, Bo, and Jeanne Mifsud Bonnici. "Protecting EU Citizens' Personal Data in China: a Reality or a Fantasy?" *International Journal of Law and Information Technology* 24, no. 2 (2016): 128–50. https://doi.org/10.1093/ijlit/eaw001.

Булгакова Д. А., Булгакова В. А.

ВІДПОВІДНІСТЬ ПРАКТИКИ ФРАНЦІЇ ЩОДО ОБРОБКИ ДАНИХ ОБЛИЧЧЯ ПАРАГРАФУ 2 (a), (g) СТАТТІ 9 ЗАГАЛЬНОГО РЕГЛАМЕНТУ ПРО ЗАХИСТ ДАНИХ ЄВРОПЕЙСЬКОГО СОЮЗУ

У цифрових екосистемах правосуб'єктність фізичних осіб має вирішальне значення, а біометричні системи відіграють життєво важливу роль у перевірці особи впродовж усього життя. Однак ці системи також становлять значні ризики і потребують відповідального використання. Європейський Союз розробив цифрову стратегію для створення надійної та безпечної цифрової ідентифікації, що встановлює глобальний стандарт технологічного розвитку в галузі ідентифікації. Відповідно до параграфа 1 ст. 9 Загального регламенту про захист даних (General Data Protection Regulation, GDPR), країни-члени повинні обґрунтовувати будь-які винятки з цього правила. Франція відіграє провідну роль у легальному використанні унікальної ідентифікації та впровадженні цифрових атрибутів, як-от розпізнавання обличчя через додаток Alicem на смартфонах для підтвердження достовірності особи в цифровому середовищі, що також вдосконалює електронні послуги. Загальний регламент про захист даних (GDPR) у параграфі 1 ст. 9 забороняє біометричну обробку, однак дає можливість країнам-учасницям згідно з параграфом 4 ст. 9 робити винятки з урахуванням умов, зазначених у параграфі 2 ст. 9 щодо випадків можливості уникнення такої заборони. Тому в цьому дослідженні проаналізовано відповідність практики Франції умовам, викладеним у пп. (a), (g) параграфа 2 ст. 9

Загального регламенту про захист даних (GDPR). Зокрема, ретельно вивчено проблематику законодавства Франції, а саме Декрет № 2019-452 від 13 травня 2019 р., який дозволив створення засобів електронної ідентифікації під назвою «Сертифікована онлайн-автентифікація на мобільних пристроях» (Authentification en ligne certifiée sur mobile (ALICEM)), тобто використання унікальної ідентифікації завдяки розпізнаванню обличчя осіб, які користуються додатком Alicem. Зважаючи на це, у дослідженні розглянуто два критично важливих питання. По-перше, чи отримує система Alicem згоду користувачів на обробку їхніх біометричних даних? По-друге, чи є використання технології розпізнавання облич для надання державних послуг необхідним засобом досягнення поставленої мети ідентифікувати користувача електронного сервісу?

У результаті дослідження було визначено п'ять ключових елементів практики додатка Alicem у Франції:

1. Задоволення суспільних інтересів. Обробка біометричних даних, яку здійснює Alicem, є публічним впровадженням, що означає, що вона призначена для надання послуги, яка відповідає суспільним інтересам. У цьому випадку такою послугою є надання електронного підтвердження особи, що дає змогу користувачам ідентифікувати себе в цифровому вигляді та автентифікувати себе за допомогою термінального обладнання, оснащеного контактним зчитувальним пристроєм статичної та динамічної системи розпізнавання обличчя.

2. Вільна згода. Людина дає дозвіл на обробку біометричних даних. Це означає, що користувачі не зобов'язані використовувати Alicem, у них є вибір – погоджуватися чи ні надавати свої біометричні дані для сервісу. Такий підхід відповідає вимогам GDPR стосовно того, що згода має бути вільною, конкретною, поінформованою та однозначною.

3. Повага до людської гідності. Дослідження показало, що Alicem поважає людську гідність завдяки надійності й точності використовуваного алгоритму. Це означає, що технологію розроблено так, щоб мінімізувати ризик помилкових ідентифікацій, які потенційно можуть завдати шкоди репутації або гідності людини.

4. Контроль користувача. Alicem встановлюється на мобільний пристрій користувача за допомогою провідної технологічної інтегрованої платформи, програмованої під егідою ANTS (Agence Nationale des Titres Sécurisés), що дає змогу користувачеві здійснювати ексклюзивний контроль над зберіганням даних. Це означає, що користувачі мають повний контроль над своїми біометричними даними і можуть видалити їх у будь-який час.

5. Необхідність і пропорційність. Дослідження показало, що обробка біометричних даних компанією Alicem є необхідною та пропорційною меті сервісу. Метою послуги є надання можливості французьким та іноземним громадянам ідентифікувати себе в електронному вигляді, що є законним суспільним інтересом. У дослідженні зроблено висновок, що розрізнення облич є пропорційним засобом досягнення цієї мети.

Отже, Франція зробила кроки для впровадження положень пп. (a), (g) параграфа 2 ст. 9 GDPR, що стосуються обробки виняткових персональних даних, приділяючи особливу увагу технології розпізнавання облич. Ця технологія була корисною для забезпечення безпечного та ефективного доступу до електронних послуг, але Франція повинна гарантувати дотримання вимог законодавства та захист унікальних даних осіб за допомогою необхідних технічних та організаційних заходів. Тому в дослідженні визначено кілька умов, які потрібно виконати для відповідального використання обробки біометричних даних. По-перше, потрібно провести оцінювання необхідності обробки біометричних даних з урахуванням принципу пропорційності, особливо щодо біометричних даних. По-друге, національне законодавство має додатково обмежувати обробку біометричних характеристик через їхній вплив на людську гідність. По-третє, національне законодавство повинно забороняти комерціалізацію елементів людського тіла, оскільки біометричні технології може бути використано для експлуатації їх з метою отримання фінансової вигоди. Зрештою, біометричні технології для ідентифікації потрібно використовувати лише в крайньому разі, коли інші методи ідентифікації є неефективними. Тож дослідження рекомендує країнам-членам ЄС зважати на конкретні потреби та занепокоєння своїх громадян, оскільки дуже важливо збалансувати переваги біометричних систем із ризиками для захисту персональних даних, гарантуючи, що відповідальне використання таких даних сприятиме створенню безпечної та надійної цифрової екосистеми.

Ключові слова: біометричні дані, розпізнавання людини, оцифрована особа, унікальна ідентифікація, додаток Alicem.

Manuscript received 04.03.2023