A. Brömme, N. Damer, M. Gomez-Barrero, K. Raja, C. Rathgeb,
A. Sequeira, M. Todisco and A. Uhl (Eds.): BIOSIG 2022,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2022

Processing Information from the Human Body: Measurements of Biological and Behavioural Signals as a Unifying Link

Lydia Belkadi[1]

Abstract: This contribution proposes the concept of "measurements of biological and behavioural signals" for interdisciplinary research on the automated processing of information from the human body. This concept has merits in mitigating legal definitions' instability. We further aim to bridge legal and technical vocabularies, both responding to specific methodologies. Revising this concept should enable a more coherent approach and account for information about the human body, emerging sensing devices, and automated systems.

Keywords: Measurements of Biological and Behavioural Signals, Information from the Human Body, Concept-building, ISO Vocabulary, Legal Definitions, Automated Processing, AI, Biometrics.

1 Introduction

The vocabulary developed by the International Organization for Standardization ("ISO") constitutes an important and resilient tool in understanding the techniques and infrastructures used for biometric recognition. However, standardised vocabularies provide limited guidance for conceptualising new processing frameworks that do not (yet) meet quality, accuracy and security standards established by academic and professional communities. At the same time, legal discussions encompass but are not limited to systems performing biometric recognition, as defined by technical communities. Hence, the legal definition of biometric data has been contested and criticised. In particular, it remains largely unclear whether it would be fit to regulate emerging forms of Artificial Intelligence processing, such as emotion recognition. Against this background, it is crucial to identify *unifying conceptual link(s)* that ensure a coherent interdisciplinary account of processing from the human body. This contribution suggests that such a unifying link should consider the etymological and technical roots of "biometric" processing to reflect further upon information about the human body, emerging sensing devices, and automated systems. In particular, we consider that *measurements of biological and behavioural signals* always constitute the initial interaction with any system processing information from the human body.

[1] KU Leuven, Faculty of Law, Center for IT and IP Law, Sint-Michielsstraat 6 box 3443, Leuven 3000, Belgium, lydia.belkadi@kuleuven.be.

2 Technical Understanding of Biometric Information Under ISO/IEC 2382-37:2022

The ISO established a standardised biometric vocabulary ('biometric vocabulary') aiming to harmonise terminologies used by academic and professional communities. This vocabulary was developed to support interoperable large-scale biometric systems and data sharing [ISO22]. In this context, the ISO defines biometric data as

> *"[a] biometric sample […] or [an] aggregation of biometric samples at any stage of the processing".*

This definition was constructed broadly to encompass all the information deduced from captured biometric characteristics and contained in the biometric sample(s) (i.e., representations of biometric characteristics) [Ki13]. Accordingly, it also accounts for any transformation carried out throughout different processing stages [Ki13, Ja16a]. The concept of "biometric characteristics" is key to understand the biometric vocabulary. This concept is defined as

> "*biological and behavioural characteristic of an individual from which distinguishing, repeatable biometric features […] can be extracted for the purpose of biometric recognition […]"*.

This definition establishes a direct link between biometric characteristics and their fitness for biometric recognition. In other words, selected biological and behavioural characteristics should cumulatively bear specific qualities and be processed for specific purposes. Firstly, the fitness of selected biological and behavioural characteristics is defined with reference to the distinctiveness and repeatability (also known as "interclass" and "intra-class" variations) of the feature(s) (i.e., numbers or labels used for comparison) that *may* be extracted. In other words, features should have a wide variation between two different persons while having a low variation when captured from the same individual. Accordingly, capturing biological and behavioural characteristics aims to establish "a realistic and invariant representation of the biometric characteristic for discerning the unique or distinctive information" [Ki13].

Furthermore, selected biological and behavioural characteristics must contain features fit for biometric recognition purposes. Biometric recognition is defined as the "automated recognition of individuals based on their biological and behavioural characteristics", through two functions (biometric identification and verification) [ISO22]. Both functionalities aim to establish the probability that two digital representations of biometric characteristics stem from the same individual through different technical implementation. Biometric verification recognises an individual through the comparison of two samples (1:1 comparison). In contrast, biometric identification recognises an individual by determining whether a biometric characteristic has been previously captured and stored through a comparison with multiple samples (1:n comparison), clarifying whether an individual is known from a specific (set of) database(s) [Ki13].

In sum, the concept of "biometric data" under the biometric vocabulary only encompasses representations (i.e., "biometric samples") of biological and behavioural characteristics that are fit to be processed for establishing the probability that two samples originate from the same individual (i.e., "biometric recognition"), through the use of two specific functionalities (i.e., biometric "verification" and "identification").

3 Legal Understanding of Biometric Information After the Data Protection Reform

The legal concept of "biometric data" was introduced within European data protection laws to regulate the processing of biometric data and mitigate the risks to individuals. From a legal perspective, biometric information should first qualify as *personal data* to further determine whether they amount to biometric data as narrowly understood by the law. On the one hand, the General Data Protection Regulation ('GDPR') and the Law Enforcement Directive ('LED') provide that personal data are

> "*any information relating to an identified or an identifiable natural person […]".*

Data protection frameworks further consider the effects of two types of transformations on the legal nature of personal data (i.e., pseudonymisation and anonymisation). Pseudonymisation is defined as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information […]". Recital 26 of the GDPR clarifies that pseudonymisation modifies the legal nature of the information. Accordingly, pseudonymised data should be interpreted as personal data about an *identifiable* individual.[2] In other words, this means that the identification of the individual is not effective, yet remains a possibility [WP07]. In contrast, anonymous information is conceptualised negatively as information that *is not* personal data. In particular, Recital 26 of the GDPR and 21 of the LED acknowledge the legal significance of *anonymising processing* that *render* personal data anonymous (i.e., transformed data). In this case, the processing should be performed in a manner that is irreversible and ensures that the data subject is not or no longer identifiable [WP14]. Anonymous data are explicitly excluded from the scope of the GDPR and the LED.

On the other hand, the GDPR and the LED define biometric data narrowly as

> *"personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person […]".*

The scope of this definition is discussed by legal scholars. In particular, the legislator has created confusion by mentioning in Recital 51 of the GDPR that photographs should not

[2] Recital 21 of the LED does not contain this precision. However, both texts similarly define pseudonymisation and underline the risks of unauthorized reversal.

systematically be considered sensitive data. Hence, this recital seems to result in a semi-exclusion of specific biometric samples, particularly "photographs". However, this precision is not found in the LED [Ki18]. Furthermore, the meaning of "specific technical processing […] allowing or confirming the unique identification of an individual" is nowhere defined nor explained and, therefore, remains debated by scholars and professional communities. Indeed, we are of the opinion that this definition is not specific as to which stages of biometric processing (e.g., capture, pre-processing, feature extraction, etc.) and which functionalities are included [Ja16a, Ja16b, Ki18, Cl19].

In sum, ascertaining whether biometric information should be understood as "personal data" depends on a specific assessment for determining whether an individual is *a minima* identifiable. Furthermore, qualifying biometric information as "biometric data" in the legal sense requires an additional assessment dependent on the interpretation given to "specific technical processing […] which allow or confirm the unique identification". Without further interpretative guidance, evaluating the exact scope of the legal concept of "biometric data" remains difficult. Regardless, this two-step assessment is crucial to comply with data protection principles (e.g., lawfulness, security, accountability, etc.) and controllers' legal obligations [Ki13, Ja16b, Ki18, Cl19].

4 On the Need for a Broader Understanding of Biometric Information

Regulators have been examining for several years the opportunity and need to develop further sub-categories of personal data and establish specific rules for new categories of personal data. For example, European legislators have adopted a non-technologically neutral stance on the regulation of AI systems. Accordingly, the AIA seeks to regulate a set of AI systems processing information extracted from the human body (e.g., remote biometric identification, emotion recognition and biometric categorisation systems, medical devices) and provide safeguards against the risks of biometric mass surveillance [COE21, EC21a, Ge21]. The negotiations for the adoption of the Artificial Intelligence Act ("AIA") have generated discussions over the need to reform the concept of biometric data [ED21, EP21 JP21, EUC22, EP22]. Recently, the Council of the European Union proposed to abandon the reference to "unique identification" [EUC22]. In contrast, the European Parliament's Draft Report proposes to distinguish the concepts of "biometric data", as understood under data protection laws, and "biometric-based data" [JP21, EP22]. These definitions are still being discussed within institutions and, hence, are not legally binding. Furthermore, the position of the European Parliament remains uncertain as the proposed amendments have not all been discussed yet.

It should be emphasised that this is not the first time regulators have examined the need to develop further sub-categories of personal data and regulate more strictly specific types of information related to the human body. For example, the legal definition of "biometric data" is a relatively new legal concept integrated into Data Protection laws

only recently [EU16a, EU16b]. Similarly, discussions were initiated by Organisation for Economic Cooperation and Development on the need to define "personal brain data" and establish additional safeguards for information derived from the human brain [OEC19]. These evolutions point towards significant technological transformations in the use of information from the human body, particularly improvements in sensing capacities and their integration with increasingly sophisticated processing frameworks. They also reveal long-standing difficulties in adopting legal definitions that withstand the pace of technological evolution while being sufficiently coherent and stable.

5 Measurements of Biological and Behavioural Signals as a Unifying Link

As a first step to bridge interdisciplinary vocabularies, this contribution suggests revising our understanding of the etymological and technical roots of "biometric" processing. The word "biometric" is etymologically derived from the Greek nouns βίος (i.e., life) and μέτρον (i.e., measure) and defined as the "measurement of living species".[3] Measuring the human body requires capturing and transforming its signal(s). In other words, signals of biological and behavioural characteristic(s) interact with a sensor that operates a transduction – i.e., the conversion of one form of energy (e.g., heat) into another (e.g., electrical) – resulting in an interaction which may be understood as a (series of) "measurement(s)".

Under the ISO biometric vocabulary, this process is detailed under the definition of *biometric capture*, defined as

> *"obtaining and recording of, in a retrievable form, signal(s) of biometric characteristic(s) […] directly from individual(s), or from representation(s) of biometric characteristic(s)*".

This definition refers to the initial interaction necessary to perform biometric recognition. Note 3 of this entry explains that signals may be generated or affected by the characteristic (e.g., a face illuminated by incident light) [ISO22]. As discussed above, the concept of biometric characteristic(s) is defined with reference to the purposes of biometric recognition (i.e., determining the probability that two samples stem from the same person). A more general concept may be built by following this blueprint and adopting the concept of "biological and behavioural characteristic(s)". Accordingly, the capture of biological and behavioural characteristic(s) amounts to a "measurement of biological and behavioural signals".

This revision is more in line with the etymological root of "biometric" and has several

[3] The term "biometric" (adj.) is not equated to the concepts of "biometrics" (n.) or "biometric recognition" (n.) as defined under technical and standardised vocabularies developed by biometric communities. The latter terms receive a standardised definition within biometric communities that reflects long-established practices reflecting accuracy, security and quality standards [ISO22, Ki13, Ja16].

merits for unifying interdisciplinary discussions. Firstly, this notion replaces the capture of information within its original scientific field, i.e., physics. Indeed, *any measurement* is a physical process governed and constrained by the laws of physics. Philosophy scholars have discussed the epistemological foundations and ethical significance of biometric capture. In particular, from an epistemological perspective, it was highlighted that such measurements should not be understood as reflecting "natural properties" per se but instead "measurable physical properties" [GK12, MT12, Va12]. In particular, measuring has been described as a non-neutral action that entails an active data reconstruction reducing and reshaping identity as only recordable quantitative aspects [Va02, GK12]. These philosophical and ethical considerations are also crucial from a legal point of view, as emerging technologies increasingly exploit complex phenomena. For example, these analyses raise questions as to *what* is measured and the limits of measurement processes in accounting for the qualitative and subjective properties of individuals (e.g., emotions, mental states, etc.) [GK12].

From a privacy and data protection perspective, the concept of processing "measurement of biological and behavioural signals" may act as a conceptual link for analysing a set of closely related (AI) systems by reconnecting them to their informational source, i.e., the human body. Furthermore, it would also mitigate the limitations of (standardised) vocabularies designed specifically for biometric recognition. Indeed, many systems emerge without meeting biometric recognition's definition or technical specifications. In particular, systems may fall short of implementing one of the two functions of biometric recognition (i.e., identification or verification) or using adequate biometric characteristics (e.g., characteristics that are not sufficiently distinctive or repeatable) [ISO22].

Finally, turning to this concept would not signal a shift in existing technical and legal scholarship analysing automated systems exploiting biological and behavioural signals. Turning to the concept of processing "measurement of biological and behavioural signal(s)" may link and provide more clarity regarding the various methodological approaches and purposes pursued in processing information from the body, as well as their specificities. In particular, scholars from many disciplines discuss the resilience, adequacy and coherence of legal definitions to assess and address the opportunities and risks of specific technical methodologies and approaches. Accordingly, using the concept of "measurement of biological and behavioural signals" may act both as an enabler and a link between various communities to develop further concepts reflecting their processing and privacy-preserving practices. Both types of practices are crucial in assessing the necessity and proportionality of data processing [Ki13].

6 Conclusion

This contribution detailed the scope and limitations of the conceptual frameworks deployed in legal and technical vocabularies to address the processing of information

from the human body coherently. In particular, both approaches rely on different concepts and different strategies to cope with technological evolutions. Against this background, this contribution has argued for the need to develop and foster concepts that may act as *unifying links* to bridge interdisciplinary vocabularies and analyses. As a first step in this direction, this contribution underlines the importance of using the concept of "measurement of biological and behavioural signals" to foster interdisciplinary discussions, concepts and research. Indeed, this concept unifies multiple disciplines analysing the capture of information from the human body, a necessary pre-condition for any further processing.

Acknowledgements. This work has been funded by the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska Curie grant agreement No.860813–TReSPAsS-ETN. The author would like to acknowledge the constructive and insightful feedback of Dr. Els Kindt and Dr. Catherine Jasserand throughout the writing of this contribution. The author also acknowledges the importance of many insightful discussions throughout the Dagsthul Seminar on 'Privacy in Speech and Language Technology' (22342) in shaping the final version of this contribution.

References

[COE21] Council of Europe Guidelines on facial recognition, https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html.

[Cl19] Clifford, D.: The Legal Limits to the Monetisation of Online Emotions, PhD thesis, KU Leuven, 2019.

[EC21a] European Commission Proposal for an Artificial Intelligence Act, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206.

[ED21] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf.

[EP21] EPRS Study Person identification, human rights and ethical principles https://www.europarl.europa.eu/RegData/etudes/STUD/2021/697191/EPRS_STU(2021)697191_EN.pdf.

[EP22] European Parliament Draft Report on the Proposal for an Artificial Intelligence Act, https://iapp.org/media/pdf/publications/CJ40_PR_731563_EN.pdf.

[EU16a] European Union General Data Protection Regulation, https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04.

[EU16b] European Union Law Enforcement Directive, https://eur-lex.europa.eu/eli/dir/2016/680/oj.

[EUC22] Council of the European Union Proposal for an Artificial Intelligence Act – Presidency compromise text, https://www.statewatch.org/media/3366/eu-council-ai-act-

presidency-consolidated-comrpomise-10069-22.pdf.

[GE21] Greens/EFA Study Biometric and Behavioural Mass Surveillance in EU Member States, http://extranet.greens-efa-service.eu/public/media/file/1/7297.

[GK12] Ghilardi, G.; Keller, F.: Epistemological Foundation of Biometrics. In (Mordini and Tzovaras): Second Generation Biometrics: The Ethical, Legal and Social Context. 23-47, 2012.

[ISO22] ISO/IEC 2382-37 Information technology – Vocabulary – Part 37: Biometrics, https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-3:v1:en.

[Ja16a] Jasserand, C.: Avoiding Terminological Confusion Between the Notions of 'Biometrics' and 'Biometric Data'. International Data Privacy Law 6/1, 63-76, 2016.

[Ja16b] Jasserand, C.: Legal Nature of Biometric Data: From Generic Personal Data to Sensitive Data. European Data Protection Law Review 2/3, 297-311, 2016.

[JP21] JURI and PETI Study Biometric Recognition and Behavioural Detection https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf.

[Ki13] Kindt, E.: Privacy and Data Protection Issues of Biometric Applications, A Comparative Legal Analysis. 2013.

[Ki18] Kindt, E.: Having yes, using no? About the new legal regime for biometric data. Computer Law & Security Review 34/4, 523-238, 2018.

[MT12] Mordini, E.; Tzovaras, D.: Second Generation Biometrics: The Ethical, Legal and Social Context. 2012.

[OEC19] OECD Recommendation on Responsible Innovation in Neurotechnology, https://www.oecd.org/science/recommendation-on-responsible-innovation-in-neurotechnology.htm.

[Va02] Van der Ploeg, I.: Biometrics and the body as information: normative issues of the socio-technical coding of the body. In (Lyon, et al.) Surveillance as Social Sorting. 2002.

[Va12] Van der Ploeg, I.: The body as data in the age of information. In (Lyon, et al.) Routledge Handbook of Surveillance Studies. 2012.

[WP07] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.

[WP14] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.