BIOMETRIC DATA VULNERABILITIES: PRIVACY IMPLICATIONS

Alžběta Krausová,* Hananel Hazan,** Ján Matejka***[1]

Abstract: *Biometric data are typically used for the purposes of unique identification of a person. However, recent research suggests that biometric data gathered for the purpose of identification can be analysed for extraction of additional information. This augments indicative value of biometric data. This paper illustrates the range of augmented indicative values of the data as well as identifies crucial factors that contribute to increased vulnerability of data subjects.*

Keywords: *augmented indicative value, biomarker, biometric data, European law, face recognition, fingerprint, General Data Protection Regulation, identification, personal data, privacy, retina, voice recognition, vulnerability*

INTRODUCTION

Biometric technology serves as an efficient and reliable means of verifying or determining an identity of a natural person. Technically speaking, biometrics is defined as *"automated recognition of individuals based on their biological and behavioural characteristics*".[2] These characteristics are usually referred to as biometric data. As opposed to other personal data, biometric data not only provide information about an individual but they also provide a unique link to this individual[3] and, therefore, can serve as an identifier.[4] This feature has been utilized in a number of applications. The most profound application is access control to premises or devices, such as using fingerprints to unlock a smartphone or home.

Biometrics is not a marginal technology and its use is constantly growing. Biometric technologies presumed to have the greatest market potential in the period from 2016 through 2025 are fingerprint sensors, voice/speech recognition, iris recognition, and facial recognition.[5] Annual biometrics revenues from these technologies shall increase every year in each region of the world and are estimated to reach the total global revenue of 15.1

* Mgr. Alžběta Krausová, LL.M. Institute of State and Law of the Czech Academy of Sciences, Prague, Czech Republic
** Hananel Hazan, Ph.D. College of Information and Computer Sciences, University of Massachusetts, Amherst, MA, United States of America
*** JUDr. Ján Matejka, Ph.D. Institute of State and Law of the Czech Academy of Sciences, Prague, Czech Republic

[1] This paper was supported by the Czech Science Foundation (GA ČR) under grant No. 16-26910S Biometric Data and Their Specific Legal Protection.

[2] ISO/IEC. International Standard ISO/IEC 2382-37. Information technology – Vocabulary – Part 37: Biometrics. Second edition. In: *International Standard Organization* [online]. 2017 [2017-10-16]. Available at: <http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>.

[3] The data do not refer to a token owned by this individual, but rather to herself, her unique characteristics that are in principle stable and unchangeable.

[4] ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 4/2007 on the concept of personal data. In: *European Commission* [online]. 20. 6. 2007 [2017-10-16]. Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>.

[5] KIRKPATRICK, K., WHEELOCK, C. Biometrics Market Forecasts Global Unit Shipments and Revenue by Biometric Modality, Technology, Use Case, Industry Segment, and World Region: 2016-2025. Executive Summary. In: *Tractica* [online]. 2017 [2017-12-01]. Available at: <https://www.tractica.com/download-proxy?report_id=6991&type=Executive+Summary>.

billion USD in 2025.[6] Currently, many people use some of these technologies on a daily basis. According to a recent study on consumer perception of biometrics, 82 % of those who have access to a technology equipped with fingerprint sensors, utilize these sensors.[7] According to market research performed by Counterpoint, over a billion smartphones with fingerprint sensors will be shipped worldwide in 2018.[8]

Processing of biometric data is regulated by laws on privacy and personal data protection. Special features of this type of data were recognized by Article 29 Working Party (hereinafter WP29), an advisory body set up by EU Data Protection Directive[9] in its opinions.[10] Despite recognizing biometrics as a convenient means of identification and authentication, WP29 highlighted also drawbacks of this technology related not only to their irrevocability, but to loss of anonymity or end to untraced movements of individuals as well.[11]

Moreover, WP29 made clear that biometric data can contain information of sensitive nature, such as health condition, predisposition to diseases, and racial or ethnic origin. Acquiring this additional information depends on sensors used for capturing biometric features as well as on algorithms used for processing a raw form of these features. Biometric features can, however, not only reveal information obvious to human eyes such as gender, ethnic origin, body deformations, or skin diseases. With constantly developing fields of medicine, biostatistics, and machine learning, raw biometric features can be analysed to retrieve information about yet undetected diseases, current mental and biological states, or probable level of performance of some tasks. Such possibilities augment indicative value of this kind of data. They also give rise to questions about the scope of such augmented indicative values of biometric data, their impact on vulnerability of data subjects, and overall impact on privacy protection in the field of biometrics.

The aim of this paper is to illustrate the augmented indicative values of biometric data and to identify critical factors that increase vulnerability of data subjects. For the purposes of this paper, vulnerability is understood as *"a state of being exposed to the possibility of being attacked or harmed, either physically or emotionally*".[12] The vulnerability increases when the possibility of being harmed is more likely. This might happen due to a number

[6] Ibid.

[7] Fingerprint is now the main ID method on mobile as consumers turn their back to PINs & passwords. In: *The Official Fingerprints Blog* [online]. 20. 9. 2017 [2017-12-01]. Available at: <https://no1biometrics.com/2017/09/20/fingerprint-is-now-the-main-id-method-on-mobile-as-consumers-turn-their-back-to-pins-passwords/>.

[8] SHARMA, P. More Than One Billion Smartphones with Fingerprint Sensors Will Be Shipped In 2018. In: *Counterpoint* [online]. 29. 9. 2017 [2017-12-01]. Available at: <https://www.counterpointresearch.com/more-than-one-billion-smartphones-with-fingerprint-sensors-will-be-shipped-in-2018/>.

[9] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[10] See ARTICLE 29 DATA PROTECTION WORKING PARTY. Working document on biometrics. In: *European Commission* [online]. 1. 8. 2003 [2017-10-20]. Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf> or ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 3/2012 on developments in biometric technologies. In: *European Commission* [online]. 27. 4. 2012 [2017-10-20]. Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf>.

[11] For details see ibid. Opinion 3/2012 on developments in biometric technologies.

[12] Vulnerability. In: *Google Dictionary* [online]. [2017-12-10]. Available at: <https://www.google.cz/search?q=Dictionary#dobs=vulnerability >.

of reasons that are to be identified in this paper including the informational power that controllers might gain over data subjects. Identified vulnerabilities shall be assessed in the light of guarantees provided by the General Data Protection Regulation.[13]

2. AUGMENTED INDICATIVE VALUES OF BIOMETRIC DATA

As stated above, biometrics is a term referring to the *"use of distinctive biological or behavioral characteristics to identify people*"[14] with help of automated means. These characteristics, however, can be examined for other purposes than just for distinguishing one person from another. Biological and behavioural characteristics are commonly used also for evaluation of identity and personality aspects (such as age, gender, ethnic origin, social status, capabilities, etc.), for assessing momentary state of an individual (identification of emotions or overall feeling), or for medical diagnosis of abnormalities and diseases.

When gathered by automated means and preserved in a digital form, biological or behavioural characteristics can be analysed with help of pattern recognition systems and machine learning techniques to derive any information desired, provided that a link has been identified between data available from biometric sensors and a certain indicative quality. Therefore, biometric data can be analysed for instance for occurrence of biomarkers. Biomarker can be defined as *"a characteristic that is objectively measured and evaluated as an indicator of normal biological processes, pathogenic processes, or pharmacologic responses to a therapeutic intervention*".[15] These biomarkers can reliably determine presence or predisposition of an illness in an individual.

As the research on biomarkers and other knowledge in biostatistics is publicly available, anyone who creates a biometric system can incorporate this kind of analysis in the biometric algorithm. So far there is a vast amount of research that indicates what information can be extracted from which source of data. Some information has a really sensitive nature and may also impact privacy of family members (genetic diseases). Other information can serve for detecting intentions of a monitored person (for instance lie detection) or for designing strategies how to efficiently influence her (for instance with help of automated detection of emotion from voice when talking on a customer phone line).

Fingerprints can be analysed for determining gender[16] or ancestral background[17] of a person. Based on their temperature, fingerprints can also indicate a state of relaxation

[13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

[14] DUNSTONE, T., YAGER, N. *Biometric System and Data Analysis. Design, Evaluation, and Data Mining*. New York: Springer, 2009. See p. 3.

[15] Cited in STRIMBU, K., TAVEL, J. A. What are biomarkers? *Current Opinion in HIV and AIDS*. 2010, Vol. 5, No. 6, [2017-12-17]. Available at: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3078627/#R1>.

[16] KAUSHAL, N., KAUSHAL, P. Human Identification and Fingerprints: A Review. *Journal of Biometrics & Biostatistics*. 2011, Vol. 2, No. 123, [2017-12-17]. Available at: <https://www.omicsonline.org/human-identification-and-fingerprints-a-review-2155-6180.1000123.php?aid=2581>.

[17] FOURNIER, N. A., ROSS, A. H. Sex, Ancestral, and pattern type variation of fingerprint minutiae: A forensic perspective on anthropological dermatoglyphics. *American Journal of Physical Anthropology*. 23 September 2015, [2017-12-17]. Available at: <http://onlinelibrary.wiley.com/doi/10.1002/ajpa.22869/abstract>.

or anxiety[18] of a person and even show intensity of acute stress.[19] Moreover, temperature of fingerprints can predict person's performance in attentional tasks[20] or indicate sympathetic responses.[21] Specificities of ridges on fingerprints (dermatoglyphics) can also contribute to diagnosis of certain illnesses, as some can be correlated with genetic abnormalities.[22] Heart rate can be measured with help of camera from a fingerprint, and potential abnormal functioning of heart could be detected.[23]

Face is a rich source of various kinds of information. Naturally, facial images can be analysed to indicate age,[24] gender,[25] racial, ethnic or cultural origin,[26] emotions,[27] or even facial attractiveness.[28] With help of machine-vision algorithms, various diseases can be detected from face as well.[29]

Iris images ran reveal information about abnormalities or diseases such as cataract, acute glaucoma, posterior and anterior synechiae, retinal detachment, rubeosis iridis, corneal vascularization, corneal ulcers, haze or opacities, corneal grafting, or iris damage and atrophy.[30]

---

[18] SHIVAKUMAR, G., VIJAYA, P. A. Emotion Recognition Using Finger Tip Temperature: First Step towards an Automatic System. *International Journal of Computer and Electrical Engineering*. 2012, Vol. 4, No. 3, [2017-12-17]. Available at: <http://www.ijcee.org/papers/489-P005.pdf>.

[19] HERBORN, K. A., GRAVES, J. L., JEREM, P., EVANS, N. P., NAGER, R., MCCAFFERTY, D. J., MCKEEGAN, D. E. F. Skin temperature reveals the intensity of acute stress. *Physiology & Behavior*. 2015, 152(Pt A), [2017-12-17]. Available at: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4664114/>.

[20] VERGARA, R., MOËNNE-LOCCOZ, C., MALDONADO, P. E. Cold-Blooded Attention: Finger Temperature Predicts Attentional Performance. *Frontiers in Human Neuroscience*. 12 September 2017, [2017-12-17]. Available at: <https://www.frontiersin.org/articles/10.3389/fnhum.2017.00454/full>.

[21] KISTLERA, A., MARIAUZOULSB, C., VON BERLEPSCHA, K. Fingertip temperature as an indicator for sympathetic responses. *International Journal of Psychophysiology*. 1998, Volume 29, Issue 1, [2017-12-17]. Available at: <http://www.sciencedirect.com/science/article/pii/S0167876097000871>.

[22] Dermatoglyphics. In: *Wikipedia* [online]. 17. 12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Dermatoglyphics>.

[23] See Measuring heart rate with a smartphone camera. In: *uavster* [online]. 10. 9. 2013 [2017-12-17]. Available at: <http://www.ignaciomellado.es/blog/Measuring-heart-rate-with-a-smartphone-camera> and HEWITT, J. MIT researchers measure your pulse, detect heart abnormalities with smartphone camera. In: *ExtremeTech* [online]. 21. 6. 2013 [2017-12-17]. Available at: <https://www.extremetech.com/computing/159309-mit-researchers-measure-your-pulse-detect-heart-abnormalities-with-smartphone-camera>.

[24] Automatic feature detection and age classification of human faces in digital images. In: *Google Patents* [online]. 18. 2. 1994 [2017-12-17]. Available at: <https://patents.google.com/patent/US5781650A/en>.

[25] KHAN, S. A., NAZIR, M., AKRAM, S., RIAZ, N. Gender classification using image processing techniques: A survey. *2011 IEEE 14t^h^ International Multitopic Conference (INMIC)*. 2011, [2017-12-17]. Available at: <http://ieeexplore.ieee.org/document/6151483/>.

[26] LU, X., JAIN, A. K. Ethnicity identification from face images. *Proceedings of SPIE*. 2004, Vol. 5404, [2017-12-17]. Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.10.2036&rep=rep1&type=pdf>.

[27] PADGETT, C., COTTRELL, G. Representing Face Images for Emotion Classification. *Advances in Neural Information Processing Systems 10 (NIPS 1997)*. 1997, [2017-12-17]. Available at: <https://papers.nips.cc/paper/1180-representing-face-images-for-emotion-classification.pdf>.

[28] KAGIAN, A., DROR, G., LEYVAND, T., MEILIJSON, I., COHEN-OR, D., RUPPIN, E. A machine learning predictor of facial attractiveness revealing human-like psychophysical biases. *Vision Research*. 2008, Vol. 48, No. 2, [2017-12-17]. Available at: <http://www.sciencedirect.com/science/article/pii/S0042698907005032>.

[29] WANG, K., LUO, J. Detecting Visually Observable Disease Symptoms from Faces. *EURASIP Journal on Bioinformatics and Systems Biology*. 2016, Vol. 13, [2017-12-17]. Available at: <https://bsb-eurasipjournals.springeropen.com/articles/10.1186/s13637-016-0048-7>.

[30] TROKIELEWICZ, M., CZAJKA, A., MACIEJEWICZ, P. Database of iris images acquired in the presence of ocular pathologies and assessment of iris recognition reliability for disease-affected eyes. *2015 IEEE 2^nd^ International Conference on Cybernetics (CYBCONF)*. 2015 [2017-12-17]. Available at: <http://ieeexplore.ieee.org/document/7175984/>.

Voice can be analysed for instance for gender, age, emotional state (anger, joy, fear or extreme fear, sadness, boredom, happiness, distress), or state of health.[31] For instance, illnesses such as Parkinson's disease,[32] praedementia and Alzheimer's disease[33] can be detected from voice. Literature mentions correlations of voice with symptoms of various mental disorders (schizophrenia, depression, autism, Huntington's disease, or suicidal tendencies),[34] as well as other traits such as *"dominance and attractiveness, threat potential, social status, personality, sexual orientation, level of self-consciousness etc."*.[35] Moreover, voice can be correlated also with hormone levels or with use of prescription medication.[36] Voice can also indicate that a speaker perceives difference in social status between herself and a listener[37] or that the speaker probably lies.[38]

Keystroke dynamics can be analysed for age,[39] gender,[40] emotional states such as happiness or stress,[41] for Parkinson's disease[42] or possibly for sleep inertia.[43]

It is obvious that biometric technologies, that are currently used on a daily basis by a vast number of people due to their user friendliness and comfort, already now reveal a significant amount of additional information. This information available in a digital form

[31] JOHAR, S. *Emotion, Affect and Personality in Speech. The Bias of Language and Paralanguage*. Springer, 2016. See Chapter 2.

[32] HAZAN, H., DAN, H., MANEVITZ, L., RAMIGAND, L., SAPIR, S. Early Diagnosis of Parkinson's Disease via Machine Learning on Speech Data. *2012 IEEE 27th Convention of Electrical Electronics Engineers in Israel (IEEEI)*. 2012 [2017-12-17]. Available at: <http://ieeexplore.ieee.org/document/6377065/>.

[33] KÖNIG, A. et alt. Automatic speech analysis for the assessment of patients with predementia and Alzheimer's disease. *Alzheimer's & Dementia: Diagnosis, Assessment & Disease Monitoring*. 2015, Vol. 1, No. 1, [2017-12-17]. Available at: <http://www.sciencedirect.com/science/article/pii/S2352872915000160>.

[34] SINGH, R., BAKER, J., PENNANT, L., MORENCY, L. P. Deducing the Severity of Psychiatric Symptoms from the Human Voice. In: *arXiv* [online]. 15. 3. 2017 [2017-12-17]. Available at: <https://arxiv.org/pdf/1703.05344.pdf>.

[35] Ibid.

[36] Ibid.

[37] LEONGÓMEZ, J. D., MILEVA, V. R., LITTLE, A. C., ROBERTS, S. C. Perceived differences in social status between speaker and listener affect the speaker's vocal characteristics. *PLOS ONE*. 2017, Vol. 12, No. 6, [2017-12-17]. Available at: <http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0179407>.

[38] HOLLIEN, H., GEISON, L., AND HICKS, J. Voice Stress Evaluators and Lie Detection. *Journal of Forensic Sciences*. 1987, Vol. 32, No. 2, [2017-12-17]. Available at: <https://www.astm.org/DIGITAL_LIBRARY/JOURNALS/FORENSIC/PAGES/JFS11143J.htm>.

[39] TSIMPERIDIS, G., KATOS, V., ROSTAMI, S. Age Detection Through Keystroke Dynamics From User Authentication Failures. *International Journal of Digital Crime and Forensics (IJDCF)*. 2017, Vol. 9, No. 1, [2017-12-17]. Available at: <http://eprints.bournemouth.ac.uk/25123/>.

[40] TSIMPERIDIS, I., KATOS, V., CLARKE, N. Language-independent gender identification through keystroke analysis. *Information and Computer Security*. 2015, Vol. 23, No. 3, [2017-12-17]. Available at: <http://www.emeraldinsight.com/doi/abs/10.1108/ICS-05-2014-0032>.

[41] FAIRHURST, M., LI, C., ERBILEK, M. Exploiting biometric measurements for prediction of emotional state: A preliminary study for healthcare applications using keystroke analysis. *2014 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BIOMS) Proceedings*. 2014, [2017-12-17]. Available at: <http://ieeexplore.ieee.org/document/6951539/>.

[42] ELLINGTON, A. D., RIEDEL, T., WINKLER, D., KNIGHT, E. Keystroke Analytics for Non-Invasive Diagnosis of Neurodegenerative Disease. In: *University of Texas at Austin. Center for Identity* [online]. 2015 [2017-12-17]. Available at: <https://identity.utexas.edu/assets/uploads/publications/Ellington-2015-Keystroke-Analysis-Non-Invasive-Diagnosis-Neurodegenerative-Disease.pdf>.

[43] GIANCARDO, L., SÁNCHEZ-FERRO, A., BUTTERWORTH, I., MENDOZA, C. S., HOOKER, J. M. Psychomotor Impairment Detection via Finger Interactions with a Computer Keyboard During Natural Typing. *Scientific Reports*. 2015, No. 5, [2017-12-17]. Available at: <https://www.nature.com/articles/srep09678>.

can and shall lead to its mass processing for various purposes. Such practice will stimulate even deeper research on correlations of various biological and behavioural characteristics. Some of this research will be done for internal purposes of companies and might never become available to public.

All of the possibilities described above increase vulnerability of individuals not only by revealing correct information about them to other subjects, but also by revealing incorrect information. Biometrics as such is not fully reliable. The same is valid for detection of augmented informative value of data. Information can be derived only in varying degrees of probability. However, even this information can be valuable for some subjects who might try to utilize its potential. It must be also noted, that diseases are mostly connected with certain symptoms and complications. These might be then derived as secondary information with yet less probability and, therefore, reliability.

3. RISKS RELATED TO AUTOMATED PROCESSING OF BIOMETRIC DATA

With regard to vulnerability of individuals, two factors are of great importance in biometric systems: monitoring sensors and algorithms that process information gathered from these sensors.

Sensors in biometrics vary according to the biometric technology used. Biometric sensors are transducers that convert information about a biometric treat of an individual into an electrical signal. They measure various kinds of energies, such as pressure, temperature, light, speed, etc.[44] Faces can be recognized with use of cameras or with infrared sensors, voice with use of microphones, fingerprints with optical, silicon or ultrasound sensors.[45]

Sensors are critical especially with regard to the amount and precision of data they can gather from an individual. The higher amount and the more precise data increase chances in deriving additional information from the biometric sample, such as specificities of biological functioning of an individual, symptoms of her diseases, information about her current state or her identity. Such information can be derived with help of special algorithms.

Biometric algorithms are in fact pattern recognition systems. As it was already stated above, pattern recognition is used also for the purposes of spotting anomalies and diagnosing diseases. Despite a certain level of technical standardization, each algorithm processes information in an original manner. Moreover, vast amounts of algorithms for processing gathered biometric treats are proprietary and, therefore, secret by their nature. For users of biometric systems, it is basically impossible to determine what information is gathered about them and how it is further processed. They must rely on the guarantees provided to them by the subject who operates the biometric system. At the same time, interests of subjects operating a biometric system and natural persons enrolled in this system do not need to be same. These interests might be even contradictory. Guarantees then might not be genuine.

[44] PARZIALE, G. Biometric Sensor and Device, Overview. In: LI, S. Z., JAIN, A. K. (eds.). *Encyclopedia of Biometrics*. Springer, 2009.

[45] VACCA, J. R. *Biometric Technologies and Verification Systems*. Oxford: Elsevier, 2007.

In order to find out whether the operators comply with own policies and what data a system is processing in which manner, a user would have to perform reverse engineering on the software running in the system. In most cases, a user will not even have access to this software. She could theoretically analyze application running for instance on her smartphone that utilizes information from fingerprint sensor. However, she may even not know that some application is using either the fingerprint sensor or a camera. This information is hard to detect and a special monitoring software is needed. Unusual activity in a smartphone can be also revealed when the device is sending data even though it should not be communicating at that moment. Still, it will not be possible to determine the information that is being communicated.

Unfortunately, opacity is inherent when processing most kinds of data by automated means. This opacity could be easily misused to the detriment of people whose personal data are being processed. Therefore, law constructs rules aiming at balancing this opacity by providing objective guarantees to natural persons.

4. LEGAL FRAMEWORK

European Union guarantees the right to the protection of personal data to all natural persons as a fundamental freedom. Recently, the EU reformed its data protection legal framework to establish unified rules and to minimize deviations in national laws.

Original Data Protection Directive required national laws to prohibit processing of special categories of data that reveal *"racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life*"[46] as by their nature they are capable *"of infringing fundamental freedoms or privacy*".[47]

The General Data Protection Regulation (GDPR)[48] that is directly applicable in all EU Member States as of 25 May 2018 has adopted a similar approach and in principle prohibits processing special categories of data including biometric data. Compared to the Data Protection Directive the Regulation states that processing of these categories of data *"could create serious risks to the fundamental rights and freedoms*".[49] These categories of data can be processed only in exceptional cases specified in Art. 9 of the GDPR.

The GDPR explicitly defines biometric data 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, such as facial images or dactyloscopic data*"[50] and establishes them as a special category of personal data. One must note, however, that the GDPR uses a narrow understanding of

[46] See Art. 8 par. 1 of the Data Protection Directive.
[47] Recital 33 of the Data Protection Directive.
[48] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
[49] Recital 51 of the GDPR.
[50] See Art. 4 par. 14 of the GDPR.

biometrics. Biometrics as such is a broad term including information about *"individual aspects of constitution or functioning or behaviour of a biological organism*".[51] As such biometric data in a broad sense can be evaluated for various purposes and additional information can be inferred just as it was presented in the previous sections. A *"process of extrapolating information about a person based on his or her known traits or tendencies*" is referred to as profiling.[52]

The dangers and risks of using biometric data for profiling have already been summarized in literature. Merging unique identifiers of a person with profiling techniques can violate the right of information self-determination, enslave the humankind and result in discrimination.[53]

Profiling is a technique widely discussed in the literature[54] and regulated by the GDPR in the Art. 22. Profiling is defined as *"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 analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*".[55]

Profiling is often connected with re-use of information and processing for other purpose than initially defined. The risk stemming from such re-use of information is referred to as "function creep" as it is related to using technology for other purposes then it was originally intended. Such usage *"may result in unanticipated use of personal data by the controller or by third parties and in loss of data subject control*".[56] The function creep can develop either little by little or a controller can have a hidden agenda from the very beginning. Biometrics then can be misused for generating unauthorized information.

The GDPR allows for processing for other than originally defined purpose in Art. 6 par. 4 on the condition, that the purposes would be compatible. The GDPR provides guidelines on assessing compatibility of purposes. Special categories of data must be assessed with a special care.

In the GDPR, profiling is tightly connected with automated decision-making. Data subjects are guaranteed a right not to be subject to an automated decision-making[57] including

[51] MATEJKA, J., KRAUSOVÁ, A., GÜTTLER, V. Biometrické údaje a jejich právní režim. *Revue pro právo a technologie*. 2018, Vol. 9, No. 17, [2018-07-10]. Available at: <https://journals.muni.cz/revue/article/view/8801/pdf>.

[52] KINDT, E. J. *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis*. Dordrecht: Springer, 2013. See p. 349.

[53] Ibid., p. 351–352.

[54] For instance HILDEBRANDT, M., GUTWIRTH, S. (eds.*). Profiling the Eropean Citizen. Cross-Disciplinary Perspectives*. Springer, 2008; or recently MENDOZA, I., BYGRAVE, L. A. The Right Not to be Subject to Automated Decisions Based on Profiling. In: T.-E- Synodinou et al. (eds.). *EU Internet Law. Regulation and Enforcement*. Cham: Springer, 2017.

[55] Art. 4 par. 4 of the GDPR.

[56] ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on consent under Regulation 2016/679. WP259 rev.01. In: *European Commission* [online]. 2018 [2018-07-10]. Available at: < https://webcache.googleusercontent.com/search?q=cache:l-b4dUk35iAJ:https://ec.europa.eu/newsroom/article29/document.cfm%3Faction%3Ddisplay%26doc_id%3D51030+&cd=1&hl=en&ct=clnk&gl=cz&client=firefox-b-ab>.

[57] The nature of this right is not so clear as some do not consider it a specific right but rather a set of obligations of a controller.

profiling. However, profiling can be done even without any decision making. If other requirements of the GDPR are met (principles and lawfulness of processing), then data subject cannot object to profiling. The importance of decision-making lies in the fact that decision-making can be done to the detriment of a data subject, while deriving extra information that would not influence behaviour of a controller towards a data subject is deemed relatively harmless.

Special attention must be paid also to the possibility of profiling done by other than automated means. Despite the WP29 stated in its opinion that profiling does not always require automated means to be considered as profiling within the meaning of the GDPR,[58] it is questionable if deriving additional information from biometric data done manually or by a person would qualify as profiling at all. This could be compared to making a diagnose by a doctor.

5. SAFEGUARDS IN THE GDPR

With regard to processing any type of personal data, the GDPR requires the processing to be as transparent as possible. Obligation of transparent processing is set out in general in Art. 5 on principles of processing personal data and specified in Art. 12 of the GDPR. WP 29 even issued guidelines on how to fulfil transparency requirements properly.[59]

Transparency is intended to lift negative effects of inherent opacity in processing personal data which often results in absence or significant reduction of control over own personal data. People, whose personal data is processed (data subjects), are entitled for both transparent information as well as transparent communication. This involves requirements on the language used which should be clear and plain. At the same time information should be concise, intelligible and easily accessible.[60] Only those who truly understand what processing their personal data entails are able to decide whether, and under which conditions, they are willing to give consent with such processing to a person who shall process the data (a controller).[61] However, it has been proven that with such a growing amount of data processing, data subjects are unable to read and comprehend all privacy policies and remember all consents they have granted. Moreover, in case of subversive use of biometrics from the very beginning, the controllers might avoid informing the data subject by design calculating risk of the probability that such practice would ever be revealed. Unfortunately, the saying *"you cannot protect yourself from discrimination if you are not aware of the fact that you are being discriminated*" can be applied also to pro-

[58] ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. WP251 rev.01. In: *European Commission* [online]. 2018 [2018-07-10]. Available at: < https://webcache.googleusercontent.com/search?q=cache:l-

[59] ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on transparency under Regulation 2016/679. WP260. In: *European Commission* [online]. 2017 [2017-12-28]. Available at: <http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850>.

[60] Ibid.

[61] A controller is defined in Art. 4 point 7) of the GDPR as *"the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*".

filing that is, in fact, often intimately connected with discrimination. Data subjects may not have a slightest idea about being used as a source of information about their physical or psychological condition.

Transparency is related also to the right to explanation of a data subject who shall be Controllers are required to process personal data lawfully. Their activities could be investigated by a national supervisory authority. This measure should help to guarantee compliance of processing. Unfortunately, given the number of controllers registered at a supervisory authority and the capacity of this authority, possible incidents cannot be handled in a timely manner.[62] Moreover, some controllers violate their obligation to register and are unknown to the authority. As biometric data can be obtained and processed remotely as well as secretly, law enforcement may fail in protection of data subjects.

In order to minimize violation of laws, the GDPR introduced a new legal institute – a data protection officer. According to Art. 37 par. 1 point c) of the GDPR, a data protection officer must be appointed in cases when processing biometric data represents the main activity of the controller.

Data protection officer is entitled to have access to all information related to processing personal data. This implies that she should also have access to the source code in order to check its real functionalities. Role of the data protection officer is to secure a constant overview of activities during processing personal data. As data subjects have limited means of checking real actions of a controller, data protection officer serves as a guarantee of lawful and legitimate ways of processing. Unfortunately, despite designating a data protection officer is a reasonable solution to problems with opacity of data processing, in practice this institution can fall short of fulfilling its function for various reasons. The main reason could be that a company would not designate a data protection officer and after gathering a sufficient amount of biometric data would be liquidated. There are always possibilities how to circumvent the law. With regard to biometric data, this, however, could significantly influence fundamental freedoms and rights of data subjects.

6. PRIVACY IMPLICATIONS

Privacy implications of processing biometric data are serious. Processing biometric data is subject not only to threats common to processing of all personal data such as circumvention of laws or sometimes their inefficient enforcement, but also to threats of losing anonymity resulting in reduction of unmonitored space for living as well as to threats of unknowing provision of highly sensitive data that might be unknown even to the data subject. Moreover, this information would be uniquely linked to an individual due to the special nature of biometric data. Cross-referencing biometric data across other databases and providing additionally inferred information to other controllers significantly increases vulnerability. The main feature that makes biometrics so popular is its comfortability and unobtrusiveness. This unobtrusiveness, however, significantly contributes to the lack of

[62] For instance, the Czech Data Protection Office has over 65.000 registered controllers. For details see Public Registry of Personal Data Processing at https://www.uoou.cz/verejny-registr-zpracovani-osobnich-udaju.asp.

transparency and its effects might not even be efficiently corrected by law. The solution to this problem lies in developing independent software for testing current biometric systems used especially in the phones and laptops, adhering to technical standards for biometrics and propagation of independent certification of biometrics.

CONCLUSION

The aim of this paper was to present the concept of augmented indicative values of biometric data and to identify critical factors that increase vulnerability of data subjects. It has been illustrated that processing biometric data has serious implications for privacy of individuals not only because of their quality to be linked to an individual but also because biometric data can be analysed for extraction of additional information directly related to their identity, mental and biological functioning as well as prognosis of this functioning. Legislators are aware of the sensitivity and harmful potential of biometric data and, therefore, prohibit its processing in general. This prohibition can, however, be lifted by a consent of a data subject to whom the biometric data pertains. Due to user comfort, the technology is spreading and becomes widely accepted by users all around the world. Users are often willing to grant their consent to controllers. This is sometimes because of their unawareness of possible impacts that collection and processing of this data may have on their privacy and life. Unfortunately, the level of unawareness is growing. With regard to the very nature of automated processing, biometric data can be analysed not only for patterns that distinguish them from other individuals, but also for deriving information based on public knowledge of biomarkers and other indicative factors. Even such commonly used technology of fingerprint recognition can, depending on a processing algorithm, determine gender, ethnicity, current mental state or probability of suffering from a genetic disease.

Automated processing of personal data is inherently opaque. Despite the GDPR requires transparency of processing personal data and requires designation of a data protection officer, there is still a high chance that the GDPR will not be adhered to by small companies or individuals, or that the GDPR will be circumvented. Currently, the only truly efficient means of protection of biometric data from being potentially analysed for additional information lies in hands of data subjects who should either carefully choose trusted companies or avoid using biometrics. In some cases, such as with devices owned by data subjects (i.e. smartphones or laptops), the data subjects could use an independently developed software that would check the factual operation of software that operates biometric sensors.