Article title: Technological, legal, and sociological summary of biometric technology usage
Authors: Ondrej Kanich[1], Jan Matejka[2], Eva Fialova[3], Marcela Petrova Kafkova[4], Tomas Dosedel[5], Martin Drahansky[6]
Affiliations: Faculty of Information Technology, Brno University of Technology, Brno, 612 00 Czech Republic[1], The Institute of State and Law, Czech Academy of Sciences, Praha, 116 00 Czech Republic[2], Department of Sociology, Faculty of Social Studies, Masaryk University, Joštova 10, Brno, 602 00 Czech Republic[3]
Orcid ids: 0000-0003-0093-8536[1]
Contact e-mail: kanich@fit.vutbr.cz

Funder: The Technology Agency of the Czech Republic
DOI: 10.14293/S2199-1006.1.SOR-.PP4IOF2.v1
Preprint first posted online: 15 September 2022
Keywords: biometrics, law, social groups

Technological, legal, and sociological summary of biometric technology usage

Ondřej Kanich[1], Ján Matejka[2], Eva Fialová[2], Marcela Petrová Kafková[3], Tomáš Doseděl[3], Martin Drahanský[1]

[1]Faculty of Information Technology, Brno University of Technology, Brno, 612 00 Czech Republic
[2]The Institute of State and Law, Czech Academy of Sciences, Praha, 116 00 Czech Republic
[3]Department of Sociology, Faculty of Social Studies, Masaryk University, Joštova 10, Brno, 602 00 Czech Republic

Corresponding author: Ondřej Kanich (e-mail: kanich@fit.vutbr.cz).

This research has been realized under the support of the following grants: The Technology Agency of the Czech Republic from the ÉTA programme "Survey and education of citizens of the Czech Republic in the field of biometrics – TL02000134" and "Reliable, Secure, and Efficient Computer Systems" – internal Brno University of Technology project FIT-S-20-6427 (CZ).

ABSTRACT The article presents biometric systems from three different standpoints. Technological standpoint, where the focus is laid on biometric system usage by the general public. Explaining basic terms and difficulties using various biometric characteristics. It also shortly describes how recognition works in several biometric characteristics (fingerprint, face, iris, and signature). After that is the legal standpoint, which is focused mainly on European Union law, where the often-mentioned GDPR is discussed, this basic legal regulation places a significantly higher standard than the previous legislation on the processing of biometric data as a particular category of personal data. Lastly, the article shows a sociological standpoint. In that part, different attitudes towards biometric technologies are discussed within the world population and different groups of the Czech Republic population. In the latest survey done by the authors in 2020 was found that age, and education play a vital role in the knowledge about biometric systems.

I. INTRODUCTION

Biometrics is a more and more used term nowadays. The general public is getting accustomed to using this technology as they buy new devices or are forced by higher entities (banks, state agencies, insurance companies, etc.). This article focuses on a complex overview of biometrics from a technological, legal, and sociological standpoint. Paper is focused mainly on biometrics usage in the European Union; sociological research was done in the Czech Republic. Technological part is concentrated in biometrics as an identification method. It also describes various biometric characteristics, focusing on the most common and accessible modalities for the public. The legal part of the article focuses mainly on the current regulation and legislation applied to the biometric data. Obligations of controllers that process this kind of data are described as well. The last part is describing biometrics from the sociological point of view. It is focused on answering questions like What the population knows about the technology they are using? How is biometrics perceived by different age groups? What about the influence of education or house of residence?

II. HOW THE BIOMETRIC RECOGNITION WORKS?

For better understanding, an explanation of the term *biometrics* is needed. In the context of this work, biometrics is an automated recognition of people based on their distinct biological and behavioral characteristics [1]. This recognition is used to determine the person's identity (or claimed identity). Identity could be authenticated by two different methods. The first one is *verification*. In this case, users enter their identity (name, email, ID) and then present the biometric characteristics [2]. Entered identity is either accepted or rejected (based on the given characteristics). The second method is *identification*. When users present characteristics and recognition systems have to present possible identity (or identities) or reject them as the user is not enrolled in the system [2].

Recognition is based on either something the user *knows* (e.g., password) or something the user *has* (e.g., keys), or something the user *is* (e.g., fingerprints) [3]. Biometrics is describing the last possibility. Because it is an integral part of the user's body (or behavior), it cannot be lost or forgotten. On the other hand, the significant disadvantage of using biometric recognition is the *comparison score*. In other means of verification, you either get accepted or rejected (there is not something like an almost correct password). On the other hand, in biometric recognition getting the exact same captured biometric sample is very suspicious.

As it was said the comparison in biometrics results in a comparison score. If the score meets the defined threshold then

the captured sample is accepted. If it is not met, then it is rejected. The various definitions of threshold lead to various *false acceptance rates* (FAR, statistical type I error, or false positive) and *false rejection rates* (FRR, statistical type II error, or false negative) [3]. Biometric systems try to minimize both, but overall a very secure system has very low FAR and possibly high FRR, on the contrary a very user-friendly system has high FAR but very low FRR. An explanatory image of both metrics is shown in Fig. 1. As can be seen, different threshold settings would result in different FAR/FRR metrics.

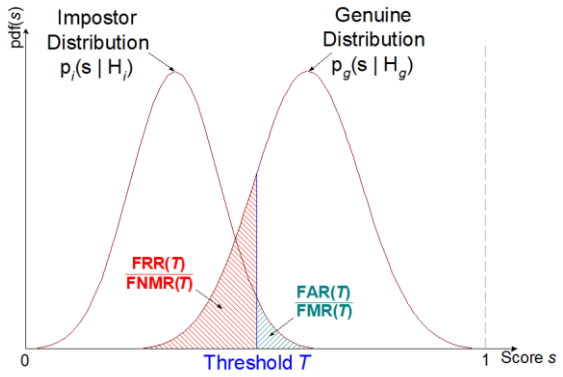

Fig. 1: Visualization of FAR/FRR metrics and their threshold relation.

The general biometric system consists of five units: sensor, extractor, database, comparator, and application [2]. *The sensor* unit is responsible for capturing biometric samples from the presented characteristic. The function of the *extractor* is to extract essential parts of the sample and create a set of biometric features. This set of features is stored in a *database* as a biometric template. If the biometric system usage goal was to register (save) a new user, then the process ends. Otherwise, if the goal was to verify (note that identification is a systematic process of many verifications) the process continues with comparison. *The comparator* takes the presented template and template from the database and compares them. The result is the comparison score which is exported into an *application*.

A. BIOMETRIC CHARACTERISTICS

Huge variety of biometric characteristics could be used for recognition of the person. In this article, the focus is laid on the several characteristics which are commonly used among the general public. Every characteristic has its advantages and disadvantages. Generally, the most important properties are price, accuracy, and scale. These properties are closely related, and the change of one influences the others.

A closer look at the ideal biometric characteristic results in eight basic properties [3] [4]. *Universality* describes that everyone should have this characteristic. *Uniqueness* defines that two persons should not have the same characteristic. *Permanence* is property connected to changes in the characteristic over time. *Measurability* shows how easy it is to acquire the characteristic. *Performance* defines that characteristic achieves sufficient accuracy. *Acceptability* describes how users are willing to use specific characteristics. *Circumvention* determines how easy it is to create presentation attack instruments (spoofs, fakes). The last property is the *price* of the solution. The general public would not use, even the excellent biometric characteristic, if the solution is too expensive. There is no biometric characteristic in the praxis that would perfectly fulfill all these properties. In the end, choosing the right characteristic depends on presumed usage. The most known (and used) biometric characteristics will be described in the following subsections.

1) FINGERPRINTS

Probably the most known and used biometric characteristics. The fingerprint itself is an image of ridges (and valleys) pattern on the fingertip surface. Usually, for identification the *minutiae* are used which are interconnections or divisions of the ridges (see Fig. 2) [4]. Each finger of the same person has different fingerprints, and also fingerprints of the twins are different [3]. Based on the orientation of the ridges, there is a possibility to classify fingerprints into three (but usually into five or six) classes [2]. From the properties, standpoint fingerprint excels in uniqueness, permanence, performance, circumvention, and price.

Fig. 2: Acquired and processed fingerprint image.

2) FACE

This biometric characteristic is the most natural for humans. Almost every one of us can pretty accurately recognize our relatives and close friends even in difficult situations. Automated recognition can be based on the mutual position and location of several key points in our face (e.g., eyes, mouth, nose, etc.) [2], see Fig. 3. Nowadays, the most typical recognizers use deep neural networks whose decision (and recognition) process is not exactly clear (generally it just uses the whole image of the face) [2]. As it is known, twins have very similar faces. Universality, measurability, acceptability, and price are typically high properties for face recognition.

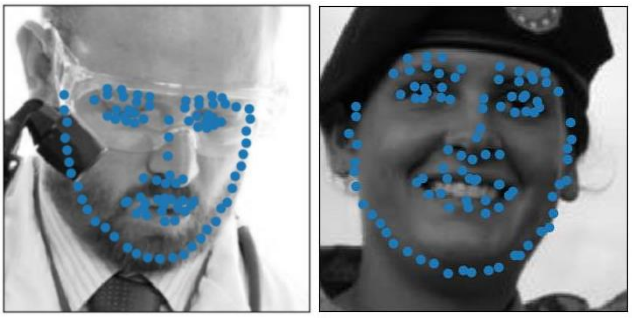

Fig. 3: Example of face images with detected key points.

3) IRIS

Iris recognition concludes three standardly used biometric characteristics in biometric passports (fingerprint, face, iris). The visual texture of the iris (which is a colored ring between sclera and pupil) is used (see Fig. 4) [2]. For the recognition the shape of the formations in the iris are more important than the color itself [2]. Each iris is different, meaning that also twins have different irises. Iris recognition excels in universality, uniqueness, permanence, performance and circumvention.

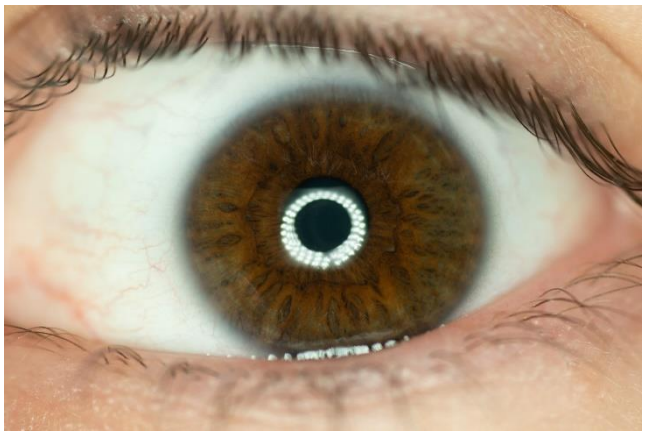

Fig. 4: Detailed image of iris.

4) SIGNATURE

Signature is the most common characteristic used by humans in everyday life. Shape of the written signature (static feature) is used for the recognition. Nowadays, some systems can also use the information about how the signature was created (dynamic features). That is, speed, pressure, and other values describing the movement of the pen [3]. Signature is one of the only (if not only) characteristics where it is possible to capture both dynamic and static features simultaneously (see Fig. 5). Unfortunately, signature recognition systems are generally used without these dynamic features, and the accuracy of static features is very low. In these cases, the only properties in which a signature is sound is measurability and acceptability, in all the others are ranked very low.

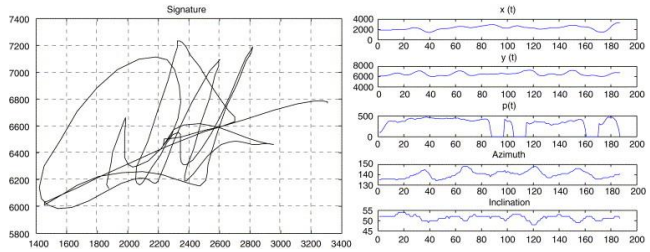

Fig. 5: Example of signature with static and dynamic features (taken from [5]).

5) OTHER CHARACTERISTICS AND COMBINATION

There are many other characteristics that were not mentioned, for example: DNA (the "ultimate" biometric characteristic), hand geometry, thermograms (usually of a face), finger or palm vein formation, retina, voice, gait, and others [2] [3]. These are typically used in specific cases or just not so often. It is possible to combine characteristics together and create a *multimodal* biometric system. In this case, that expects more than one biometric characteristic as input and decides based on the evaluation of all comparison scores. That further enhances the system's accuracy, making it more robust and circumvention harder.

III. BIOMETRIC DATA REGULATION IN THE EUROPEAN UNION

The processing of the biometric data in Europe is regulated by the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ("GDPR"). GDPR lays down rules relating to the protection of natural persons also regarding the processing of personal data and fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and the right to privacy. GDPR is built on a risk-based approach. The greater the risk to individuals' rights and freedoms the processing of personal data or the nature of the data presents, the more obligations GDPR imposes on the persons processing the personal data, i.e., controllers.

A. LEGAL-NORMATIVE APPROACH

According to Art. 4 (1) GDPR, personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person can be identified, directly or indirectly, in particular by reference to one or more factors specific, among other characteristics, to the physical, physiological, genetic or mental identity of that natural person.

Pursuant to art. 4 (14) GDPR biometric data means 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 dactyloscopic data. The biometric data processed for a purpose of unique identification of an individual (data subject) are personal data that belong to a so-called special categories of data. Although art. 9 (1) GDPR refers to the identification, this regulation covers both identification as well as authentication [6]. The authentication is explicitly mentioned in recital 51 GDPR. The processing of the special categories of data is pursuant to this article prohibited unless GDPR explicitly allows to process those data. The data controller (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) can process the biometric data e.g. if the data subject has given explicit consent. The controller that processes biometric data on the basis of the explicit consent must always be able to demonstrate that such consent has been given and, moreover, that it has been given freely. Article 29 Data Protection Working Party, predecessor of the European Data Protection Board considers the explicit consent as an express statement of consent [7]. The consent must be an active, a pre-marked consent in the electronic form does not represent a valid consent [8].

B. LAWFUL BASIS FOR PROCESSING

The controller has many obligations when processing personal data, not only biometric data. The controller has to stick to the principles of data processing. Personal data must be processed lawfully, fairly and transparently and collected for specified, explicit, and legitimate purposes (principles of anonymity, proportionality, and purpose binding). The controller has to process the necessary data for the purpose and accurate and updated. The purpose determines a time limit for processing. The controller must take appropriate security measures to ensure the integrity and confidentiality of the data.

The lawfulness of processing means that the controller can process the data when there are one or more legal grounds for processing enumerated in art. 6 GDPR. Besides the explicit consent, the processing must be necessary

- for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject before entering into a contract;
- for compliance with a legal obligation to which the controller is subject;
- to protect the vital interests of the data subject or of another natural person;
- for the performance of a task carried out in the public interest or the exercise of official authority vested in the controller; or
- for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject that require personal data protection.

C. PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

The controller that processes special categories of data has some other obligations. Since the processing of biometric data constitutes a risk to the rights and freedoms of natural persons, the controller, as well as the processor must implement according to art. 32 GDPR appropriate technical and organizational measures to ensure a level of security appropriate to the risk. The implemented measures depend on the consideration of the controller (or the processor). The controller is accountable for the mitigation or elimination of risk.

The leakage or another integrity or security breach of biometric data will probably result in the obligation of the controller to notify the data breach to a supervisory authority under art. 33 GDPR. This notification must occur since the violation of biometric data usually presents a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result even in a high risk to the rights and freedoms of natural persons, the controller must communicate the personal data breach to the data subject.

High risk to the rights and freedoms of natural persons means that the controller has to carry out a so-called data protection impact assessment (DPIA), elements of, which are described in art. 35 GDPR. The DPIA serves as a tool for the controller to eliminate the risks for data subjects connected with the processing. The DPIA is required, i.e. in the case of processing on a large scale of special categories of data.

Suppose the core activities of the controller or the processor consist of processing on a large scale of special types of data. In that case, the controller or the processor has to designate a data protection officer who monitors compliance with the data protection law and recommends proper steps in data processing (art. 36 GDPR).

GDPR is not the only law that regulates the use of biometric data. The biometric data is used in travel documents, ID cards, or driving licenses. Since the state issues these documents, the application and holding thereof are regulated by special legislation. The biometric data are processed during the application of a biometric passport following Act no. 329/1999 Coll., on the travel document. The identity of the holder is verified based on biometric data. The same function has biometric data in a residence permit card issued to third-country nationals according to Act no. 326/1999 Coll., on the Residence of Aliens in the Territory of the Czech Republic.

D. TOWARDS A LEGAL PERSPECTIVE ENCOMPASSING SOCIAL IMPACT

The data protection principles of anonymity, proportionality and purpose binding should be upheld when it comes to the handling of biometric data by GDPR. The key in which the traditional core identity is stored will shift from standard alpha-numerical to biometric in the near future. The use of biometrics creates additional risks to privacy and data protection that must be mitigated through legal and technical

controls [9]. To maintain adequate standards of security, all reasonable technical privacy options for the use of biometric data should be used. Therefore, it is necessary to insist on the thorough application of all related legal and technological guarantees against the misuse of this sensitive data and on the simultaneous existence of a clear legal title; all this with regard to the legal framework of data subject (human) rights where the protection of the fundamental right to human dignity, i.e. the right to the fulfilment of which practically almost all other human rights directly or indirectly lead, necessarily plays a leading role.

IV. PUBLIC KNOWLEDGE OF THE BIOMETRICS

Biometric systems are still rather new in everyday usage, but their utilization is growing. Covid epidemic emphasized remote and contactless ways of verification and payments, which escalated the use of biometric systems. Society's attitude and knowledge of these systems are rapidly changing. Despite that, the current understanding of the topic will be described.

Present knowledge about biometrics and worries about its usage is culturally conditioned. A comparison of attitudes of Finland, Germany, and Spain populations showed greater understanding of German population which was associated with a more positive attitude towards biometrics [10]. Reference [11] found high intercultural differences in attitudes to biometrics, with respondents from India perceiving biometrics the most favorably, while respondents from the United Kingdom showed the least positive attitude towards biometrics. Intercultural differences were also found when comparing the attitudes of users from India, Great Britain, and South Africa. Specifically, they found out that Indian respondents evaluated biometric technology as the most acceptable authorization method even better than token-based authorization. South Africans considered biometrics the most acceptable form of authentication, although they preferred biometrics less than Indian respondents. The British evaluated the acceptability of biometrics differently. For them, passwords were the most acceptable form of authentication than the token-based and biometrics authentication.

A. PUBLIC WORRIES TOWARDS THE BIOMETRICS USAGE

Generally, there are two types of worries of (potential) users. Firstly, there are worries about collection of biometric data and the risk of their abuse, and secondly, worries arising directly from biometric data usage, violation of privacy, and reliability of the technology [12]. The research of [11] identified more obstacles of biometric technology acceptance. The most significant were worries of personal data theft, health concerns, and generally the safety of the devices.

Several types of research focused on the specific usage of biometrics. That was the verification before ATM withdrawal and user acceptance of these methods. Reference [13] conclusively identifies that biometric technologies disturb individual autonomy, and its significant expansion for identification by state administration bodies could create a class of marginalized people and, as such is in conflict with the current values of human society. Recently, biometric technologies are growing primarily because of the private sector, not the state administration. Reference [12] conclude that based on the American bank clients' study, the greatest risk of biometric authentication acceptance is the risk of personal data theft or abuse. Awareness of the risk of biometric data theft is the main obstacle for clients' greater acceptance of the biometric verification methods. Reference [14] pointed out that fingerprint authentication leaves a latent fingerprint on the ATM, which could be misused. The important fact is that fingerprint theft is irrevocable. Considerable risk is the existence of extensive fingerprint databases which could be attacked. Another problem lies in the possible usage of the same fingerprint for credit card payment authorization and smartphone verification. User preferences show that people accept biometric authentication in banking, but in retail, there are more vigilant [15].

B. SOCIOLOGICAL DATA FROM THE CZECH REPUBLIC

Besides business-driven surveys focusing on user preferences and behavior towards biometric systems, there was also an omnibus survey realized in September 2018 within regular continuous investigation called “Our society” in the Czech Republic. The Public Opinion Research Centre conducted this survey in the Institute of Sociology of the Czech Academy of Sciences, and it contained several questions focused on the so-called biometrics and its quickly expanding usage in various fields, especially in information technologies. The survey was carried out on a representative sample of 1037 respondents older than 15 years [16]. Except for the survey performed by the authors of this article, these are the most recent quantitative data about biometric system used in the Czech Republic. Because of that, the results of the aforementioned survey will be described more thoroughly.

According to this research, approximately half of the population has some knowledge about biometric data. Thorough analysis shows that more understanding about biometric data has men than women (52 % men vs. 42 % women). Knowledge about the topic does not grow linearly with age; the most knowledgeable are people from the age group from 30 to 44 years (54 % “knows well” or “roughly knows”). On the other hand, the lowest knowledge is in the youngest age group, 15 to 19 years (33 %), and the oldest one 60 years and older (40 %). Declared knowledge is the most conditioned by education, wherein the group with a tertiary education, 29 % “knows well” and other 45 % “roughly knows” what are biometric data.

Meanwhile, in the group with primary education approximately half of them had never heard of biometric data. Significantly better known is the term for big city residents. The opinion that essential technology used by biometric systems must be maximally user-friendly and services should

be adapted to the needs and preferences even at the cost of personal data usage is held by 21 % of respondents. On the other hand, 63 % of people prefer privacy protection at the expense of lower comfort and limitation of personal-focused services. More thorough analysis shows that younger people prefer user comfort and services focused on their individual needs, and with increasing age, the support for this claim is lower. Preference for privacy protection is significantly lower in the youngest group from 15 to 19 years (39 %), overall, 52 % in the age group 29 years and younger. Education level does not change the attitude of the people [16].

1) NEWLY ACQUIRED DATA FROM 2020

The 2020 authors did preliminary research using six focus groups and a representative survey of the Czech Republic population [17]. The goal was to choose respondents so they represent the age, socio-economic and spatial diversity of the Czech Republic population. There is presumed different knowledge in the usage of biometric systems. Analysis of group interviews showed a big difference in knowledge and use of biometrics systems which are age-related. The differences are related to socio-economic status and place of residence.

Children from the capital city in the elementary school age had, in comparison with other groups, not only significantly higher knowledge of the technology in general as well as specifically biometrics but also personal experience with identity theft, data hacking, hacking into accounts (mainly games accounts) and some experience in fingerprint spoof production for unlocking the smartphones. They also had advanced knowledge in data security. It is also a group that uses fingerprint biometrics for locking the smartphone very often. On the contrary, seniors often have their mobile phones completely unsecured based on the thought that there is no sensitive data that should be protected.

In general, almost all of the participants agreed that fingerprint biometrics used for locking smartphones is a comfortable security method without questioning its security. The most significant factor in using biometric technologies is age. The breaking point is the 50th year. Nevertheless, persons with higher education maintain knowledge for about seven years longer. Women have slightly lower knowledge about biometrics and surprisingly there is no difference based on the place of residence.

V. CONCLUSION

This article is looking at the biometric in a complex manner. It discusses the basics of biometrics from three different and very important standpoints. The first one is the one most often mentioned - the technological part. In this part, the basics of how the biometric systems work are described with some information about the most used biometric characteristics (fingerprint, face, iris, and signature). The second standpoint is the legal one, which is closely describing the term GDPR. Looking into obligations for those working with biometric data. Which places a significantly higher standard than the previous legislation on processing biometric data as a special category of personal data. The last standpoint is sociological, the one often neglected. How exactly the non-expert users (general public) are looking at the biometric systems. The attitude towards biometric systems is different around the world and also within different sociological groups. This part is focused on the Czech Republic, where basically only two surveys were done on this matter. The author's results showed a vast difference between knowledge about biometric systems before and after the 50th year of age and that education is having a compensating role (conserving knowledge for about seven years longer).

REFERENCES

[1] *Information technology — Vocabulary — Part 37: Biometrics*, ISO/IEC 2382-37:2017, 2017.

[2] A. K. Jain, P. Flynn and A. Ross, *Handbook of Biometrics*, Springer, 2008, p. 548. DOI 10.1007/978-0-387-71041-9.

[3] M. Drahanský, F. Orság et al., *Biometrie (Biometrics)*, Brno, Czech Republic: Computer Press a.s., 2011, p. 294. ISBN 978-80-254-8979-6.

[4] O. Kanich, "Research in Fingerprint Damage Simulations," Ph.D. dissertation, FIT, Brno Univ. of Technology, Brno, Czech Republic, 2018.

[5] M. Faundez-Zanuy, "On-line signature recognition based on VQ-DTW," *Pattern Recognition*, vol. 40, no. 3, pp. 981-992, Jul., 2007, DOI 10.1016/j.patcog.2006.06.007.

[6] J. Matejka, A. Krausová, V. Güttler et al., *Biometric Data and Its Specific Legal Protection*, Praha, Czech Republic: Institute of State and Law of the CAS, 2020, p. 192. ISBN: 978-80-87439-43-2.

[7] Article 29 Working Party. "Guidelines on consent under Regulation 2016/679," European Data Protection Board, Brussels, Belgium. WP259 rev.01, Apr. 10, 2018. [Online]. Available: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

[8] Judgement of the Court of Justice of the European Union of 1 October 2019. *Case C-673/17 (Planet49)*. [Online]. Available: https://eur-lex.europa.eu/legal-content/GA/ALL/?uri=CELEX:62017CJ0673

[9] J. Matejka, S. Matochová and J. Prokeš, "Analýza biometrických údajů v kontextu obecného nařízení o ochraně osobních údajů (Analysis of biometric data under the general data protection regulation)," *Acta Informatica Pragensia*, vol. 8, no. 2, pp. 88-111, Dec. 2019, DOI 10.18267/j.aip.126.

[10] BioSec Consortium, "Report on results of first phase usability testing and guidelines for developers," BioSec, 2004.

[11] C. Riley, K. Buckner, G. Johnson and D. Benyon, "Culture & biometrics: regional differences in the perception of biometric authentication technologies," *AI & Society*, vol. 24, no. 3, pp. 295–306, Jun., 2009, DOI 10.1007/s00146-009-0218-1.

[12] S. Byun, and S.-E. Byun, "Exploring perceptions toward biometric technology in service encounters: A comparison of current users and potential adopters," *Behaviour and Information Technology*, vol. 32, no. 3, pp. 217–230, Mar., 2013. DOI 10.1080/0144929X.2011.553741.

[13] S. G. Davies, "Touching Big Brother How Biometric Technology Will Fuse Flesh and Machine," *Information Technology & People*, vol. 7, no. 4, pp. 38–47, Dec., 1994, DOI 10.1108/09593849410076807.

[14] P. Greig and J. Irvine, "IEDs on the road to fingerprint authentication: Biometrics have vulnerabilities that PINs

and passwords don't," *IEEE Consumer Electronics Magazine*, vol. 5, no. 2, pp. 79-86, Apr., 2016, DOI 10.1109/MCE.2016.2521978.

[15] P. Jones, P. Williams, D. Hillier and D. Comfort, "Biometrics in retailing," *International Journal of Retail & Distribution Management*, vol. 35, no. 3, pp. 217–222, Mar., 2007, DOI 10.1108/09590550710735077.

[16] Centrum pro výzkum veřejného mínění, "Zpráva z výzkumu: Biometrika a její využívání v pohledu české veřejnosti (Report from research: Biometrics and its usage in scope of Czech population)," CVVM, Praha, Czech Republic, 2018.

[17] M. P. Kafková, T. Doseděl and K. Reimerová, "Výzkumná zpráva: Průzkum a edukace občanů České republiky v oblasti biometrie (Research report: Survey and education of citizens of the Czech Republic in the field of biometrics)," Masaryk University, Brno, Czech Republic, 2021. [Online]. Available: https://webcentrum.muni.cz/media/3338383/precobi_vyzkumna-zprava.pdf