DOI: https://doi.org/10.21564/2707-7039.1.275645
UDC 342.7

Daria Bulgakova*

UNIQUE HUMAN IDENTIFICATION UNDER THE GDPR ARTICLE 9 (1) (2)

I. The Regulation of Biometric Data Processing

Personal data is any information relating to a data subject – identified or identifiable natural person.[1] Digital identity is a specific factor that makes a person identifiable in digital environment. Such a result of mechanical recognition is precisely used in biometric systems. EU legally formed one of the world's largest biometric databases when in April 2019 the European Parliament approved the Common Identity Repository.[2] According to international standards, biometric data processing is interpreted as a database with matching template to tendered data willing to determine uniqueness and, if appropriate, identify the person concerned. Human samples are compared with the database of control templates, and programs have decided which has the most significant degree of similarity to achieve unique human identification. Depending on the result obtained, a final decision is made about whether a particular person is identifiable.[3]

During the development of regulation for the processing of biometric data, in the EU established the Working Group on the Protection of Individuals concerning the Processing of Personal Data (A29/A29WP) with the status of an advisory body that is acted as an independent structure.[4] A29 issued a Working document on biometrics[5] that played an

* Daria Bulgakova, Doctor of Laws, PhD in International Law; Visiting Scholar at the Department of Law, Uppsala University (Sweden). The author is thankful for the scientific environment and financial support given at Uppsala University
Булгакова Дар'я Анатоліївна, доктор права, доктор філософії з міжнародного права; запрошений науковець Департаменту права, Уппсальський Університет (Швеція). Автор висловлює подяку за наукове середовище та фінансову підтримку при Уппсальському Університеті.
e-mail: dariabulgakova@yahoo.com
ORCID ID: https://orcid.org/0000-0002-8640-3622

[1] Convention 108+, Article 2 (a).

[2] European Commission, Feasibility Study of a Common Identity Repository (CIR), Management Summary, Brussels, (December 2017).

[3] Asaf Lubin, "The Liberty to Spy," *Harvard International Law Journal* 61, no. 1 (2020): 185–243.

[4] The A29WP was established according to Article 29 of Directive 95/46/EC, and inter-alia, on its own initiative, makes recommendations on all matters relating to data protection. A29 acts independently and composes to be a representative of the national Data Protection Authorities (DPAs) in Member-States, a representative of the European Data Protection Supervisor, and a representative of the Commission's visions on a targeted matter. On 25 May 2018, the A29WP ceased and was replaced by the European Data Protection Board. All documents issued by the former body are still applied, and they remain available at http://ec.europa.eu/justice/article-29/documentation/index_en.htm (last visited 1 July, 2022).

[5] A29, Working Document on Biometrics, On the Protection of Individuals with Regard to The Processing of Personal Data, 1 August 2003.

integral role in the legislative persuasion of unique human identification about who is identifiable and what data is placed for that purpose. In the view of the study, that document helps to provide a relevant regulation for biometric data processing and contributes to the application of data protection regulation overly for the best human advocacy. It is settled a standard for understanding of how the unique identification process guards biometric data processing. It is explained that biometric data, by its very nature, provides information about a human being to unique characteristics accordingly and, therefore, can always be considered as information directly relating to a natural person. Moreover, a study states that biometric identification is the automatic process when the person is identifiable by own biological attributes. Since biometric characteristics could be used for identification, authentication, or verification purposes, the data subject may be distinguished as a particular person from others by its unique identification essence.

In modern EU law, the institution of biometric data – a subset of personal information – is a particular category of personal data that requires the implication of a specific legal consciousness under the core of the General Data Protection Regulation (GDPR),[6] which is in Article 9 (1) (2) cognizes the processing of biometric data for the purpose of unique identification and equates it to a specific personal data subtype. Under that, a study is aiming for the legal protection of a person because a unique identifier is vital for a human's official digital existence. Among other things, it was completed Directive 95/46/EC. Directive is the first particular EU legal act dedicated to the processing protection of personal biometric data under the right to personal data protection (RPDP), and laid down rules to fulfill the protection of biometrics for the prevention, detection offenses and related unlawful activities. Nevertheless, this document is not binding for the implementation by Member-States and did not have an international effect, as is the case of GDPR; its goals did a foundation for the free circulation of personal data between the EU Member-States within the framework of the functioning of the internal market and the effective guarantee of the RPDP.

The GDPR Article 9 (1) (2) is a binding stipulation that is characterized by the consolidation as a fundamental and inalienable right of individuals at the level of primary law in the founding of EU Treaties, Lisbon Treaty, and the Charter of Fundamental Rights of the EU (CFREU). A mentioned article is challenged from the time as the affair about not excessive data processing within the automated action is weighed up. This matter is starting to be vital for the Council of Europe, which has issued Convention 108;[7] this document was

[6] Regulation (EU) 2016/679 of the European Parliament and 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), OJEU L 119/1 (2016).

[7] Council of Europe, Amendments to the Convention for the Protection of Individuals regarding Automatic Processing of Personal Data (ETS No. 108) adopted by the Committee of Ministers in Strasbourg (15 June 1999); Council of Europe, Additional Protocol to the Convention for the protection of individuals regarding the automatic processing of personal data, regarding supervisory authorities, CETS No. 181, 2001. The research is turning attention, this Protocol is no longer applied as its provisions have been updated and integrated into Convention 108+.

amended in 2018 to the Modernized Convention/Convention 108+[8] and up to this day is the only international legally binding document on data protection law. The same as in GDPR Article 9, data with biometric nature recognized explicitly under the special categories under the Convention 108+ Article 6 when biometric framed to be for unique human identification. Aware fact, human data is processed with the dedication of biometric techniques, and Convention 108+ is the only international act applicable to cover this operation. Within the framework of Convention 108+, there is much notable 18 January 2021 – the date of adoption of Guidelines on Facial Recognition.[9] The supervision for compliance is held by the activity of the European Data Protection Supervisor. Also, an essential novel in the studied area of law is the formation an independent supervisory body, the European Commissioner for Data Protection, and the creation of the European Agency for Network and Information Security. In 2019 under the Regulation (EU) 2019/881[10] this institution was updated by the creation of ENISA. Nevertheless, this body does not entirely specialize in biometrics as the A29 does, and symbolized significant changes in the legislation in the face of biometric environment caused by new technologies.[11] An academic Paul Lambert[12] ponders the necessity to ensure the protection of every natural person on the territory of the participating countries, regardless of citizenship or place of residence, in particular the right to personal secrecy and data protection due to the risky biometric-tech occupation.

Human characteristics factors and the ultimate recognition result are precisely and overcome used in biometric systems. Biometric outcome includes fragmented human characteristics that are more mangled than the former biological characteristics or their representation. That issue has found its result in the one of the democratic groundworks – civil initiative[13] that, among other things, has been realized for the first time from all the

[8] Amending Protocol to the Convention for the Protection of Individuals with Regard to the Processing of Personal Data, adopted by the Committee of Ministers at its 128th Session in Elsinore on 18 May 2018 and Adopting Modernised Convention (Convention 108+) for The Protection of Individuals with Regard to Automatic Processing of Personal Data (128th Session of the Committee of Ministers, Denmark, 17–18 May 2018).

[9] 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).

[10] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (The European Union Agency for Cybersecurity) and Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) NO 526/2013 (Cybersecurity Act), L 151/15 OJEU (2019).

[11] Jörg Ukrow, "Practitioner's Corner ·Data Protection without Frontiers? On the Relationship between EU GDPR and Amended CoE Convention 108," *European Data Protection Law Review (Internet)* 4, no. 2 (2018): 239–47.

[12] Paul Lambert, *Understanding the New European Data Protection Rules* (Auerbach Publications, CRC Press, 2018).

[13] TFEU, Article 24; Regulation (EU) No. 211/2011 of the European Parliament and of the Council of 11 February 2011 on the Civil Initiative; *See more* at https://europa.eu/citizens-initiative/faq_en (last visited 1 July, 2022).

time of personal data protection regulation. In 2020 EU citizens initiated legal action for a ban on use biometric technology and further unique human identification. Initiative asks the Commission to "act against the inherently disproportionate and unlawful practice of using biometric technologies."[14] On 7 January 2021, the Commission implemented Decision[15] to register mentioned initiative. Currently, it was given time to prepare some proposals from citizens of the EU about new legal acts in the sphere of biometric vision.[16]

Thus, the legal regulation in a rapidly evolving digital environment and needs constant improvement to ensure the consistency of existing rules and the effective exercise of the RPDP. And here, the research draws attention to the development of the digital right of individuals to the process of biometric data that reveals human nature. Hence, for the first time, the GDPR grants to an individual adequate legal data protection in the field of biometric when, among other things, any person who has suffered material or non-material damage has the right to receive compensation from the controller or processor for the damage caused. The significant innovation is that the regulation contains an extensively updated terminology based on the technology practice, achieving the regulation technology neutral. Furthermore, the legal core is about the determined framework, whereas the processing is possible when strictly necessary and when the processing of such data is allowed only if it is permitted by the legal acts of the Union or the legislation of the Member States, and solely for the vital interests' protection of natural persons.

II. A Subject and Object for the Protection

1. A Subject of Unique Identification

The critical element in legal relations concerning biometric data processing is its subject. The ability of an individual to be a subject of biometric data arises from birth. [17] The mother's data on the woman's pregnant exchange card identifies the newborn. Therefore, individuals are subjected to the informational capacity for unique human identification from birth.[18]

[14] Civil Society Initiative for a Ban on Biometric Mass Surveillance Practices, para 2. – Draft legal act, the principle of proportionality became a legal ground to justify the practice of biometric technology in EU, where it is stated: "Based on the competence attributed to the EU by Article 16(2) and/or Article 114 TFEU, we call on the Commission to adopt a legislative proposal under secondary EU law for binding rules which – building on and with full respect for the general safeguards in the GDPR and LED – would explicitly prohibit the use of biometric data for identification, recognition (including of emotions), profiling, prediction and any related purpose, in public or publicly-accessible spaces (including online spaces) because this leads to inherently unnecessary and disproportionate mass surveillance."

[15] Decision (EU) 2021/27 of 7 January 2021 on the request for registration of the European citizens' initiative entitled "Civil society initiative for a ban on biometric mass surveillance practices" (notified under document C (2021) 32), OJEU, L13/1Б, 15 January 2021.

[16] Ibid, 5, 8.

[17] See Albin Dearing, *"*Human Dignity: The Right to Be a Person*," in Justice for Victims of Crime: Human Dignity as the Foundation of Criminal Justice in Europe* (Cham: Springer, 2017), 139–292.

[18] The Committee of Ministers to the Member States, Recommendations 6 on the Research on Biological Materials of Human Origin (11 May, 2016).

The subject of biometric data is a natural person whose unique characteristics are processed; an individual, a person that is a participant in legal relations concerning automotive processing. This concept covers EU citizens, the citizens of third countries, and stateless persons in the EU legally. Human's data is processed by automatic tech with respect to any action or set of actions, such as collection, registration, accumulation, storage, adaptation, change, renewal, use, distribution, implementation, transfer, depersonalization, destruction of biometric data, including the use of information by automated systems.[19] From research discovery, recognition leads to consider a person as a re-presenter of a human being with unique characteristics.[20] Since biometric data is vital information, and its processing belongs to the main types of information activities, biometrics' relationship includes a person subjected to act as an informative element because biometric characteristic is a source taken from the human body. Thus, an individual receives the subject data status within its unique identification procedure when a person's status differs in two ways. First, since biometric processing provides unique information, the person is a mandatory participant in such legal links, without whom biometric processing outcome – unique identification – cannot occur. Secondly, a biometric data subject is endowed with personal non-property rights.[21] Therefore, in the view of the study, biometric data processing could endow a person's credentials similar to the subject of civil ties with its personality and legal capacities.

From a modern point of view, the consideration of a biometric data subject is running to be with a new means based on the developed Quantified-Self Status (QSS).[22] It is because the GDPR imposes constraints on collecting and disseminating personally identifiable information.[23] However, this distinction is conflicting, correlating with challenges of the freedom to act in matched identification and to respect human dignity value. It means, each individual is free to decide who a person is and what to do with part of the body.[24] Thus, the protection must ensure the person is free to develop personality to the fullest.

A prohibition to process biometrics is an element of the GDPR that causes QSS conflict. The legal status of a person leads to freedom restrictions.[25] A person is free to act as a socially

[19] European Parliament and the Council, Directive (EU) 2016/1148 concerning Measures for a High Common Level of Security of Network and Information Systems across the Union, OJEU, L 194/1 (2016).
[20] Massimo Leone, "From Fingers to Faces: Visual Semiotics and Digital Forensics," *International Journal for the Semiotics of Law = Revue Internationale De Sémiotique Juridique* 34, no. 2 (2021): 579–99.
[21] TFEU, Article 16.
[22] See John Danaher, Sven Niholm, and Brian D. Earp, "The Benefits and Risks of Quantified Relationship Technologies: Response to Open Peer Commentaries on 'the Quantified Relationship'," *American Journal of Bioethics* 18 (2018): W3 – W6.
[23] Dominik Leibenger, et al., "Privacy Challenges in the Quantified Self Movement – an EU Perspective," *Proceedings on Privacy Enhancing Technologies* 2016, no. 4 (2016): 315–34.
[24] Edward J. Eberle, "Observations on the Development of Human Dignity and Personality in German Constitutional Law: An Overview," *The Liverpool Law Review* 33, no. 3 (2012): 201–33.
[25] Regulation (EU) 2018/1725, Article 25.

valuable unit with respect to biological nature.[26] Under those argues, a person – a party of legal relationship concerning biometric data processing – is an autonomous one who can decide what to let others know about whether human data would or would not be available for the machine processing.[27] It is the case when specific data of a person is limited to be shared by the automotive means with other persons.[28] Resembling the QSS, a person is involved in two puzzles while interacting with biometric technology a) what do parties say that individuals should do, and b) what do other people do in the same position.[29] Questions must be solved by what is lawful.

The case law[30] has developed proportionality criteria for the "lawful justification," especially regarding to the restriction of fundamental rights and interference with data protection. Among criteria are 1) interference is following the law, 2) a legitimate aim, 3) the intervention is necessary for a democratic society. In the view of the study, biometric recognition interferes with fundamental right to data protection and may be regarded as proportionate only if the disadvantages caused are not disproportionate to the aims pursued but leave the open debate about values that must prevail in a democratic society and, kind of (digital) society to live in. It is a cloverleaf of social forces for quantification with its personification manner of the unique identification to the physical, physiological, and behavioral characteristics accordingly.[31] For example, to check from a distance whether the actual user of the chipcard is lawful holder, – biometrics that facilitates privacy friendly applications with the decentralized storage of a single biometric detail on a single chipcard placed in the hands of the person from whom the biometric detail originates, – "lawful" solution. The other extreme consists storage of biometric data in a single central file for online "lawful" status check of people's identities. Central in this context means that all stored biometric details can be directly accessed and compared with each other and can be physically concentrated at the exact location (but this is optional). This central approach makes it possible to perform additional checks only when it would not be possible with separate chipcards alone. For example, the administrator of a central file of biometric images

[26] The Committee of Ministers to the Member States, Recommendations 4 on the Research on Biological Materials of Human Origin, Explanatory Memorandum (2006).

[27] See A. Reis Monteiro, "Human Dignity Principle," in *Ethics of Human Rights* (Springer International Publishing, 2014), 199–236.

[28] Minke D. Reijneveld, "Quantified Self, Freedom, and the GDPR," *SCRIPT-Ed* 14, no. 2 (2017): 285–325.

[29] Ibid, 301.

[30]For example, Case C-275/06, Productores de Música de España (Promusicae) v Telefónica de España SAU, ECLI:EU:C:2008:54, para 68.

[31] It acknowledged that human characteristics are needed for biometric recognition, including physical and physiological properties (fingerprint, face, or iris) and behavioral properties (voice, gait, signature). The difference between physiological and physical features could be exceptionally bright. Most specialists in biometric recognition solely refer to pair varieties, either bodily and behavioral, oppositely physiological, and behavioral. Others render the corresponding models for physical and physiological like fingerprints, palm geometry, face, and palm geometry.

can immediately establish whether a person is already included in the file but under a different name. The distinction between central/decentralized has legal importance because central storage involves interference with else fundamental right to privacy.

To properly understand the subject of unique identification, a study proposes to distinguish between a person-related detail derived from the body and a personal detail traced back to a person. An anonymous biometric characteristic detached from biometric template without anything in common with the source, – cannot be regarded as a personal detail because it cannot be traced back to the person from whom the measured value originated, or this can only be done with a disproportionate effort. An example is left (after person's consuming) glassware in a restaurant. It is a hopeless task to trace a fingerprint on one of the glasses to a restaurant diner who has already left. A personal biometric characteristic is, therefore, person-related but is not necessarily a personal detail. The decisive factor regarding the legal position of a biometric detail is whether it can be traced back to the right person. To this extend, it is necessary look at all surrounding technical, procedural, and organizational provisions. Therefore, suppose a biometric detail is anonymous, in that case, its use does not fall within the constraints set by data protection legislation for personal data because there are no legal obstacles to anonymous biometrics use. Moreover, a biometric (personal) detail does not lose its anonymous character for a verification if the authority – e.g. the card issuing authority – knows precisely whom the person concerned is but may only reveal a person-related detail with the biometric application confirmation. Many biometric applications do, however, use biometrics registered in people's names (personalized biometrics), even if the purpose of the application can be achieved just as well with anonymous biometrics. Under the study, biometrics will not realize its full social significance until the legislator recognizes and utilizes the wide-ranging possibilities offered by the anonymous use of biometrics.

2. An Object of the Biometric Data Processing

Moving on to the following problem assessment of biometric data as an object for the protection, a study refers to the argument that biometrics is personal data resulting from the remarkable technical processing of the biological characteristics of a natural person.[32] Present EU law defines biometric into three legal categories.[33] The first category includes information concerning physical characteristics, and physiological features are in the second category. The third category prescribes data related to human behavior, such as any behavioral characteristics of a person that is unique, therefore making it possible to identify a particular

[32] See Worku Gedefa Urgessa, "The Feasibility of Applying EU Data Protection Law to Biological Materials: Challenging Data as Exclusively Informational," *Journal of Intellectual Property, Information Technology, and Electronic Commerce Law* 7 (2) (2016): 96–109.

[33] GDPR, Article 4 (14) established the definition of biometric data as follows: "Personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data."

person. Furthermore, the headway prohibits biometric data processing based on the GDPR Article 9 (1), despite that, the following power of GDPR Article 9 (2) allows it. At the same time, CFREU is a significant legal tool for defending a biometric ban within the execution of the right to personal data protection.[34] An Article 52 of the CFREU ensures the application of the principle of proportionality on the right to personal data protection. Moreover, the GDPR also predicaments that each personal data shall be processed to the principle of proportionality application accordingly.[35]

Therefore, a study proposes to apply one of proportionality criteria to comply with the processing operation. Among them are specified purpose and balance of competing interests. In the view of the study, the mentioned criteria are assured along with the GDPR Articles 5, 6, and 51. Under that stipulation, biometric data is required to be processed (1) lawfully, fairly, and transparently; (2) specifically, explicitly; (3) be limited; (4) secure; (5) accurate and accountable. Thus, the processing requires strict examination of the specific criteria because it legitimizes biometric data processing especially when, for example, the processing is necessary for a substantial public interest, based on Union or Member State law which shall be proportionate to the aim pursued.[36] In turn, DPAs weave its Opinion[37] about required strict review of biometric use according to the principle of proportionality measurement. The processors, party of the legal relationship concerning biometric data processing (together with biometric data subject) would, therefore, in the view of the study, have difficulties demonstrating that the processing of biometric data is necessary for unique identification. It is vital because the necessity criterion is a pre-condition for the proportionality assessment.[38] A legitimate aim is the next step further to eliminate proportionality.[39] In this regard, the necessity to achieve the purpose dictated by the proportionality application must be understood as a legitimate ground for such processing.

However, the different meanings of unique identification (that is purpose) for biometric processing have an exact and narrow sense. The digital identity connected to biometric recognition does not establish civil or juridical identity. It proves the identity of the self by matching a biometric characteristic previously saved in biometric templates. It only discovers

[34] Maja Brkan, "The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors," *Maastricht Journal of European and Company Law* 23 (5) (2016): 812–41.
[35] GDPR, Recital 4.
[36] GDPR, Article 9 (2, g).
[37] CBPL, Opinion N°17 on biometric data, in particular, the section "Rechtmatigheid en proportionaliteit"/"La légitimité et la proportionnalité," analyses risks for the data subjects (pp. 12–13) having a reference to the essential requirement that shall strictly review the proportionality and justify biometric data systems (p. 14) with examples introduced (pp. 17–19).
[38] Regulation (EU) 2019/881.
[39] CFREU, Article 52 (3) states: "[i]n so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law from providing more extensive protection."

that neither sample/template matches an identical person's human characteristics.[40] Unique processing is attributable to a single individual by a biometric identifier(s).[41] Therefore, the law should regulate biometric functions depending on the processing techniques. While prohibition on processing is outlined in GDPR Article 9 (1) but it does not distinguish between one-to-one (1:1) biometric comparisons (i.e., verification) and one-to-many (1:n) comparisons (i.e., identification),[42] and other way around refers to two functionalities "which allow or confirm"[43] the unique identification.

Since studied article forbids biometric data processing only "to uniquely identify," it is leaving uncertain if this prohibition is also applied to the processing by biometrically based technologies that confirm identification regardless of the verification or authentication.[44] The verification is used to increase an authentication method defending who a person is through biometric characteristics to something an individual possesses (likewise, embedded in a token or intelligent card) and to something a person prizes (likewise, biometric ID).[45] The differentiation is an exception to process human characteristics for the identity recognition need. Therefore, that distinguishing needs to be clarified from a legal perspective. Authentication is used to identify uniquely, and the difference is only in the comparison methods by biometric-based technology.[46] Identity verification is regularly asked for the authentication because it is employed as an analog of verification. Thus, the verification is used to authenticate the person by uniquely identifying who the person is in the system. However, in the view of the study, it is insufficient to use biometric systems for such confirmation as the functionality trailed contrary to the identification merely the averages of authentication that should be circumvented. This is also essential for the processing accuracy because it brings us to the essence of biometric systems; likewise, GDPR Recital 51 specifies authentication in defiance of unique identification.

Therefore, the study proposes to make two distinctions. The first is identification, or verification relating to the envisaged knowledge concerning a person's identity with two alternatives: 1) establishing precisely who someone is (identification); 2) establishing whether a person is a right person, for instance, the same person as expected (verification). Establishing a person's true identity involves an investigation into someone's identity. It is deemed sufficient to establish whether a person is the same person as expected, by ascertaining whether several pieces of human characteristics belong to the same person.

[40] A29, Opinion 3/2012 (n 8) 5.
[41] ISO/IEC 2382–37 (n 24), Term 37.08.03.
[42] Els Kindt, "A First Attempt at Regulating Biometric Data in the European Union," *Regulating Biometrics: Global Approaches and Urgent Questions* (2020): 66.
[43] GDPR Article 4 (14).
[44] European Data Protection Supervisor and Agencia Espanola Proteccion Datos, Joint Paper on 14 Misunderstandings with regard to Biometric Identification and Authentication, June 2020.
[45] Els Kind, "The Processing of Biometric Data, A Comparative Legal Analysis Focuses on the Proportionality Principle and Recommendations for a Legal Framework" (PhD diss., 2012), 496.
[46] Ibid.

This is often erroneously referred to as "identification:" in fact, it yields no more than a verification. Verification is less far-reaching than identification when it remains unsure whether a person is whom he says he is. For example, using the person-related character of a biometric detail, it is possible electronically, without human intervention to establish that the same person has arrived and departed without needing to know the exact unique identity of the visitor. And, the second distinction is inclusion and exclusion, which relates to another basic approach for checking someone's identity 1) positively establishing whether someone is indeed the right person. This is referred to as the "inclusive" use of a recognition technique, and 2) negatively establishes that someone is not the right person. This is referred to as the "exclusive" use of a recognition technique. In the actual practice of biometrics, this difference has significant implications, especially when comparing two images of a physical characteristic, for instance, two fingerprints. A single point of difference is to exclude someone with one hundred percent certainty. On the other hand, inclusive use only gives one hundred percent certainty, even though that certainty does of course grow.

Accordingly, the purpose is not to authenticate a person's identity but singularly to verify that.[47] That means the verification is enough to identify a particular human since it must be understood as an acceptable alternative method to recognize a personality without employing uniquely biometric-based techniques.

III. The Protection of a Natural Person Characteristics

1. Biometric Identification to the Processing of Genetic and Health Data Contrasted

The regulatory requirements for the processing of physical, physiological, and behavioral characteristics of a natural person are under the guise of a prohibition norm of the GDPR Article 9 (1) and the permissive norm of the GDPR Article 9 (2). A study considers the processing of biometric data as a separate type; however, it is also referred to the processing in line with "personal data relating to racial or ethnic origin, political opinions, religious or philosophical convictions < … >"[48] That lead do disregard of studied data specific and shall fall under own regime.

Sites search on the pilgrimage, religious books, could be treated as revealing a religious opinion because may remain clear reading interests of a papal encyclical. This also falling under a special category as well as the names of patronymics reveal the racial origin, or any photo of a person buying a bible book on a website can reveal religious beliefs. But it is inconceivable to treat names systematically, and photographs that reveal personal origin because differ from the biometric case. Thereof, considering the means and way of processing, the footage of an individual can only be premeditated as biometric one if it has been specifically and technically processed for the inimitable identification purposed person. As well as, the processing of photographs should not systematically be considered as constituting

[47] The correlation rule is known as "one to one matching" under A29, Opinion 3/2012 (n 9) 6.
[48] GDPR, Article 9 (1).

the processing of special categories of personal data given the fact of being processed according to a common but not biometric technical method.[49]

Hence, based on the GDPR Article 9 (1) (2) and tenacity of Article 4 (14), three criteria must be reputed to differentiate the processing of biometric data from other special categories of personal data. The first criterion is the nature of data dominated by a natural person of physical, physiological, and behavioral characteristics. The second one includes the prescribed "means and way of processing"[50] in the sense of a result from a specific technical processing. Thirdly, it is the purpose of the processing, which is a unique identification of a natural person. The study thinks, having considered each of the criteria indicated and derived by the research, it is possible to assert a specific protection, thereby providing a high legal guarantee for the person whose characteristics are in the crosshair. Thus, referring to the highlighted criteria, the GDPR defines certain specific for biometric in contrast to genetic data and data concerning health. To study further, it is important to find out differences by looking at the subject of those data. According to the GDPR, the data subject is the natural person identified or identifiable by personal data. After all, to obtain neither biometric, genetic, or health data, – a natural person is involved in a particular data outcome, which is not very clear with regard to purposeful processing outcome. Therefore, depending on the processing stage – a different identification result would be obtained, and, therefore, the legal protection should be relevant under a specific target of particular data processing.

Compared biometric to the genetic data, the last allows identifying several people related to an individual's hereditary characteristics or those in a relationship with such characters forming the heritage of a group of related individuals.[51] At the same time, the GDPR defines genetic data as "data of a personal nature relating to the hereditary or acquired genetic characteristics of a person which provide information unique to the physiology or state of health of this natural person and which result, in particular, from an analysis of a biological sample of the natural person in question."[52] In terms of this, a study found that a genetic datum is assimilated to a piece of data relating to the health. Indeed, genetic data is frequently used for health intent. And here, the treatment does not have a medical purpose, but rather an identification aims as an example for the perpetrator of a crime or instance in the context of a paternity action from the father of a child. While some scholars out of law may think this data relates to an infringement, this is not the case in the law. The study removes ambiguity at this level by considering that this data type should be subject to increased protection. The A29WP in this regard states: "one of the fundamental characteristics of genetic data consists of distinctive characteristics marking of an individual with others. In the fact that these data and more precisely characteristics are structurally shared by all

[49] GDPR, Recital 51.
[50] Ibid.
[51] Council of Europe, Recommendation No. R. 5 (97) on the Protection of Medical Data (13 February, 1997); Recommendation on the Protection of Personal Health Data (8 June, 2018).
[52] GDPR, Article 4 (13).

members of the same biological group, while other mechanisms where personal data is shared depend on the data subject, custom, social, or legal rules."[53]

Thus, the question is whether the protection is applied to the singular or plural person concerned. The study presents two possible scenarios. According to the first, family members could be considered as concerned persons having all related data from them "by blood." Another option would be when family members are under personal data protection but under a different nature of data that were processed. Regardless, the guarantees for legal protection under the studied article should be considered to keep various conflicts that may arise between the different demands from family members and either keep it confidential.[54] The last scenario does not correspond to the given GDPR protection of a natural person. To determine whether a natural person is identifiable, and the purpose is going to be achieved, the account should be taken as means reasonably likely to be used to identify the natural person directly or indirectly, such as through targeting.[55]

Assuming, genetic data is not data alike to biometric. It is because particularly genetic data is about genetic characteristics that provide unique information about physiology status or health status, but not about physical, physiological, or behavioral characteristics. Also, the use of processing target results in the sense that genetic data is limited to medical and forensic identification and tends to diverse fields such as insurance, genealogy, marketing, and the fight against immigration.[56] In the view of the study, genetic data is advanced under the concept of medical data and focused on the character of affiliation to a group of individuals or any data baselined to the exchange of genes concerning an individual or a genetic line, but the processing of biometric data characterizes a specific person who is not similar and incomparable with others in terms of belonging. [57] Consequently, the expression of generative data would belong to whole data of the class, which touch the ancestral characteristics of an individual and is correlated to the before-mentioned components composing the heritage of a group of individuals related. However, it is not used to identify as possible with biometric uniquely. Another difference deduced by the study is the processing performance fulfilled by genetic similarities from procreation shared

[53] A29, Genetic Data Discussion Paper, WP 91, p. 8 (17 March, 2004).

[54] Ibid. Italian Data Protection Commission (Garante per la Protezione dei dati personali) granted a lady the possibility to access her father's genetic data even though not granted his consent. It is based in substance on the prevalence of the lady's right over of his father. This request is granted because the father's right to confidentiality could not override the lady's right to health of psychological and physical well-being, Home – Garante privacy en – Garante Privacy (last visited 1 July, 2022).

[55] GDPR, Recital 26.

[56] The French DPA, The National Commission for Information Technology and Civil Liberties, Opinion about Genetic data (2017).

[57] GDPR, Recital 34: "Genetic data should be defined as data of a personal nature relating to the hereditary or acquired genetic characteristics of a natural person, resulting from the analysis of a biological sample of the natural person in question, including analysis of chromosomes, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA), our analysis of another element making it possible to obtain equivalent information."

by two or more individuals. That contradicts biometric identification having only two legally recognized unique features like a human face and fingerprints, and only through which a specific person is recognized, but not through finding similarities or differences with other people like with genetic forward way for the processing.

The GDPR is also defined as secluded data narrating to the physical, and mental constitution of a natural physique, including health anxiety with unveils information roughly the wellness status of this person.[58] Additionally, this definition is broader than what appeared in Directive 95/46/EC because it is neither long spun overlays data reciting the health, but reveals information about the state of health. However, it would not be possible to assert this at the time of the previous directive, because, for instance, the indication of an injured person indoors the sense of provision 8 (1) of the Directive 95/46 following data that amidst a description of a person's health state; likewise, alcohol or drug use are unquestionably intimate data linking to health and ancestral data, in particular, because set down in a medical record.[59]

Therefore, despite the inclusion in studied article of two categories of health data and genetic data into one, this has nothing to do with biometric data, which does not symbolize a medical record and based on the current GDPR appreciation, biometric does not characterize the status of a person acquired from the birth or acquired under the guise of vital activity. The health data, therefore, concerns more general information about a person rather than biometric; and constitutes an individual body status as a whole, but biometric data is focused on a small part of a specific sample from the human. In other words, to be considered biometric data and rightfully implement norms of GDPR Article 9 (1) (2), the processing of data must allow or confirm the unique identification of the person concerned, which is not the case of common technical records for other types of personal data as it was proven with comparison provided above.[60]

2. The Processing of Behavioral Characteristics alike to Biometric

The types of biometric data under the GDPR have included human characteristics like fingerprints and facial features and now also include an individual's behavioral traits. It is important to note here, due to a large number of automatize processing through various types of technologies, in the legal field as well as in the practice of applying the norms of law, discussions are being held about whether a behavioral characteristic of a person is biometric data and, therefore, whether such processing will fall under GDPR Article 9 (1) (2). The study states that only some behavioral characteristics are biometric data. Behavioral

[58] GDPR, Article 4 (15).

[59] A29, Discussion Paper on the Processing of Personal Health-related Data Contained in Electronic Medical Records (EMRs), WP 131, p. 8 (15 February, 2007).

[60] See also Belgian DPA, Hearing of Michel Parisse and Willem De Beuckelaer, President & Vice-president of the Commission for the Protection of Privacy, Camera surveillance, Report, Legislative document No 3–1413 / 1 (2005-2006).

analysis is often in use for commercial purposes such as targeted advertising and unsolicited contact. Some scholars have else opinions, for example, a scholar Krausova[61] claims, data about online behavior fall into the biometric category within the GDPR meaning.[62] Moreover, in the view of the scholar, e-behavior of a person can not only be understood upon biometric profiling but also lead to the biometric data generation while utilizing the internet.[63] Scholar believes, in particular environments, the technique of combining alike to biometric types of data typically happens in multi-modal biometric systems, and it is called information fusion.[64] Especially in the online behavior recognition area, systems might start to utilize various types of data, including activity initiated solely by a device.[65] Such identification based on hybrid data fusion should be considered as biometric data.[66]

However, the study does not agree with the scholar-mentioned consideration mainly because the statements are based on the technical features and do not lead to the natural features of data as it is required for data to be recognized under the GDPR Article 9 (1) (2).[67] Behavioral characteristics in the means of GDPR Article 9 (1) (2) developed throughout life and unique habits subconsciously guide a person; however, behavioral characteristics in the means of the legal regime applicable to profiling are based on the decision – making behavior[68] through the right to automated individual decision-making,[69] i.e., makes a request or a complaint or a demand of some sort. Behavioral activity is different because each person considerably needs to press buttons, and each person creates just applied style as an e-user. In contrast, behavioral biometric is not required and is enough to certify accurate personality. That characteristic may not have disability, injury, or illness. Thus, it is not particularly unique but distinctive to prove a low level of identity and analyze the common type of behavior from a user (consumer) perspective. The same approach could be found with human behavior performance on the internet, whereas companies refer to data analysis.

In this regard, behavioral data is a piece of knowledge about a person's actions coming from human behavior idea that in the age of the internet creates a new challenge and would be esteemed as profiling is. Profiling means "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's

[61] 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.
[62] Ibid, 164.
[63] Ibid.
[64] Ibid, 169.
[65] Ibid.
[66] Ibid.
[67] European Data Protection Board, Guidelines 3/2019, 5.1 "General Consideration when Processing Biometric Data;" See also European Data Protection Board, Guidelines 3/2019 on Processing of Personal Data through Video Devices, para 74, p. 18 (2020).
[68] A29, Guidelines on Automated individual decision-making and Profiling for Regulation 2016/679 adopted on 3 October 2017 and revised on 6 February 2018.
[69] GDPR, Article 22.

performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements."[70] Thus, the applicable legal regime must derogate on this regard since e-behavior indicators do not fall within the means of GDPR Articles 4 (14) and 9 (1) (2) and shall be considered within the means of the GDPR Article 14 (4) and regard with profiling thought that used to target experiences, services, or products like, and to predict consumer preferences and personal opinions.

Traditional biometric and predictive behavioral analytics are a nascent discipline of technological advances. Here they are common because immersive technology uses psychography data to make online service into a popular and profitable enterprise, but not identify a single person through its recognition system as it is a matter in the case of biometrics. These matters involve a disruption to the mental processes because online users are forced to verbalize what they think which might change their thinking.[71] A study agrees, behavioral characteristics are also mere to a user's psychography. Thus, behavior characteristics in the means of common use might be changed and cannot be maintained for long periods; they are permanent and may change significantly over time, when the biometric means cannot change the behavior characteristics. For example, walking style is a biometric characteristic of a person in a complex of human moves. The walking style can be described with a camcorder as a series of movements of several different joints coming from all growing periods of a person's life. But the human performance on the internet may be manipulated by advertising and related only to the personal interests of an individual concerned in the marketing modeling and lead to the self-identity of e-personality. Also, for instance, the signature of each person has a unique way of writing. The signature requires user-side access to physical contact with the writing medium and active participation. A signature is widely accepted as an official identifier in the case of document use. However, even the autographs of the same person differ considerably from each other, and a skillful risk may succeed in deceiving the identification shower system, like it also would be impossible for a person to write an injury or illness situation. Thus, the behavioral characteristics usually lead in to complex behavioral biometrics if even may change over time. However, it is prone to physical and emotional changes in a human being. Based on the stated, the legal regime to regulate unique human identification in the scope of GDPR Article 9 (1) (2) does not apply to behavioral characteristics in the sense of profiling and data acquisition. Those data must be considered as a chain of the elements set necessary to capture data from a machine to its storage for immediate or future use through user profiles which can contain a large amount of behavior actions, including preferences, cookies, user

[70] GDPR, Article 14 (4).

[71] Brittan Heller, "Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law," *Vanderbilt Journal of Entertainment and Technology Law* 23, no. 1 (2021), https://scholarship.law.vanderbilt.edu/jetlaw/vol23/iss1/1.

navigation data, record traces of the user's digital identity, and analyze the contextual information of metadata.[72]

IV. Processing Risk and its Mitigation

1. Commodification Risks

One of the EU's values is respect for human beings to shape Europe's digital future, and taking into account a competitive economy with biometric trade, it will help Europe for "his or her physical and mental integrity"[73] pursue its way towards a digital transformation that works for the benefit of people and respects fundamental values.[74] Biometric characteristics are a part of the human body[75] and it must be respected (a) the free and informed consent of the person concerned,[76] (b) prohibition on making the human body and its parts a source of financial gain.[77] A human-centric approach is a tool to ensure that biometric systems are developed and used in a way that respects European union law and fundamental rights. It is vital to prevent breaches of fundamental rights and if they occur by national authorities. For example, biases in algorithms or training data used to recruit biometric systems would be illegal under EU human rights laws.[78]

Biometric data some time ago was difficult to acquire and process, and it is significantly easier to access now as unique identifiers by advances in technology. The same happened with Social Security Numbers that were never intended to be used as identifiers. However, because everyone has one, after a while, it was legally recognized as an identifier in the governmental and private sectors.[79] Given how sectors and technology spurred the commodification of social security numbers, extensive commercial industry uses biometric on a similar regard. This is compensated when companies or other stakeholders are confident that the e-user, being uniquely identified, is a legitimate user of the web system. At the same time, a user of a biometrically installed system is confident in the security of e-service and on legitimate e-status obtained, because no one except such an individual with particular biometric characteristics will be able to pass a unique identification task to receive the desired service. In this context, a high-quality and safe service is modulated for biometric protection, and a person receives the desired service in return. In this context, the discussion is about the legal lack of digital protection of a human as a user of the biometrically performed service

[72] Indra Spiecker genannt Döhmann et al., "Multi-Country · the Regulation of Commercial Profiling – A Comparative Analysis," *European Data Protection Law Review (Internet)* 2, no. 4 (2016): 535–54.
[73] CFREU, Title 1 DIGNITY, Article 3.
[74] European Commission, Shaping Europe's Digital Future – Questions and Answers, 1, Brussels (19 February 2020).
[75] Rec. (2006) 4 of the Committee of Ministers to Member States on Research on Biological Materials of Human Origin, Explanatory Memorandum.
[76] Ibid.
[77] Ibid.
[78] Ibid.
[79] Carolyn Pucket, "The Story of the Social Security Number," *Social Security Bulletin* 69 (2) (2009): 55–74.

in the context of data cyber commodification practice.[80] Scholars state: "Personal information has been commodified,"[81] because impersonation through standardization has changed.[82] Under Gemeinschaft law, people are related to each other as natural members of a whole,[83] and on the other hand, under Gesellschaft law, individuals are entirely independent of one another and enter into relationships only of their own free will.[84]

Considering biometric data processing to be a voluntary based operation,[85] the economic theory supports these voluntary exchanges so long as they lead to efficient outcomes;[86] and negative externalizations would exist when individuals could choose to disregard their human characteristics by sharing them with data collection companies. Hence, if a company shares a user's biometric, then person's enrollment supports practices that can harm. Under business methods impact, biometric data subject believes that using unique human identification is beneficial relying on convenience and safety functionalities over the potential costs of biological uniqueness. Each human aiming to receive biometrically digitized service cannot avoid this social benefit. Likewise, people usually process biometric data as a security tool, but it could become perverse the more widely it is used. A company that implements biometric tech often considers them as the benefits of improved security and reduced fraud measure.[87] However, the company needs to pass the human' costs imposed. It is either difficult or inefficient to exclude others from having some data, and once it is trended, – it can be used and transferred at no cost. In the face of that, a person may not have a choice to refuse unique identification and exposes to unnecessary security risks when the company is forced to rely on vulnerable and irreplaceable measures.[88] And, data subject bears the cost, which is external to the company, significantly if human data is compromised cause a ripple effect throughout biometric systems (because the same characteristic may be enrolled in multiple systems) that accessed by third parties[89] where an individual's data in those or other systems harmed.

[80] Miriam A. Cherry, "Cyber Commodification," *Maryland Law Review* 72, no. 2 (2013): 381.
[81] Teemu Juutilainen, "Law-Based Commodification of Private Debt," *European Law Journal: Review of European Law in Context* 22, no. 6 (2016): 743–57.
[82] Ibid, 752.
[83] Christian Becker, "Die normativ verweiste Gemeinschaft. Überlegungen zum Schicksal der Ethik im freiheitlichen Rechtsstaat," *Annual Review of Law and Ethics* 27 (2019): 39–54.
[84] Ivo Schwander, "Das Statut der Internationalen Gesellschaft," *Schweizerische Zeitschrift für internationales und europäisches Recht* 12 (1) (2002): 57–77.
[85] GDPR, Article 9 (2, a)
[86] Jena Martin, "Business and Human Rights: What's the Board Got to Do with It?" *University of Illinois Law Review* (2013): 959.
[87] GDPR, Recital 75.
[88] Sara Rosenbaum and Elizabeth Taylor, "The Irreplaceable Program in an Era of Uncertainty," *The Journal of Law, Medicine & Ethics* 46, no. 4 (2018): 883–86.
[89] Fiona Q. Nguyen, "The Standard for Biometric Data Protection," *Journal of Law & Cyber Warfare* 7, no. 1 (2018): 61–84.

Taken the Titanic Phenomenon when the titanic builders were so confident of its stability that they did not have enough lifeboats when the ship sank.[90] The same is valid with biometric: proponents that view the technology as infallible, but biometric systems will fail and, when they do, there will not be adequate safeguards.[91] Economists argue: "when markets fail, intervention is necessary to remedy the parties"[92] misaligned incentives. Hence, biometric would suffer from market failure. The only way to prevent commodification is to live in isolation.[93] Thus, preventing the use of biometric ultimately is hard, but merely justifying intervention expected to build proper legal protection.

Biometric immersive systems essentially make the human body machine-readable[94] and could be used for a statistical rate when companies collect biometric in exchange for goods and services, even without the knowledge of the individuals.[95] Such an expansive view about tradable data goods interpreted "as any part of a person that someone else needs, wants or as values with a price."[96] In the view of the research, it is happening because the "Pareto" efficiency of financial economics[97] exists in a voluntary market transaction where the legitimate interest of both parties is beneficial from the transaction.[98] Applying economic theory to non-market behavior, a metaphorical market of denial or rights deprivation constitutes the autonomous ability to establish a state of inequality among human beings, where everything becomes a market transaction.[99] The voluntary transfer system is presumptively efficient in characterizing biometrics sufficiently to salable or tradable value. This vision treats human attributes, relationships, and social interactions as commodities, and creates a market of human attributes and identities.

Human attributes allow others to recognize when individuals closely aligned identify themselves through these attributes. As such, they are essential for personhood and warrant protection and must be dignity – inalienable because human cannot be restricted from enjoying those biometric characteristics. Likewise, when a person is interacting with biometric technology, using voice, showing faces, and touching things around. People placed

[90] Daniel J. Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security* (New Haven [Conn.]: Yale University Press, 2011).
[91] Ibid.
[92] Joseph Stiglitz, "Regulation and Failure," in *New Perspectives on Regulation*, eds. David Moss and John Cisternino (Cambridge, MA: The Tobin Project, 2009), 11–23.
[93] Aaida Peerani, "The Reasonable Person," *Law Now* 46, no. 1 (2017), https://www.lawnow.org/the-reasonable-person/.
[94] A29, Opinion 3/2012, at 4.
[95] Elizabeth M. Walker, "Biometric Boom: How the Private Sector Commodifies Human Characteristics," *Fordham Intellectual Property, Media & Entertainment Law Journal* 25, no. 3 (2015), https://ir.lawnet.fordham.edu/iplj/vol25/iss3/5.
[96] Thomas Hobbes, *Leviathan* (Oxford University Press, 2009).
[97] Gabrielle Gayer et al., "Pareto Efficiency with Different Beliefs," *The Journal of Legal Studies* 43, no. 2 (2014): 151–71.
[98] Ibid, 152.
[99] Tamara Todorova, "Transaction Costs, Market Failures and Economic Development," *Journal of Advanced Research in Law and Economics* 7, no. 3 (17) (2016): 678–84.

personal and non-monetized value in their fingers, eyes, face, voice, and other attributes. The use of biometric for a variety business purpose creates a risk of monetization of the human characteristics,[100] and therefore must be used legitimately because biometric data is not goods that can be asked for in exchange. Further, as more institutions implement biometric systems, individuals will be left with fewer choices until they must enroll in their characteristics. Furthermore, humans only pay attention to a limited number of things, and inconspicuous items are often ignored. Even if the hidden items' shrouded attributes are important, humans may ignore them, often to a detriment. Thus, even if pay attention to shrouded costs/benefits, a human may undervalue them or fail to recognize them. These human errors are highlighted together with the decision-making act, where costs and benefits are complex and frequently bundled with other items, and individuals need help to evaluate all relevant information relying on simplified models. The same occurs when unique identification is a necessary part for transaction completion. A person may not see or consider only factors with limited information, excluding important items, that leads to sub-optimal decisions regarding biometric profitability. This negligence makes biometric data freely available to the public. Therefore, biometric data is a component of personhood, is a monetization attribute, and detachable from the person-undermines identity.

2. Technical and Organizational Measures

The employment of biometric models designed for people interests and civilization grows serious attention about its influence on the legitimate interest of a biometric data subject, which is seen between dignity, respect, and the right to personal data protection, freedoms in decision – making and digitalization. [101] Profound challenges concern how big data analytics may create such an opaque decision-making environment that individual autonomy is lost in an impenetrable set of algorithms.[102] Hence study finds the critical concern about lack of transparency. Difficulties in understanding biometric tech for natural persons, who did not study that area, make it a problem to analyze all processes. While the complexity of biometric data processing increases, many individuals are aware with appropriate notice and control. However, others are subject to decisions they do not understand and have no control over.[103] People cannot efficiently handle technical control overhead and give essential consent for the processing without legal grounds for using an automated biometric system.

While both forms as biometric samples and templates make possible to identify a particular human, some may argue that the capability to identify is only valid for samples; this is not correct because if technology has a template, it should be possible to perform an

[100] Walker, "Biometric Boom."
[101] Market study report prognosticates that portable biometrics will increase quicker, reaching $49.33 billion over 2022, https://www.marketsandmarkets.com/Market-Reports/next-generation-biometric-technologies-market-697.html (last visited 1 July, 2022).
[102] US, White House Report on Big Data: Seizing Opportunities, Preserving Values, Executive Office of the President, p. 10 (May 2014).
[103] A29, Opinion 3/2013 on Purpose Limitation, Annex 2.

identification by using a raw dataset. This way of identification does not necessarily provide identity information but merely a "hit" that confirms a certain person, whether an individual is on the "green" list or a deny list. That method is applicable for law enforcement purposes and could not be used as a legal ground in the scope of studied Article.

The legal ground has become dominant while European Commission is legally recognized biometric identification methodology in use by digital technology for automatic recognition.[104] This is the main element to follow for the legitimate purpose and correlate the legitimate interests of the parties concerned. Because automotive processing conducts over biometric characteristics to obtain biometric data by stringing it simultaneously into the system, – a person may not know what happened with data afterward. In this circumstance, the biometric data subject may be weak or reluctant. Informational imbalance among the companies who keep biometric data and those whose biometric companies processed builds the deployment for an extensive data application and the importance of understanding the risks here of "linking an individual to his or her civil identity"[105] because biometric data has to be detected, otherwise "the principles of data protection should therefore not apply to anonymous information, namely, information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."[106] Thus, removing directly identifying elements, unique human identification is no longer accurate and the protection is no longer active.[107]

Biometrics must be accountable to ensure that unique characteristics are processed only for those time that need to achieve unique identification purposes. After some time, it can occur that the legal basis for biometric data processing being actual before, for now, can loss its actuality, for instance, because a person has already been once uniquely identified. And, since the purpose is achieved, so the question is whether further storage of processed biometric retrieved from human characteristics, has a legal base to store and process further as such. In that means, unique identification is no longer necessary to achieve the legitimate interest of a person, and such data has to be deleted. On the argue defense, in October 2018, the Danish DPA found that the Danish taxi service Taxa 4×35 had kept the data from nearly 9 million taxi rides for five years, and faces roughly €160,000 for not deleting its users' data. [108] This hoarding records goes against GDPR Article 5 about data to be "adequate, relevant and limited to what is necessary about the purposes for which they are processed" and "kept

[104] For example, Dublin Convention digital Automated Fingerprint Identification System (AFIS) within Eurodac, at https://ec.europa.eu/home-affairs/what-we-do/networks/european_migration_network/glossary_search/automated-fingerprint-identification_en (last visited 1 July, 2022).
[105] Els J. Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (Dordrecht: Springer, 2013).
[106] GDPR, Recital 26.
[107] A29, Opinion 05/2014 on Anonymisation Techniques (2014).
[108]Information retrieved from https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/mar/tilsyn-med-taxa-4x35s-behandling-af-personoplysninger/ (last visited July 1, 2022).

in a form which permits identification for no longer than is necessary for the purposes for which the personal data are processed." Thus, it is necessary to take additional technological and organizational techniques to protect unique identification, depending on the context and time of purpose in the unique identification need for which human data is intended.

In addition, high-risk biometric systems must be certified, tested, and controlled, as cars, cosmetics, and toys are.[109] The GDPR in Article 42 provides a high degree of self-organization aiming to reduce red tape in the performance and burden for the business. Under this core, it is suggested certification schemes in order to ensure that biometric products, services, and processes certified under such schemes, and comply with specified requirements for better availability, authenticity, integrity, and confidentiality of stored, transmitted, or else processed data throughout products and services life cycle.[110] In the context of the pan-European certification mechanism,[111] it can used other "proof" tools that demonstrate a dispositive reach. Consequently, developers can integrate different safeguard sets in ways that are not unanticipated or harmful to a person.[112] This means that the processing company must implement appropriate technical and organizational measures, both during the determination of the processing preparation and during the processing of human characteristics, to show the protection effectively.

The A29 has confirmed that the data processing subject shall use a pseudonymous technique over other personal data linked to biometric one.[113] The research found that pseudonymization is when the processing data can no longer be tied to biometric data subject without more information. Such way helps shape biometric technology into a privacy-friendly approach. In principle, biometric systems and algorithms are welcome in the European market as long as they comply with EU rules. Regarding that, for example, Apple matching digital biometrics on its products aims to the Secure Enclave[114] measure; and in the same way, Touch ID revolutionized authentication using a fingerprint, Face ID revolutionizes facial recognition with intuitive and secured privacy authentication enabled by the state-of-the-art True Depth camera system with advanced technologies to map the face geometry accurately.[115] Those examples demonstrate compliance work with data

[109] European Commission, Shaping Europe's Digital Future – Questions and Answers, 2, Brussels (19 February 2020).
[110] Regulation (EU) 2019/881, Recital 75.
[111] The certification of controllers is carried out by special certification bodies of the Member States, accredited by the competent supervisory authority or by the national accreditation body, and designated to meet the requirements of the international standard EN-ISO/IEC.
[112] See Heller, "Watching Androids," 1. Some of the risks referred to in GDPR' Recital 75 and relevant to operated biometric systems in most Member States, except France, however, fail to recognize their legislation. Upon deploying biometric technologies, the study believes there is a risk for human identification and the use of biometric data as unique identifiers, such as identity fraud, function creep, and the errors inherent to any biometric system that lead to loss factors of data integrity.
[113] See The EU's-funded project ACTIBIO.
[114] See more at https://support.apple.com/en-us/HT208108 (last visited 1 July, 2022).
[115] Ibid.

protection by design and by default,[116] but may disregard privacy negative outcome. Therefore, it is necessary count the risk of disclosing any other personal information throughout a biometrically digitalized process. According to that, biometric data processing without appropriate safeguards interferes with the fundamental right to privacy and data protection under the CFREU Article 7 and Article 8 taking together. For example, in June 2020, the Romanian DPA fined Estee Lauder Romania € 3.000 for disproportionate biometric data processing and disclosure of personal data (name, surname, telephone number, date of birth, and health information) without any valid legal basis. Following an examination, the Romanian DPA found[117] Estee Lauder Romania SRL violated Articles 6, 7, and 9 GDPR. Thus, companies shall implement appropriate tech and organizational measures where risks vary.[118]

From the given outset, the company shall guarantee compliance with the GDPR and ensure that other linked information to biometric data is protected and that an assessment has taken place. Therefore, certain processing is likely to pose specific risks and should be independent on the techniques used.

V. Personal Information Management System

Unique identity found its application in the "Your Europe," "A European strategy for data," "Shaping Europe's digital future" and a "European approach to trust" facilitating interactions between citizens and businesses under the user-centric and user-friendly approaches that support uniform conditions for the implementation of the gateway solutions. The interests of the person who needs the outcome of unique identification (business) and the interests of the person who is the source of biometric data information (biometric data subject) are expressed in the explicit consent from the data source and in the view of the study, have to be together with the aspect of inviolable dignity.[119] After all, if a person is not aware and does not understand how such processing takes place, this could lead to a disproportionate effect of the processing. Dignity in the context of biometrics plays an important role, and only in this way does a person feel secure and protected facing the stress of unique identification.

One of the intentions of the EU is to design a sole European Data Space (EDS)[120] and make the processing more peaceful, to expand growth and profit from the reproduction of digital footprint for the strength of the EU Digital economy.[121] Furthermore, unique

[116] GDPR, Article 25; See Lina Jasmontaite et al., "Data Protection by Design and Default: Framing Guiding Principles into Legal Obligations in the GDPR," *European Data Protection Law Review* 4 (2) (2018): 168.
[117] Information retrieved from https://www.dataprotection.ro/?page=Amenda_pentru_incalcarea_RGPD_iunie_2020&lang=ro (last visited 1 July, 2022).
[118] Ibid, (2).
[119] CJEU, C-377/98, Netherlands v. European Parliament and Council, paras 70–77 (9 October 2001).
[120] Having regard to Regulation (EU) 2016/679, 119 OJEU 1 (4 May 2016).
[121] Having regard to Regulation (EU) 2018/1725, Article 58 (3) (c), 295 OJEU 39 (21 November 2018).

identification plays a principal role in achieving the EC goal to "enable the EU to become the most attractive, most secure and most dynamic data-agile economy in the world."[122] The objective of the deliberation is to assemble views on the personal identity conception as a complex and with the practice of open, informative, precise and dignity respectable advocating the following statement: "[S]ome people might not feel comfortable that you are taking their body features and that you are making their body algorithmic < … > It can humiliate people."[123] The CFREU Article 8 cherishes the protection of personal data as a fundamental right of each person and the GDPR strives to authorize individuals to occur control their biometrics. For this legal objective, effective practical appliances and services are necessitated.

The presented EU model of a Personal Information Management System (PIMS) has practically found a breakthrough solution to helps people have accurate control over biometric data given techniques of Personal Data Cloud Identification.[124] The PIMS enables individuals by each self to operate and control online identity and therefore advances a new legal approach where people are the in-fact holders of their data and when the very essence of human dignity is respected. It allows to govern data in a secure local and/or online storage orderliness and dispense data on when and among whom a person wants, when an individual capable of selecting exact settings for data execution and to what third interests' data may be accorded. This solution corresponds to a human-centric distinction and increased technology designs, guarding against unlawful profiling techniques, and strive to circumvent applications for a high level of protection. Likewise, a Eurobarometer survey started in March 2019. It showed that 51% of the respondents observed unfair control over their data, while 30% believed they were out of control, and just 14% deemed they were in complete control.[125] Thus, PIMS challenge is significant due to the questionable position of individuals regarding the capacity to be a supervisor of collected data.

The studied data is regularly processed in the digital ecosystem, driving people to devise digital footprints. The GDPR also grants the right to access and rectification. The biometric services addressee is indeed challenging for people to have complete control of how their biometric is processed, who can hold access to it, and how to administer practical legal stipulations and objections for unique identification. A PIMS concept is implementing its access over control and has trail access. Data can be securely obtained by other treatments using application programming interfaces that grant the capacity to admit and deny access

[122] EU, 119 OJEU 89 (4 May 2016).

[123] European Union Agency for Fundamental Rights, Report Freedoms, Under Watchful Eyes: Biometrics, EU IT systems, and Fundamental Rights, Luxembourg 43 (2018).

[124] European Data Protection Supervisor, Opinion 9/2016 on Personal Information Management Systems towards more User Empowerment in Managing and Processing Personal Data (20 October 2016); European Union Agency for Network and Information Security, Final Report on Privacy and Security in Personal Data Clouds 46 (November 2016).

[125] Information retrieved from https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2222 (last visited 1 July, 2022).

permissions on an ad-hoc cornerstone. On the other hand, people and providers would need to find a way to authenticate a biometric storage center.[126] To do so, an individual can install the freewheeling and open-source software or obtain the software as a service (SaaS) by collaborating with service providers. In the view of the research, this facilitates individuals to hunt back other parties who may process their biometrics, and individuals can customize the types of biometrics (likewise, facial or finger data) they want to assign, with whom, when among other things, a person can delete comprehensive information. Lastly, it supports minimization, ensuring that third individuals can obtain only necessary bits. Therefore, that proof-protected storage, transfers, and controlled moves of biometric footprints between biometric data systems and applications give a high level of interoperability and portability. A similar solution is UK-based "MyDex" that offers a portable and interoperable online identifier.[127] With this functionality, a person obtains distinct online access through a secure personal store; thus, verified records are managed.

There are rare cases of projects force declaring PIMS peculiarities. One is the Next Cloud[128] with a personal online data store (POD) that can be accessed by compatible apps empowering people and organizations to handle their own cloud sets for file sharing and digital collaboration as well as assigning files beyond various Next Cloud servers.[129] In the view of the study, it stands for the creation of decentralized biometric applications and grants individuals self-determination. It demands consolidation of industry necessities for unique human identification and raising open legal standards for the protection empowerment, calls to ensure security from unauthorized and/or accidental entree or modification, and relies on privacy enhancing technologies that include trusted biometric environments, homomorphic encryption,[130] giving secure multiparty computation based on differential privacy and cryptography application.[131]

Implementing PIMS, the protection assumed to be correctly designed serves for the technical and organizational benefits to measure and perform the protection. Nevertheless, these appliances or operations need to be adequately designed, for instance, when biometric

[126] See Solid Project, https://solid.mit.edu/ (last visited 1 July, 2022).

[127] Information retrieved from https://www.gov.uk/government/organisations/office-of-the-regulator-of-community-interest-companies (last visited 1 July, 2022).

[128] See more at https://nextcloud.com/ (last visited 1 July, 2021).

[129] Declaration of MyData Principles, https://mydata.org/declaration/ (last visited 1 July, 2022); See Daniel Le Metayer, "Whom to Trust? Using Technology to Enforce Privacy," in *Enforcing Privacy: Regulatory, Legal and Technological Approaches, eds. David Wright and Paul De Hert (Springer International Publishing Switzerland, 2016)*, 395–437.

[130] See Michèle Finck, "Blockchains: Regulating the Unknown," *German Law Journal* 19, no. 4 (2018): 665–92.

[131] Cryptographic points used to establish the identity authenticity based on preferences to authorized purposes and sanctioned remembrance periods against providers and third interests accordingly. A cryptography example is an encryption-based measure relying on the confidentiality and uprightness of repositories. In the view of the study, this solution moderates the risks of an unauthorized entree or biometric disclosure.

data subjects will not be enabled to run personal digital identity because ignorantly might be determined. In an unusual situation, though, the law shall specify how and to what extent biometrics are processed. For example, the determination of the processing period that would give transparency by informativeness,[132]time reservation, etc. Also, in an online setting, business often collects data for commercial supposed services. A person is faced to "agree" or "not" having no transparency about technical means. The study thinks the PIMS provides transparency on policies and tech design because the information is given in real-time, and dashboards afford processing traceability. Therefore, the PIMS realizes even more guarantees to data access because biometrics are in repositories under a person's direct control. Therefore, PIMS's strengths afford conclusive evidence that business no longer handles one's data.

Research facilitates that biometric data must be processed when there is proper a digital biometric ecosystem, whether national digital identity systems, functional digital identity systems, or both. In the view of the study, it is not only provided a high level of protection but also creates a single source of trust among EU citizens.

Conclusion

Biometric data, by its very nature, provides information about the unique characteristics of a human being and is therefore considered as information directly relating to a natural person when the data subject is distinguished from any other person by its burning essence. Therefore, unique human identification is an automatic process when a person is identifiable by biometric attributes. Developing a universal approach to the legal nature of biometric data processing is a distinct process in contrast to other special categories of data like genetics and health. It is rational that biometric data processing directly depends on machine employment. It can mistakenly process extra biometric data and additional information about a person, which entails the risks of non-compliance with the processing rules developed and derived specifically for biometrics.

In legal relations, the leading participant is the person himself because the target protection aims to protect unique data that can only be taken from a person as a biological carrier. An individual is advantaged to form any information about him, both reliable and unreliable; however, in the case of biometrics, the person has no chance to do that because humans born with unique and personal characteristics that cannot be similar to any other kind of data. Therefore, a person cannot structure and form information about personhood, but this is possible when subjected to the technology trends, which need a better legal core and reliable protection employing biometric-like technologies.

The phenomenon of biometric data processing shall execute data protection functions. With the advent of digital recognition, biometric technology considerably increases and accumulates unique identification as much as possible, preserving it, if possible. And therefore, it is necessary to introduce a special legal mechanism to protect unique human

[132] GDPR, Recital 63 and 66.

identification. The processing of biometric data includes complicated, complex algorithms when processed data can be transformed and fragmented several times. The eventual result is more complex to reconstruct than the standard processing of any personal configuration. A personalization process of certain information during unique identification leads to the inevitable linking to a particular person; therefore, provision must pay attention to the individualized nature.

It is found that unique human identification is protected based on the legal nature of data, specific technical application, and purpose of the processing. Specific techniques are used to create a biometric dataset to what the present legislation should extent data protection. It is proposed to adopt specific norms about multiple biometric identities, which the GDPR leaks to specify.

Unique human identification needs for the formation of digital law and biometric data processing has to be at the center of detailed legislation. To avoid legal and technological confusion, the justification of individual titles shall explicitly place and interpret when biometrics will be protected, especially in the digital era, from the unjustified employment of biometric technology and keep respect for the biological nature of human origin. Thus, the study calls for forming a biometric data ecosystem where "we are no longer judged based on our actions, but on what all the data about us indicate our probable actions."[133]

The research emanates the subsequent suggestions presented below under prohibition and permission gateways.

Prohibition gateway:

1) No biometric data processing without knowledge of the data subject.

2) Use for incompatible purposes, and reuse of biometric data has to be forbidden.

3) The protection by anonymous technique is not allowed for biometric data processing.

4) Biometric applications shall not be based solely on automated decisions.

5) No combination with additional personal data.

6) An explicit prohibition on processing biometrics in central databases. Limited exceptions are determined by law only.

7) Prohibition on to use biometric systems for unique identification without explicit law.

8) Explicit limitation of the use of biometric data as a unique identifier in practice is needed.

Permission gateway:

1) Consent and choice of the data subject.

2) Transparency for the data subject and role of certification. The data subject recommended receiving information through a wise module map.

3) While the biometric data process, a biometric template's deletion has to be guaranteed by law.

4) The protection of biometric data processing in a pseudonymization way.

[133] European Data Protection Authority, Norwegian Big Data Report, p. 7, point 8 (2020).

5) The processing of biometric data for the strict public necessity based on the law of a particular country.

6) The distinction of processing finalities needs to be legally established. The use of verification by businesses is appropriate.

7) An alternative identification shall be guaranteed by law.

8) Business request for unique human identification requires additional legal basis.

Bibliography

Becker, Christian. "Die normativ verweiste Gemeinschaft. Überlegungen zum Schicksal der Ethik im freiheitlichen Rechtsstaat." *Annual Review of Law and Ethics* 27 (2019): 39–54.

Brkan, Maja. "The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors." *Maastricht Journal of European and Company Law* 23 (5) (2016): 812–41.

Cherry, Miriam A. "Cyber Commodification." *Maryland Law Review* 72, no. 2 (2013): 381–451.

Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Guidelines on Facial Recognition (January 28, 2021).

Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data (Strasbourg, 2–4 February 2005).

Committee on Legal Affairs and Human Rights. Report on Doc. 12522 at February 16, 2011, The Need for a Global Consideration of the Human Rights Implication of Biometrics (January 23, 2012).

European Data Protection Supervisor and Agencia Espanola Protection Datos. Joint Paper on 14 Misunderstandings with Regard to Biometric Identification and Authenification (June 2020).

Danaher, John, Sven Niholm, and Brian D. Earp. "The Benefits and Risks of Quantified Relationship Technologies: Response to Open Peer Commentaries on 'the Quantified Relationship.'" *American Journal of Bioethics* 18 (2018): W3 – W6.

Dearing, Albin. "Human Dignity: The Right to Be a Person." In *Justice for Victims of Crime: Human Dignity as the Foundation of Criminal Justice in Europe*, 139–292. Cham: Springer, 2017.

Eberle, Edward J. "Observations on the Development of Human Dignity and Personality in German Constitutional Law: An Overview." *The Liverpool Law Review* 33, no. 3 (2012): 201–33.

Finck, Michèle. "Blockchains: Regulating the Unknown." *German Law Journal* 19, no. 4 (2018): 665–92.

Gayer, Gabrielle, Itzhak Gilboa, Larry Samuelson, and David Schmeidler. "Pareto Efficiency with Different Beliefs." *The Journal of Legal Studies* 43, no. 2 (2014): 151–71.

Heller, Brittan. "Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law." *Vanderbilt Journal of Entertainment and Technology Law* 23, no. 1 (2021). https://scholarship.law.vanderbilt.edu/jetlaw/vol23/iss1/1.

Hobbes, Thomas. *Leviathan.* Oxford University Press, 2009.

Jasmontaite, Lina, Irene Kamara, Gabriela Zanfir-Fortuna, and Stefano Leucci. "Data Protection by Design and Default: Framing Guiding Principles into Legal Obligations in the GDPR." *European Data Protection Law Review* 4 (2) (2018): 168–89.

Juutilainen, Teemu."Law-based Commodification of Private Debt." *European Law Journal: Review of European Law in Context* 22, no. 6 (2016): 743–57.

Kindt, Els. "A First Attempt at Regulating Biometric Data in the European Union." *Regulating Biometrics: Global Approaches and Urgent Questions* (2020): 62–69.

Kindt, Els. *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis*. Dordrecht: Springer, 2013.

Kindt, Els. "The Processing of Biometric Data, A Comparative Legal Analysis Focuses on the Proportionality Principle and Recommendations for a Legal Framework." PhD diss., 2012.

Krausova, Alžběta. "Online Behavior Recognition: Can We Consider It Biometric Data under GDPR." *Masaryk University Journal of Law and Technology* 12 (2) (2018): 161–78.

Lambert, Paul. *Understanding the New European Data Protection Rules.* Auerbach Publications, CRC Press, 2018.

Leibenger, Dominik, Frederik Möllers, Anna Petrlic, Ronald Petrlic, and Christoph Sorge. "Privacy Challenges in the Quantified Self Movements – An EU Perspective." *Proceedings on Privacy Enhancing Technologies* 4 (2016): 315–34.

Leone, Massimo. "From Fingers to Faces: Visual Semiotics and Digital Forensics." *International Journal for the Semiotics of Law* 34, no. 2 (2021): 579–99.

Lubin, Asaf. "The Liberty to Spy." *Harvard International Law Journal* 61 (1) (2020): 185–244.

Martin, Jena. "Business and Human Rights: What's the Board Got to Do with It?" *University of Illinois Law Review* (2013): 959.

Metayer, Daniel Le. "Whom to Trust? Using Technology to Enforce Privacy." In *Enforcing Privacy: Regulatory, Legal and Technological Approaches*, edited by David Wright and Paul De Hert, 395–437. Springer International Publishing Switzerland, 2016.

Monteiro, A. Reis. "Human Dignity Principle." In *Ethics of Human Rights*, 199–236. Springer International Publishing, 2014.

Nguyen, Fiona Q. "The Standard for Biometric Data Protection." *Journal of Law & Cyber Warfare* 7, no. 1 (2018): 61–84.

Peerani, Aaida. "The Reasonable Person." *Law Now* 46, no. 1 (2017). https://www.lawnow.org/the-reasonable-person/.

Pucket, Carolyn. "The Story of the Social Security Number." *Social Security Bulletin* 69 (2) (2009): 55–74.

Reijneveld, Minke D. "Quantified Self, Freedom and the GDPR." *Scripted: Journal of Law, Technology and Society* 14 (2) (2017): 285–325.

Rosenbaum, Sara, and Elizabeth Taylor. "The Irreplaceable Program in an Era of Uncertainty." *The Journal of Law, Medicine & Ethics* 46, no. 4 (2018): 883–86.

Schwander, Ivo. "Das Statut der Internationalen Gesellschaft." *Schweizerische Zeitschrift für internationales und europäisches Recht* 12 (1) (2002): 57–77.

Solove, Daniel J. *Nothing to Hide: The False Tradeoff between Privacy and Security.* New Haven [Conn.]: Yale University Press, 2011.

Spiecker genannt Döhmann, Indra, Olivia Tambou, Paul Bernal, Margaret Hu, Carlos Molinaro, Elsa Negra, Ingo Wolfgang Sarlet, Laura Schertel Mendes, Normann Witzleb, and Florian Uger. "Multi-Country · the Regulation of Commercial Profiling – A Comparative Analysis." *European Data Protection Law Review (Internet)* 2, no. 4 (2016): 535–54.

Stiglitz, Joseph. "Regulation and Failure." In *New Perspectives on Regulation*, edited by David Moss and John Cisternino, 11–23. Cambridge, MA: The Tobin Project, 2009.

Todorova, Tamara. "Transaction Costs, Market Failures and Economic Development." *Journal of Advanced Research in Law and Economics* 7, no. 3 (17) (2016): 678–84.

Ukrow, Jörg. "Data Protection without Frontiers: On the Relationship between EU GDPR and Amended CoE Convention 108." *European Data Protection Law Review* 4 (2) (2018): 239–47.

Urgessa, Worku Gedefa. "The Feasibility of Applying EU Data Protection Law to Biological Materials: Challenging Data as Exclusively Informational." *Journal of Intellectual Property, Information Technology, and Electronic Commerce Law* 7 (2) (2016): 96–109.

Walker, Elizabeth M. "Biometric Boom: How the Private Sector Commodifies Human Characteristics." *Fordham Intellectual Property, Media & Entertainment Law Journal* 25, no. 3 (2015). https://ir.lawnet.fordham.edu/iplj/vol25/iss3/5.

Working Party 29 on the Protection of Individuals with Regard to the Processing of Personal Data. Working Document on Biometrics (August 1, 2003).

Daria Bulgakova. Unique Human Identification under the GDPR Article 9 (1) (2)

Abstract. The rapid development of information technology has exacerbated the need for robust personal data protection safeguarded by the European Union instrument. Safeguarding a fundamental right to data protection entails new and significant challenges as technological advances expand the frontier of data processing. The large-scale employment of digital biometric technology has shaken the private sector. Biometric data processing already became crucial for a person's unique identification in the private sector and posed a risk to the unique characteristics of a human being. The research seeks to study the recent defining biometric data and automatizing processing as legally established categories under GDPR Article 9 (1) (2) when the subject and object of the processing are uncertain. The study calls to protect a person from whom unique human data is extracted and finds a way to protect biometric characteristics based on its differentiation form defined in the studied article's else special categories of personal data. To this end, the studied article assumes a natural person, but it is used only in the context of the finality of processing. Therefore, there are possible prior risks for the process and after processing that shall be defined and mitigated under the high level of legal protection. In this regard, a study thinks unique characteristics of human origin shall be carried in the legal field by having clearly defined status, preservation measures regardless of biometric nature, and finding a solution for a biometric data subject to control automotive employment as the Personal Information Management System in the EU does.

Keywords: personal data protection; biometric data; automotive processing; identity recognition.

Дар'я Булгакова. Унікальна ідентифікація людини відповідно до статті 9 (1) (2) GDPR

Анотація. Масштабне застосування інформаційних технологій загострило потребу у надійному захисті персональних даних, гарантованому в Європейському Союзі інструментом права. Забезпечення фундаментального права на захист даних спричиняє нові та серйозні

проблеми, оскільки технологічні досягнення розширюють межі їх обробки. Обробка біометричних даних стала вирішальною для унікальної ідентифікації людини і поставила під загрозу її характеристики. Так як суб'єкт та об'єкт обробки потребують наукового аналізу, дослідження спрямоване на вивчення недавнього закріплення біометричних даних та автоматизованої обробки як законодавчо встановлених категорій відповідно до статті 9 (1) (2) GDPR. Задачі спрямовані для захисту особи, яка безпосередньо є носієм унікальних даних від природи, та запропоновано спосіб їх вирішення на основі диференціації біометричних характеристик від інших визначених категорій у розрізі спеціальних персональних даних. Дослідження також показало, що стаття, яка вивчається, використовується тільки в контексті остаточності обробки. Отже, існують можливі попередні ризики, та в процесі опрацювання, які мають бути визначені та знижені в рамках правового поля. У зв'язку з цим, пропонується чітко визначити статус унікальних людських характеристик, і вжити заходів для захисту таких відповідно до їх біометричної природи шляхом надання можливості суб'єкту біометричних даних контролювати та керувати їх рух при застосуванні автоматизованих функціональностей на прикладі Системи Управління Особистої Інформації, дієвої в Європейському Союзі.

Ключові слова: захист персональних даних; біометричні дані; автоматизированная обработка; розпізнавання особистості.

Дарья Булгакова. Уникальная идентификация человека в соответствии со статьей 9 (1) (2) GDPR

Аннотация. Масштабное применение информационных технологий обострило потребность в надежной защите персональных данных, гарантированной в Европейском Союзе инструментом права. Обеспечение фундаментального права на защиту данных влечет за собой новые и серьезные проблемы, поскольку технологические достижения расширяют границы обработки данных. Масштабное применение цифровых биометрических технологий потрясло частный сектор. Обработка биометрических данных уже стала решающей для уникальной идентификации человека и поставила под угрозу его характеристики. Так как субъект и объект обработки нуждаются в научном анализе, исследование направлено на изучение биометрических данных и автоматизированной обработки в силу правового закрепления таковых на законодательном уровне в соответствии со статьей 9 (1) (2) GDPR. Задачи направлены для защиты лица, непосредственно носителя уникальных данных от природы, и предложен способ их решения на основе дифференциации биометрических характеристик от других определенных в категории специальных персональных данных исследуемой статьи. Результат показал, что изучаемая статья используется только в контексте окончательности обработки. Следовательно, существуют возможные предшествующие риски, которые должны быть определены и снижены в рамках высокого уровня правовой защиты. В этой связи, предлагается четко определить статус уникальных человеческих характеристик, и принять меры по защите таковых в соответствии с их биометрической природой путем разработки возможности субъекта биометрических данных контролировать и управлять таковыми при применении автоматизированных функциональностей на примере Системы Управления Личной Информации, введенной в Европейский Союзе.

Ключевые слова: защита персональных данных; биометрические данные; автоматизированння обработк; распознавание личности.

Одержано/Received 25.05.2022