INSTITUTE OF STATE AND LAW
of the Czech Academy of Sciences

Ján Matejka

Alžběta Krausová

Vojen Güttler et al.

Biometric Data and Its Specific Legal Protection

Biometric Data and Its Specific Legal Protection

Biometric Data and Its Specific Legal Protection

Ján Matejka, Alžběta Krausová, Vojen Güttler et al.

CITATION
MATEJKA, J. – KRAUSOVÁ, A. – GÜTTLER, V. et al. *Biometric Data and Its Specific Legal Protection*. Praha: Institute of State and Law of the Czech Academy of Sciences, 2020, 192 p. ISBN 978-80-87439-43-2

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

AUTHORS
JUDr. Ján Matejka, Ph.D.
Mgr. Alžběta Krausová, LL.M.
JUDr. Vojen Güttler
JUDr. Eva Fialová, Ph.D., LL.M.
Hananel Hazan, Ph.D.

REVIEW
Doc. JUDr. Ing. Otakar Schlossberger, Ph.D.
Doc. JUDr. Martin Štefko, Ph.D.

GRAPHICAL LAYOUT
Graphical layout and print: **SERIFA**®, s. r. o., Jinonická 80, 158 00 Praha 5

BOOK COVER PHOTO
www.shutterstock.com

ISBN 978-80-87439-43-2 (print)
ISBN 978-80-87439-44-9 (e-book)

	INSTITUTE
OF	STATE
AND	LAW

Contents

About the Authors

Ján Matejka is the Director of the Institute of State and Law of the Czech Academy of Sciences. Jan is a senior lecturer of Data Protection Law of Faculty of Mathematics and Physics of the Charles University in Prague. He is an author of more than hundred expert and popularization works on Internet and computer law and a grant holder of many projects. His specialties are privacy and data protection, software law, copyright law, labour law, telecommunications law, domain names, license and service contract negotiation, cyberlaw and questions of artificial intelligence and legal liability.

Alžběta Krausová is a legal scholar at the Department of Private Law of the Institute of State and Law of the Czech Academy of Sciences, head of the Center for Innovations and Cyberlaw Research (CICeRo) project, an external lecturer at the Faculty of Informatics of the Czech Technical University and at the Faculty of Law of the Charles University in Prague, a public speaker, and a member of the European Commission's Expert group on New Technologies and Liability. Her research specializes on privacy and data protection, legal aspects of artificial intelligence, robotics, brain-computer interfaces, and merging technology with organic life.

© A. Ležatka/ Ústavní soud

Vojen Güttler is a legal scholar at the Institute of State and Law of the Czech Academy of Sciences. In the past has worked as a civil law judge, director of Rehabilitation Department at the Ministry of Justice of the Czech Republic and a judge at the Czech Constitutional Court. Vojen is an author of a number of publications. He has wide expertise in fundamental rights protection. He has presented his scientific work at a number of international conferences in Europe, Unites States of America and in Asia.

Eva Fialová is a researcher at the Institute for the State and Law of the Czech Academy of Sciences. In her research she focuses on the artificial intelligence, algorithms and autonomous systems. Besides that, she has experience in the information technology law, especially in privacy and data protection. Eva is a member of various expert groups specialized in legal aspects of artificial intelligence and new technologies. She obtained her Ph.D. in privacy and data protection at the Masaryk University. Eva studied also at the University of Amsterdam where she obtained a LL.M. in information law.

Hananel Hazan holds a Ph.D. in Computer Science from University of Haifa (2014). In 2014–2017, Hananel worked as a postdoctoral researcher at the Network Biology Research Laboratories at Technion – Israel Institute of Technology where he developed a new experimental low cost platform for closed-loop interactions with a cortical neuronal network and machine learning that analysed the activity in real time. In 2017–2019, Hananel worked as a postdoctoral research associate at the College of Information and Computer Sciences at University of Massachusetts Amherst. He is currently working as a research scientist at the Levin Lab at Tufts University.

List of Abbreviations

AI	Artificial Intelligence
BMS	Biometric Matching Service
CC	Czech Civil Code – Act No. 89/2012 Coll., the Civil Code, as amended
CIR	Common Identity Repository
Convention 108	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
Convention 108+	Convention 108+. Convention for the protection of individuals with regard to the processing of personal data
CPC	Czech Criminal Procedure Code
CRA	Czech Criminal Register Act
CVVM	Public Opinion Research Centre of the Institute of Sociology of the Academy of Sciences of the Czech Republic (Centrum pro výzkum veřejného mínění)
DPD	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 (Data Protection Directive)
DPDCJA	Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Data Protection Directive for Police and Criminal Justice Authorities)
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ECHR	European Court for Human Rights
ECHRF	European Convention for the Protection of Human Rights and Fundamental Freedoms
EDPB	European Data Protection Board
EEA	European Economic Area

EES	Entry/Exit System
ECRIS-TCN	European Criminal Records Information System for third-country nationals
eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
ESP	European Search Portal
ETIAS	European Travel Information and Authorisation System
ETTSA	Act No. 297/2016 Coll., on trust services for electronic transactions, as amended
EU	European Union
EU Charter	Charter of Fundamental Rights of the European Union
FB	Facebook
FBI	U.S. Federal Bureau of Investigation
fMRI	Functional Magnetic Resonance
GDPR	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)
MID	Multiple-Identity Detector
MIT	Massachusetts Institute of Technology
MPA	Czech Military Police Act
OECD	Organisation for Economic Co-operation and Development
PCRA	Act on the Police of the Czech Republic
PDPA	Act No. 110/2019 Coll., on Personal Data Processing (Personal Data Protection Act).
PET	Privacy Enhancing Technologies
PIA	Privacy Impact Assessment
PLD	Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (Product Liability Directive).

PNR	Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.
QEEG	Qualified Electroencephalography
RFID	Radio-Frequency Identification
SIS	Schengen Information System
SST	Steady-State Topography
TFEU	Consolidated version of the Treaty on European Union and the Treaty on the Functioning of the European Union
UN	United Nations
VIS	Visa Information System
WP29	Article 29 Data Protection Working Party set up in accordance with Art. 29 of the Data Protection Directive

Introduction

"*Never trust to general impressions, my boy, but concentrate yourself upon details.*"

Sherlock Holmes

Human beings are a rich source of information. Just by looking at someone we are able to quickly assess who this person probably is and to distinguish her from others. We can more or less precisely determine the age, gender and ethnic origin based on the physical appearances of the body. We can also guess about a social status of a person or her preferences based on an overall look including not only the body but also the style of clothing. When talking to a person we may be able to guess what mood the person is in or maybe even how educated she is.

The science of deriving information about other humans fascinates many of us. People are especially thrilled when someone, such as the legendary but also imaginary Sherlock Holmes, can deduce detailed conclusions about someone's character, preferences, health or daily activities. An ability to do so requires mind trained to pay attention to detail. It is not a quality that can be easily acquired. Hardly ever are we required to rigorously inspect another person and notice small nuances related to her physical appearance or behaviour.

However, what is in this regard not easy for a human, presents no problem for a machine. Currently, with help of various sensors machines are able to monitor different aspects of both our physical constitution as well as behaviour. This type of technology is called biometrics and the aforementioned aspects of an individual are typically referred to as biometric features.

From a historical point of view, people have been always recognized based on their biometric features, however, this recognition was not done automatically. People distinguish other people according to their appearance, behaviour, typical gestures, manner of speech, etc. For instance, handprints were reportedly used to verify authorship of laws passed in the form of clay tables as early as in the times of King Chamurappi.[1] Automated methods of biometric verification did not appear until the early 1970s.[2] Currently, biometric authentication is used on a daily basis – for instance fingerprint or facial recognition are used in majority of smartphones.

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.[3] 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 billion USD in 2025.[4] Currently,

---

1 KINDT, E. J. *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis*. Dordrecht: Springer, 2013, p. 15.

2 Ibid., p. 18.

3 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>.

4 Ibid.

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.[5] According to market research performed by Counterpoint, over a billion smartphones with fingerprint sensors were presumed to be shipped worldwide in 2018.[6]

Given these numbers, it is obvious that biometric technology has an impact on many people and this impact shall only increase. Therefore, the aim of this monograph is to describe the fascinating technology of biometrics both from technological and legal perspectives and provide an overall picture of how does this technology function, what it is capable to do, what impacts its use can have on rights and freedoms of humans and how are humans protected by legal means with regard to biometrics. Legal analysis focuses on law of the European Union and law of the Czech Republic. In individual cases examples from other countries will be provided for illustrative purposes. Moreover, this monograph contains a comparative study of laws of several EU Member States.

The first chapter titled "Biometric Technology" describes the nature and functioning of the technology. It provides various definitions in order to illustrate what all can be considered biometrics. These definitions are then contrasted with the notion of biometrics in law. The chapter also identifies various risks related to biometrics.

The second chapter titled "Biometrics from the Perspective of International and EU Law" describes the legal framework on the level of international agreements and the law of European Union. The main focus is put on General Data Protection Regulation as well as on individual national derogations in the area of regulating biometric data. The chapter describes also other laws related to biometrics and provides a perspective on future regulation of artificial intelligence that is utilized in biometric systems.

The third chapter titled "Czech Legislation on Biometrics" assesses constitutional aspects of biometric regulation, current personal data protection legislation as well as specific public laws that regulate use of biometric technologies mainly for identification or verification of identity of an individual. Moreover, this chapter describes specificities of certain uses of biometrics.

The fourth chapter titled "Data Subjects and Their Options with Regard to Protecting Own Biometric Data" describes the scope of individual freedom and autonomy of humans with regard to use of biometric technologies. The chapter provides an overview of both legal and technical instruments that individuals may use for protection of their biometric data.

The fifth chapter titled "Recommendations for Data Controllers" provides guidelines to controllers on how to lawfully process biometric data and how to provide various safeguards to data subjects with regard to various levels of privacy protection.

---

[5] 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/>.

[6] 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/>.

Finally, the monograph contains also an Annex I. titled “Research Report on Augmented Indicative Values of Biometric Data”. This report provides an overview of what information can be derived from various types of biometric data, namely from fingerprint, face, iris, voice, and keystroke dynamics.

1. Biometric Technology

1.1 Purpose and Characteristics of Biometrics

Biometric technology serves as an efficient and reliable means of verifying or determining an identity of a natural person. Biometrics can be defined as "methods of recognizing a person based on a physiological or behavioral characteristics".[7] These characteristics are usually referred to as biometric data. Biometric systems as such "target only 'measurable physical properties'"[8] of living organisms. These organisms are characterized by "highly specific qualities which are unique and stable enough to be used as identifiers".[9] Current biometric systems capture these identifiers using various kinds of sensors, measure the electrical signal produced by these sensors, and usually convert the measurements into a computer code, which they then use as an electronic representation of a person. This process translates information from an analogue form to a digital form[10] and, thus, allows processing of such information by electronic information systems.

The initial phase of operation of a biometric system is called an enrolment. In this phase, the "system is trained to identify a specific person".[11] During this phase, at first the person provides a proof of her identity that is often issued by a trusted party. An identity card is the most common example. Next, specific features of the person are measured with an acquisition device and a so called biometric sample is collected. More samples can be collected from an individual. For instance, a fingerprint can be scanned from more positions, or fingerprints can be collected from more fingers. The collected biometric sample is then further processed and stored as a biometric template. The way "how biometric systems extract features and encode and store information in the template is based on the system vendors proprietary algorithms".[12]

The most commonly used biometric technologies that are each based on different distinctive features of a person are facial recognition, fingerprint recognition, hand geometry, iris recognition, retina recognition, signature dynamics, keystroke dynamics, voice recognition, and RFID chips with a unique number implanted in a person.[13]

From the above mentioned list of technologies, it is obvious that biometrics analyses various kinds of biometric features. With regard to the degree of uniqueness (or distinctiveness) and permanence, these features are divided into three categories: strong biometrics, weak biometrics, and soft biometrics.[14] *Strong biometrics* analyses features that are unique and stable, such as fingerprint, iris, or retina. *Weak biometrics*, on the other hand, utilizes less stable and less unique features that may be subject to change, such as gestures or gait, voice, or electrophysiological activities,

---

7 VACCA, J. R. *Biometric Technologies and Verification Systems*. Oxford: Elsevier, 2007, p. 3.
8 MORDINI, E. – TZOVARAS, D. (eds). *Second Generation Biometrics: The Ethical, Legal and Social Context*. Dordrecht: Springer, 2012. See p. 7.
9 Ibid., p. 8.
10 Ibid., p. 7.
11 VACCA, J. R. *Biometric Technologies and Verification Systems*, p. 23.
12 Ibid., p. 24.
13 Ibid., pp. 27–28.
14 MORDINI, E. – TZOVARAS, D. (eds). *Second Generation Biometrics: The Ethical, Legal and Social Context*, p. 8 et seq.

including brain waves. *Soft biometrics* uses generic features such as gender, age, ethnicity, and other information and these features can in particular serve as additional indicators for systems using strong or weak biometrics.[15]

Moreover, science distinguishes first generation and next (second) generation biometrics.[16] The first generation biometrics relies mostly on body morphology and capturing relevant data in a single moment (e.g. a photo of a face) and asks a question "who are you", while the next generation biometrics relies on measuring certain physiological functions over a period of time (e.g. voice recognition) and asks a question "how are you".[17] The next generation is sometimes referred to as "behavior-based authentication mechanisms" and is further classified as:

> "(1) Behavioral Biometrics (Authorship based, Human Computer Interaction Based, Motor Skill, and Purely Behavioral), (2) Behavioral Passwords (syntactic, semantic, one-time methods and visual memory based), (3) Biosignals (Cognitive and semi-controllable biometrics); and (4) Virtual Biometrics (representations of users in virtual worlds)."[18]

Behavioural biometrics focuses exclusively on quantifying behavioural characteristics of individuals and creating their profiles for subsequent identification. Unlike most other forms of biometrics,[19] this type of biometrics can be used in a very inconspicuous manner as data collection can be done without the user's knowledge.[20] Behavioural biometrics can identify a person, for example, by analysing text and identifying authorship, by identifying special features displayed by a person when using a computer, or even by analysing capabilities a person has in performing certain, especially cognitive, tasks.[21]

After the enrolment phase a biometric system is consequently used either to verify an identity of a person (verification) or to identify a person (identification). These two processes differ in the manner how they function.

The aim of the verification process is to determine whether a person is who she claims to be. In the verification process a person at first provides an identifier. Then she lets herself to be scanned by a respective device. Based on the provided identifier, the biometric system selects the corresponding template that was initially stored during the enrolment phase and compares the template with the newly captured data (a trial template). In order for the verification process to be successful, both the initial template and a trial template must correspond. During the verification process, the system compares a trial template only with one other template that was associated with the original identifier (one to one matching).

The aim to the identification process is to determine identity of a person who has enrolled into a biometric system but who does not present any identifier during the consequent use of the system. When a person provider her trial template, the system compares this template with other stored biometric templates and determines whether the trial template corresponds to any of them (one to many matching). By doing so the system determines the identity of a person without a need to

---

15 Ibid.

16 MORDINI, E. – TZOVARAS, D. (eds). *Second Generation Biometrics: The Ethical, Legal and Social Context*, p. 9.

17 Ibid.

18 Ibid., p. 10. This term was proposed by Yampolskiy.

19 An exception is for instance the technology of facial recognition with help of common cameras operated in public spaces.

20 By this we mean that a user does not need to use a specific technology to perform a certain action, such as placing a finger onto a sensor for unlocking a smartphone. For details see YAMPOLSKIY, R. V. – GOVINDARAJU, V. Taxonomy of Behavioural Biometrics. In: WANG, L. – GENG, X. (eds). *Behavioral Biometrics for Human Identification: Intelligent Applications*. IGI Global, 2009, [2019-12-08]. Available at: <https://www.igi-global.com/book/behavioral-biometrics-human-identification/99#table-of-contents>.

21 Ibid.

rely on any other identifier beyond the enrolment phase. Identification systems can serve both for positive and negative identification. Positive identification means that the system matches a trial template with an existing template. This match is utilized mainly for access control to premises and information systems. On the other hand, negative identification means that a trial template cannot be associated with any existing template. This is useful mainly for the purposes of avoiding misuse of public benefits programs or in "a surveillance system that uses a watch list"[22] and compares people in a monitored area with templates of people who are on this watch list in order to alert authorities when this person gets identified.

Unfortunately, biometric systems are not fool proof. The main failures are false positive and false negative matches. A false positive match (false acceptance) refers to a situation when a system wrongly associates a trial template with an existing biometric templates, i.e. the system says that an individual is someone who she is not. A false negative match (false rejection) refers to a situation when a system wrongly concludes that a trial template does not correspond to an existing biometric template, i.e. the system says that a person is not the person who she truly is. Number of these errors occurring during operation of biometric systems is used to calculate False Positive Identification Rates and False Negative Identification Rates. These rates measure performance of algorithms used in biometric systems.

In addition to the definition of biometrics that highlights its function to recognize people from one another, biometrics may be also defined as "the application of mathematical and statistical methods to describe and analyze data concerning the variation of biological characteristics obtained from either observation or experiment".[23] In this sense, biometrics is used to obtain information on the functioning of a biological organism and, where appropriate, to diagnose or predict future health developments. This concept is related to bioinformatics, a scientific field that studies health and diseases of biological systems. For the diagnostic and predictive purposes bioinformatics uses so-called biomarkers. "Biomarker is 'a characteristic that is objectively measured and evaluated as an indicator of normal biological processes, pathogenic processes, or pharmacologic responses to a therapeutic intervention' (Biomarkers Definitions Working Group, 2001)."[24] Data obtained from individual human recognition applications can also be analysed for biomarkers. For example, voice analysis may indicate at some people a possible neurodegeneration and early signs of Parkinson's disease.[25] Certain biomarkers, on the other hand, are also used for monitoring for the purpose of person's authentication.[26]

There is a great variation in existing biometric systems and their functioning as these systems are based on various sensors and use different algorithms. Nevertheless, biometric systems are subject to technical standardization. For instance, a standardization subcommittee ISO/IEC JTC 1/SC 37 Biometrics at the International Organization for Standardization (ISO) has so far issued 125 standards for biometrics and 35 other standards are currently being developed.[27] These standards relate, for

---

[22] VACCA, J. R. *Biometric Technologies and Verification Systems*, p. 26.

[23] LI, C. C. Biometrics. *AccessScience*. 2014 [2017-10-16]. Available at: <https://doi.org/10.1036/1097-8542.083700>.

[24] AZUAJE, F. *Bioinformatics and Biomarker Discovery. "Omic" Data Analysis for Personalized Medicine*. Chichester: John Wiley & Sons, Ltd., 2010, p. 2.

[25] HLAVNIČKA, J. – ČMEJLA, R. – TYKALOVÁ, T. – ŠONKA, K. – RŮŽIČKA, E. – RUSZ, J. Automated analysis of connected speech reveals early biomarkers of Parkinson's disease in patients with rapid eye movement sleep behaviour disorder. *Scientific Reports*. 2017, Vol. 7, No. 12 [2019-12-08]. Available at: <https://www.nature.com/articles/s41598-017-00047-5>. doi:10.1038/s41598-017-00047-5. ISSN 2045-2322.

[26] JENKINS, J. – SWEET, C. – SWEET, J. – MOEL, S. – SZU, H. Authentication, privacy, security can exploit brainwave by biomarker. In: *SPIE.digital library* [online]. 19. 6. 2014 [2019-12-08]. Available at: <https://www.spiedigitallibrary.org/conference-proceedings-of-spie/9118/1/Authentication-privacy-security-can-exploit-brainwave-by-biomarker/10.1117/12.2051323.short?SSO=1>.

[27] An overview of the current status of ISO standards on biometrics can be found here: https://www.iso.org/committee/313770/x/catalogue/. However, this catalogue does not include standards for protection techniques, security testing or evaluations of biometric data. This work is done within the subcommittee ISO/IEC JTC 1/SC 27 at the ISO.

example, to programming interfaces, security assurance, a framework for the exchange of biometric formats, testing methodologies, or individual types of biometric applications. Definitions related to biometrics are included in the freely available standard ISO/IEC 2382-37: 2017,[28] which replaced the 2012 standard.

The crucial concept in biometric systems is the concept of biometric data. This concept not only defines functioning of biometric systems but has also serious legal implications. According to the ISO/IEC 2382-37: 2017 standard, biometric data is "a biometric sample or aggregation of biometric samples at any stage of processing".[29] The biometric sample is then an "analog or digital representation of biometric characteristics prior to biometric feature extraction"[30] and a biometric characteristic is defined as "biological or behavioural characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition".[31] Biometric feature is then understood as "numbers or labels extracted from biometric samples and used for comparison".[32] Unfortunately, this can be considered as a so called circular definition. Nevertheless, this standard itself states that biometric data does not need to be directly attributable to an individual. This definition of biometric data, however, does not correspond to the concept of biometric data as understood by law.

1.2 Biometrics and Law in General

Use of biometric systems is presumed by law for certain identification purposes, such as biometric passports or other documents. The law works mostly with the term biometric data as a subgroup of personal data. In general, biometric data refers to individual aspects of a structure, functioning or behaviour of a biological organism. Although the term biometric data is used mainly to refer to a human, Czech law also uses this term in relation to animals[33] and European law also in relation to rice.[34] However, these are rare cases. In all other cases, the law associates biometric data with natural persons. Biometric data represents a special category of personal data. Processing of this type of data is regulated both by general rules for the processing of personal data as well as by specific and stricter rules that may differ in different contexts.

Although any measurable category of structure or functioning of a biological organism can generally be considered biometric data, in law the biometric data is generally associated with a unique identification of a natural person. Typical biometric data are facial images or dactyloscopic data. At the same time, law presupposes that these data must be processed in a certain way to become biometric data. As a rule, a simple facial image cannot be considered as biometric data[35] because

[28] International standard ISO/IEC 2382-37:2017 Information technology – Vocabulary – Part 37: Biometrics. Second edition 2017-02. In: *International Organization for Standardization* [online]. 2017 [2017-10-16]. Available at: <https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>.

[29] Ibid., point 3.3.6.

[30] Ibid., point 3.3.21.

[31] Ibid., point 3.1.2.

[32] Ibid., point 3.3.11.

[33] Biometric data are mentioned in the Czech law in connection with the capture of wild animals and their release into the wild for the purpose of monitoring the status of wild animals. See § 14 par. 6 of Act No. 246/1992 Coll., On the protection of animals against cruelty, as amended.

[34] With regard to a protected geographical indication of a particular type of rice, the following biometric characteristics of the rice grains shall be specified: length, width, thickness and shape. For details see Commission Regulation (EC) No 205/2009 of 16 March 2009 approving minor amendments to the specification for a name entered in the register of protected designations of origin and protected geographical indications (Riso Nano Vialone Veronese (PGI)).

[35] Nonetheless, the scientific literature states that even a photograph depicting a face may, under certain conditions, be considered as a biometric data. A photograph of a face taken in accordance with § 3 of the Decree No. 415/2006 Coll., Laying down the technical conditions and procedure for acquisition and further processing of biometric data contained in a data carrier of a travel document shall be considered biometric data. For details see MATOUŠOVÁ, M. – HEJLÍK, L. *Osobní údaje a jejich ochrana*. 2nd edition. Praha: ASPI, Wolters Kluwer, 2008. See p. 94.

without processing it lacks accurate information regarding, for instance, the distance of individual key points in a face or their relative ratios. This derived information, as a result, creates a system for comparing individual features and measured categories between the original template (e.g. face photo in the passport) and the subsequent measurement (a camera image of the face at passport control), allowing identity verification or identification.[36] Identifying and verifying identity is one of the main purposes for which the law uses biometric data.

The concept of biometric data but is used in different contexts throughout the legal system. Processing of biometric data is regulated mainly 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 the EU Data Protection Directive[37] in its opinions.[38] 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.[39]

Originally, the term biometric data appeared in the Working Document on Biometrics.[40] In this document, this term refers to biometric samples that can be processed both in the original (raw) form and in the form of a template based on the biometric sample. The working document underlines that if raw data contains sensitive data at the time of enrolment (the so-called enrolment phase), the enrolment must also meet the requirements for processing sensitive personal data.

A more sophisticated definition of biometric data is contained in the 2007 WP29 document on the concept of personal data. The document defines biometric data as "biological properties, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability".[41] 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[42] and, therefore, can serve as an identifier.[43] 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.

In 2012, WP29 issued a special document on developments in biometric technologies,[44] in which it reiterated the previous definition and at the same time highlighted an important characteristics of the

---

[36] Identity verification means a situation in which a system compares whether the measured biometric data of a person correspond to the biometric template that it submitted as a proof of the person's identity. Upon identification, the system measures the person's biometric data and compares it with its database to find a match. For more details, see e.g. MORDINI, E. – TZOVARAS, D. (eds). *Second Generation Biometrics: The Ethical, Legal and Social Context*, p. 8.

[37] 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.

[38] See ARTICLE 29 DATA PROTECTION WORKING PARTY. Working document on biometrics. In: *European Commission* [online]. 1. 8. 2003 [2019-12-08]. Available at: <https://ec.europa.eu/justice/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 [2019-12-08]. Available at: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf>.

[39] For details see ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 3/2012 on developments in biometric technologies*.

[40] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Working document on biometrics*.

[41] ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 4/2007 on the concept of personal data. In: *European Commission* [online]. 20. 6. 2007 [2019-12-08]. Available at: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>. See p. 8.

[42] 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.

[43] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 4/2007 on the concept of personal data*.

[44] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 3/2012 on developments in biometric technologies*.

technology: “Biometric data changes irrevocably the relation between body and identity, because they make the characteristics of the human body ‘machine-readable’ and subject to further use”.[45]

The first legally binding definition of the term biometric data appeared in the EU’s General Data Protection Regulation (hereinafter GDPR).[46] According to Art. 4, par. 14 the term refers to “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”.

In the Czech law the term biometric data is used in a number of public laws. The Czech law itself does not provide any definition of biometric data. Both former and current data protection acts mention the term biometric data with regard to the definition of so called “sensitive data”. The former Data Protection Act defines sensitive data as “personal data revealing national, racial or ethnic origin, political opinions, trade-union membership, religious or philosophical beliefs, conviction for a criminal offence, information about the health and sexual life of a data subject and genetic data of a data subject; sensitive data is also a biometric data that allows direct identification or authentication of a data subject”.[47] The current Personal Data Processing Act that was adopted as a reaction to the GDPR mentions that wherever the existing legislation uses the term sensitive data, as of the entry into force of the new Personal Data Processing Act, it refers to “personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, genetic data, biometric data processed for the purpose of unique identification of a person, health data, data on sexual behaviour, sexual orientation, and data related to criminal judgments and offences or related security measures”.[48]

1.3 Risks Associated with Using Biometrics

Biometric data have been classified as a special category of personal data in law because of processing of this kind of data significantly increases vulnerability of data subjects whom the biometric data refers to. Vulnerability can be understood as “a state of being exposed to the possibility of being attacked or harmed, either physically or emotionally.”[49] The vulnerability increases when the possibility of being harmed is more likely. This might happen due to a number of reasons that are to be identified in this subchapter.

In general, risks of data subjects related to use of biometrics can stem from the design and purpose of operation of a biometric system or from an attack on a biometric system that can have carious impact and consequences for a data subject. Moreover, certain risks for data subjects may stem also from data protection legislation and regulation itself in cases in which it allows for certain processing of biometric data.

[45] Ibid., p. 4.
[46] 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).
[47] See § 4 par. b) of the Act No. 101/2000 Coll., on Personal Data Protection and on Amendments of Some Acts.
[48] See § 66 par. 6 of the Act No. 110/2019 Coll., on Personal Data Processing (PDPA).
[49] Vulnerability. In: *Google Dictionary* [online]. [2017-12-10]. Available at: <https://www.google.cz/search?q=Dictionary#dobs=vulnerability>.

1.3.1 Risks Related to Design of Biometric Systems

There is a number of risks that are connected to the manner how biometric systems are set up and operated. The most profound and underlying risk that increases vulnerability of data subjects is an inherent set-up by which a person operating a biometric system (in terms of the GDPR a controller)[50] gains information about data subjects and exercises certain power over them while data subjects can have only limited influence on the system and usually do not have much information about functioning of the system. Economics and contract law use a term "information asymmetry" to describe situations in which "one party has more or better information than the other".[51] In this regard, defence uses a similar concept and refers to it with a term "information superiority"[52] or recently "information advantage". Working definition of information advantage is "the credible advantage gained through the continuous, adaptive, decisive and resilient employment of information and information systems".[53]

This information asymmetry or information advantage and ability to exercise control over data subjects on the side of a controller are manifested through various characteristics and types of usage of biometric systems. These are namely opacity of biometric systems, their use for biometric surveillance, increasing knowledge about data subjects with help of cross-matching of data from various databases or by extracting additional information from biometric data and, thus, augmenting indicative value of biometric data, evaluating and making (often automated) decisions about data subjects, and setting up a level of security of biometric systems.

1.3.1.1 Opacity of Biometric Systems

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.[54] Faces can be recognized with use of cameras or with infrared sensors, voice with use of microphones, fingerprints with optical, silicon or ultrasound sensors.[55] 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 specifics of biological functioning of an individual, symptoms of her diseases, information about her current state or her identity. Such information can be derived with the 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,

---

50 See Art. 4 (7) of the GDPR.

51 Information asymmetry. In: *Wikipedia* [online]. 10. 10. 2019 [2019-12-10]. Available at: <https://en.wikipedia.org/wiki/Information_asymmetry>.

52 MINISTRY OF DEFENCE. Joint Doctrine Note 2/13. Information Superiority. In: *GOV.UK* [online]. 2013 [2019-12-10]. Available at: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819814/archive_doctrine_uk_info_superiority_jdn_2_13.pdf>.

53 MINISTRY OF DEFENCE. Joint Concept Note 2/18. Information Advantage. In: *GOV.UK* [online]. 2018 [2019-12-10]. Available at: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/764075/20181126-JCN_2_18_Information_Advantage_web.pdf>.

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

55 VACCA, J. R. *Biometric Technologies and Verification Systems*. Oxford: Elsevier, 2007.

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.

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 analyse an application running for instance on her smartphone that utilizes information from fingerprint sensor. However, she may not even know that some application is using either the fingerprint sensor or a camera. This information is hard to detect. In some cases a special monitoring software could help. However, if the data is handled directly by a firmware (software embedded directly into the hardware that cannot be deleted), it is almost impossible to detect a leak of data. 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, such attempts to analyze data leaks can be made very difficult by using good compression algorithms or clever communication protocols.

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. An example of such misuse is so called function creep, i.e. using a system for additional purpose than initially planned. In order to prevent the above mentioned risks, law constructs rules aiming at balancing opacity by providing objective guarantees to natural persons.

1.3.1.2 Biometric Surveillance

Biometric surveillance is defined as “the application of biometric methods for identifying people and determining whether or not they are a security risk”.[56] These methods use among others also methods of soft biometrics. These “go beyond human physical appearance to include human behaviors and particulars about physical appearance, e.g., height, weight, and even clothing styles as long as they satisfy requirements like distinctiveness or uniqueness, permanence or invariance, and collectability”.[57] The aim of monitoring systems using biometrics is especially to aid humans who are not able to process information as quickly as information systems.

The most profound application of biometric surveillance is in the area of evaluation of visual information, i.e. videos from security cameras, from individuals that share videos on social networks, etc. This also applies to individual images. Current systems are able to assist “to distinguish a person of interest from other people”.[58] Biometric surveillance can, however, be applied also in other areas, such as gait recognition.[59] In the U.S., biometric surveillance is used within the program “E-Verify” that “identifies those eligible to work legally in the United States”.[60] Surveillance using biometrics can also focus not only on distinguishing a person but also on prediction of her behaviour and

[56] TOOR, A. S. – WECHSLER, H. – NAPPI, M. Biometric surveillance using visual question answering. *Pattern Recognition Letters*. 2019, Vol. 126, pp. 111–118 [2019-12-08]. Available at: <https://doi.org/10.1016/j.patrec.2018.02.013>.

[57] Ibid.

[58] Ibid.

[59] MOHAPATRA, S. et al. Real time biometric surveillance with gait recognition. *AIP Concerence Proceedings*. 2018, Vol. 1952, No. 1 [2019-12-08]. Available at: <https://aip-scitation-org.ezproxy.techlib.cz/doi/abs/10.1063/1.5031969>.

[60] GOLDSTEIN, D. M. – ALONSO-BEJARANO, C. E-Terrify: Securitized Immigration and Biometric Surveillance in the Workplace. *Human Organization*. 2017, Vol. 76, No. 1, pp. 1–14 [2019-12-08]. Available at: <https://search-proquest-com.ezproxy.techlib.cz/docview/1879074866>.

intentions.[61] In Europe, methods of behaviour detection and prediction were developed for instance in the EU's project "Automatic Detection of Abnormal Behaviour and Threats in crowded Spaces".[62]

On one hand, biometric surveillance can significantly help in prevention of threats and in enforcement of law, on the other hand its use can have a significant impact on "individual privacy, autonomy, bodily integrity, dignity, equity, and personal liberty".[63] Moreover, its deployment may also lead to "unjustified discrimination and stigmatization on the one hand; loss of public trust on the other".[64]

In some cases, biometric surveillance can be related to profiling (see section 1.3.1.5).

1.3.1.3 Cross-Matching of Data

Cross-matching of data from multiple databases is another way of using biometrics that increases vulnerability of data subjects. Cross-matching can refer to merging data from publicly available databases, such as social networks, or to so called multimodal biometrics.

One of the richest source of biometric data in publicly available database, is a database of portrait images that have been made available on Facebook (hereinafter FB). FB has developed own technology for face recognition and utilizes input from users that tag pictures and provide name of not only themselves but also their friends and acquaintances.[65] Data from social networks are also utilized by other big companies, such as Google. This company "filed for a European patent on the use of social network data to improve face recognition".[66] Although the patent application was filed in 2011, Google made sure to take in account privacy protection: "The patent application made specific reference to privacy controls, such as making results of a search available only to someone positively identified in an image, or seeking permission from people identified before releasing the information".[67] Nevertheless, given the availability of data, private companies can "build massive databases of names matched to faces".[68]

Databases of biometric data are, however, built also by governments. In the U.S., the FBI developed a system called "Next Generation Identification" that combines biometric information with information on criminal history.[69] The system also uses multimodal biometrics. In the EU, on 16 April 2019, the European Parliament approved a proposal for establishing "interoperability between EU information systems in the field of borders and visa".[70] With regard to this proposal three EU regulations were

---

[61] SUTROP, M. – LAAS-MIKKO, K. From Identity Verification to Behavior Prediction: Ethical Implications of Second Generation Biometrics. *Review of Policy Research*. 2012, Vol. 29, No. 1, pp. 21–36 [2019-12-08]. Available at: <https://onlinelibrary-wiley-com.ezproxy.techlib.cz/doi/abs/10.1111/j.1541-1338.2011.00536.x>.

[62] Automatic Detection of Abnormal Behaviour and Threats in crowded Spaces. In: *CORDIS* [online]. [2019-12-08]. Available at: <https://cordis.europa.eu/project/id/218197>.

[63] SUTROP, M. – LAAS-MIKKO, K. *From Identity Verification to Behavior Prediction: Ethical Implications of Second Generation Biometrics*.

[64] Ibid.

[65] MANSFIELD-DEVINE, S. Social identity: is biometric technology on social networks a benefit or a threat? *Biometric Technology Today*. 2012, Vol. 2012, No. 10, pp. 5–9 [2019-12-08]. Available at: <https://doi.org/10.1016/S0969-4765(12)70203-5>.

[66] Ibid.

[67] Ibid.

[68] Ibid.

[69] Next Generation Identification (NGI). In: *FBI* [online]. [2019-12-08]. Available at: <https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi>.

[70] European Parliament legislative resolution of 16 April 2019 on the amended proposal for a regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399, Regulation (EU) 2017/2226, Regulation (EU) 2018/XX [the ETIAS Regulation], Regulation (EU) 2018/XX [the Regulation on SIS in the field of border checks] and Regulation (EU) 2018/XX [the eu-LISA Regulation] (COM(2018)0478 – C8-0294/2018 – 2017/0351(COD)).

adopted.[71] Among others, these regulations "ensure interoperability between the Entry/Exit System (EES), the Visa Information System (VIS), the European Travel Information and Authorisation System (ETIAS), Eurodac, the Schengen Information System (SIS), and the European Criminal Records Information System for third-country nationals (ECRIS-TCN)".[72] Interoperability shall be secured through four specific components: a European search portal (ESP), a shared biometric matching service (shared BMS), a common identity repository (CIR), and a multiple-identity detector (MID).[73]

Merging data from various databases can have a form of so called multimodal biometrics. "A multimodal biometrics system utilizes more than one biometric trait for recognition and verification purposes".[74] Some systems use soft biometrics to improve performance of biometric verification or identification. However, in case of leakage of information from soft biometric database, privacy risks for data subjects increase.[75]

1.3.1.4 Augmented Indicative Value of Biometric Data

Biometric data can contain information of a 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.

As already stated, biometrics is a term referring to the "use of distinctive biological or behavioral characteristics to identify people"[76] with the 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.

---

[71] Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726; Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA; and Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816

[72] Art. 1 (1) of the Regulation (EU) 2019/818.

[73] Art. 1 (2) of the Regulation (EU) 2019/818.

[74] SADHYA, D. – SINGH, S. K. Privacy risks ensuing from cross-matching among databases: A case study for soft biometrics. *Information Processing Letters*. 2017, Vol. 128, pp. 38–45 [2019-12-08]. Available at: <https://doi.org/10.1016/j.ipl.2017.08.001>.

[75] Ibid.

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

When gathered by automated means and preserved in a digital form, biological or behavioural characteristics can be analysed with the 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 soft biometrics or biomarkers. Soft biometrics can be in this regard defined as follows: "Soft biometric traits are physical, behavioral, or material accessories, which are associated with an individual, and which can be useful for recognizing an individual. These attributes are typically gleaned from primary biometric data, are classifiable in pre-defined human understandable categories, and can be extracted in an automated manner".[77] Typical personal attributes that can be derived as soft biometric data are "gender, age, ethnicity, hair color, height, weight, and so on".[78] Biomarker, on the other hand, 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".[79] These biomarkers can reliably determine presence or predisposition of an illness in an individual.

Research has shown that information from soft biometrics can be divided into several categories, each of which contains specific types of data: demographic attributes (age, gender, ethnicity, colour of eyes, hair and skin); anthropometric and geometric attributes (body and facial geometry); medical attributes (health condition, body weight/BMI, wrinkles); and material and behavioural attributes (accessories such as hat, scarf, bag, clothes, glasses, etc.).[80] Soft biometrics is used for instance for demographic analysis in which age, gender and race are used for analysis.[81]

Although the mentioned research has shown types and categories of data that can be derived about individuals based on their biometric data, more extensive research had to be done in order to show the real potential of biometric data and their augmented indicative value.[82] 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 the help of automated detection of emotion from voice when talking on a customer phone line).

The following summary of augmented indicative value of biometric data is based on a research report that focused on identification of what other types of information can be identified from biometric data. The report focused on five biometric technologies: fingerprint, face, iris, voice, and keystroke dynamics. The whole research report can be found in Annex I.

---

77 DANTCHEVA, A. – ELIA, P. – ROSS, A. What Else Does Your Biometric Data Reveal? A Survey on Soft Biometrics. *IEEE Transactions on Information Forensics and Security.* 2015, Vol. 11, No. 3 [2019-12-08]. Available at: <https://ieeexplore-ieee-org.ezproxy.techlib.cz/document/7273870>.

78 Ibid.

79 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>.

80 DANTCHEVA, A. – ELIA, P. – ROSS, A. *What Else Does Your Biometric Data Reveal? A Survey on Soft Biometrics*.

81 SUN, Y. – ZHANG, M. – SUN, Z. – TAN, T. Demographic Analysis from Biometric Data: Achievements, Challenges, and New Frontiers. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2017, Vol. 40, No. 2 [2019-12-08]. Available at: <https://ieeexplore-ieee-org.ezproxy.techlib.cz/document/7855777>.

82 Original research on augmented indicative values of biometric data was published in KRAUSOVÁ, A. – HAZAN, H. – MATEJKA, J. Biometric Data Vulnerabilities: Privacy Implications. *The Lawyer Quarterly*. 2018, Vol. 8, No. 3, pp. 295–306 [2019-12-10]. Available at: <https://tlq.ilaw.cas.cz/index.php/tlq/article/view/291>.

Fingerprints can be analysed for determining gender[83] or ancestral background[84] of a person. Based on their temperature, fingerprints can also indicate a state of relaxation or anxiety[85] of a person and even show intensity of acute stress.[86] Moreover, temperature of fingerprints can predict a person's performance in attentional tasks[87] or indicate sympathetic responses.[88] Specificities of ridges on fingerprints (dermatoglyphics) can also contribute to diagnosis of certain illnesses, as some can be correlated with genetic abnormalities.[89] Heart rate can be measured with the help of camera from a fingerprint, and potential abnormal functioning of heart could be detected.[90]

Face is a rich source of various kinds of information. Naturally, facial images can be analysed to indicate age,[91] gender,[92] racial, ethnic or cultural origin,[93] emotions,[94] or even facial attractiveness.[95] With help of machine-vision algorithms, various diseases can be detected from face as well.[96]

Iris images ran reveal information about abnormalities or diseases such as cataracts, acute glaucoma, posterior and anterior synechiae, retinal detachment, rubeosis iridis, corneal vascularization, corneal ulcers, haze or opacities, corneal grafting, or iris damage and atrophy.[97]

---

83 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>.

84 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>.

85 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>.

86 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/>.

87 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>.

88 KISTLERA, A. – MARIAUZOULSB, C. – VON BERLEPSCHA, K. Fingertip temperature as an indicator for sympathetic responses. *International Journal of Psychophysiology*. 1998, Vol. 29, No. 1 [2017-12-17]. Available at: <http://www.sciencedirect.com/science/article/pii/S0167876097000871>.

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

90 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>.

91 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>.

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

93 LU, X. – JAIN, A. K. Ethnicity identification from face images. In: *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>.

94 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>.

95 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>.

96 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>.

97 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. In: *2015 IEEE 2nd 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.[98] For instance, illnesses such as Parkinson's disease,[99] praedementia and Alzheimer's disease[100] 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),[101] as well as other traits such as "dominance and attractiveness, threat potential, social status, personality, sexual orientation, level of self-consciousness etc.".[102] Moreover, voice can be correlated also with hormone levels or with use of prescription medication.[103] Voice can also indicate that a speaker perceives difference in social status between herself and a listener[104] or that the speaker probably lies.[105]

Keystroke dynamics can be analysed for age,[106] gender,[107] emotional states such as happiness or stress,[108] for Parkinson's disease[109] or possibly for sleep inertia.[110]

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 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 the 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

---

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

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

100 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>.

101 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>.

102 Ibid.

103 Ibid.

104 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>.

105 HOLLIEN, H. – GEISON, L. – 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>.

106 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/>.

107 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>.

108 FAIRHURST, M. – LI, C. – ERBILEK, M. Exploiting biometric measurements for prediction of emotional state: A preliminary study for healthcare applications using keystroke analysis. In: *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/>.

109 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>.

110 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>.

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. Moreover, such information can be further used for profiling individuals and, potentially discriminating them.

1.3.1.5 Discriminative Decision-Making

Discriminative decision-making with regard to operation of biometric systems can be caused mainly by "false interpretation of biometric characteristics".[111] The most profound example of unjust discrimination is identifying someone as a potential threat (i.e. a criminal offender or a terrorist). This can be a result of technology malfunction (false positive identification of an individual from a watch list)[112] or a result of wrong set-up of evaluation criteria in a system.

Potentially discriminative decision-making is based on evaluation of certain aspects of an individual. Law refers to this evaluation of a person as to "profiling".[113] There are many applications that use this type of technology. Profiling is used for instance for security purposes in the context of employment. Behaviour of employees when interacting with a device can be analysed to identify a potential insider attack.[114] Profiling also refers to predicting of potential of a person or her future behaviour. This is done for instance in the area of algorithmic risk assessment. Unfortunately, decision-making based on biometric data and profiling may not be free of bias.

In this regard, the term "algorithmic bias" is nowadays commonly used. This term refers to "systematic and repeatable errors in a computer system that create unfair outcomes, such as privileging one arbitrary group of users over others".[115] Discrimination can be either explicit (i.e. intended) or implicit (i.e. unintended).[116] Use of profiling and, therefore, also potential occurrence of algorithmic biases have been identified in areas such as predictive policing, DNA profiling, consumer scoring, and consumer marketing.[117] Scientists have repeatedly pointed out that especially in the area of predictive policing people are discriminated base on their racial profile.[118] Moreover, scoring of people may not be reliable. For instance, forecasting of violent crimes by the company Northpointe in 2013–2014 proved to be successful only in 20 % of cases.[119]

---

[111] SUTROP, M. – LAAS-MIKKO, K. *From Identity Verification to Behavior Prediction: Ethical Implications of Second Generation Biometrics*.

[112] JOHNSON, M. L. Biometrics and the threat to civil liberties. *Computer*. 2004, Vol. 37, No. 4, pp. 90–92 [2019-12-08]. Available at: <https://ieeexplore-ieee-org.ezproxy.techlib.cz/document/1297317>.

[113] Art. 4 (4) of the GDPR.

[114] SOH, Ch. et al. Employee profiling via aspect-based sentiment and network for insider threats detection. *Expert Systems with Applications*. 2019, Vol. 135, pp. 351–361 [2019-12-08]. Available at: <https://doi.org/10.1016/j.eswa.2019.05.043>.

[115] Algorithmic bias. In: *Wikipedia* [online]. 12. 12. 2019 [2019-12-15]. Available at: <https://en.wikipedia.org/wiki/Algorithmic_bias>.

[116] ZARSKY, T. Understanding Discrimination in the Scored Society. *Washington Law Review*. 2014, Vol. 89, No. 4, pp. 1375–1412 [2019-12-15]. Available at: <https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=4822&context=wlr>.

[117] JACKSON, J. R. Algorithmic Bias. *Journal of Leadership, Accountability and Ethics*. 2018, Vol. 15, No. 4, pp. 55–65 [2019-12-15]. Available at: <https://search-proquest-com.ezproxy.techlib.cz/docview/2170233068?pq-origsite=summon>.

[118] MAYSON, S. G. Bias In, Bias Out. *Yale Law Journal*. 2019, Vol. 128, No. 8, pp. 2218–2300 [2019-12-15]. Available at: <http://web.a.ebscohost.com.ezproxy.techlib.cz/ehost/detail/detail?vid=0&sid=e39e5a41-db7c-4c08-874e-31f478e4eff8%40sdc-v-sessmgr03&bdata=Jmxhbmc9Y3Mmc2l0ZT1laG9zdC1saXZl#AN=137113291&db=a9h>.

[119] KIRKPATRICK, K. Battling algorithmic bias: How do we ensure algorithms treat us fairly? *Communications of the ACM*. 2016, Vol. 59, No. 10, pp. 16–17 [2019-12-15]. Available at: <http://delivery.acm.org.ezproxy.techlib.cz/10.1145/2990000/2983270/p16-kirkpatrick.pdf?ip=195.113.241.166&id=2983270&acc=ACTIVE%20SERVICE&key=D6C3EEB3AD96C931%2E507606E42780605B%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&__acm__=1576440854_59828787bbd98db1cee32497e251627a>.

Algorithmic bias represents a great drawback of the technology and research is trying to find ways how to eliminate it from the process of automated decision making. Instruments of automated reduction of gender and racial bias have already been introduced.[120]

1.3.1.6 Insufficient Cybersecurity

Controllers operating biometric systems are also in charge of properly securing these systems from attacks. Unfortunately, recent developments show that despite all the concerns about biometric data, some databases still lack proper protection and encryption. In August 2019, a team of ethical hackers identified a leak "of up to 1 million fingerprint records plus facial images exposed on an open database".[121]

Every day people use mobile biometric applications that are vulnerable to a number of type of attacks by which stored fingerprints and facial images can be stolen.[122] Therefore, controllers must be ready for various kinds of attacks (for details see Section1.3.2). A special type of attack that is considered to be "a purely biometric vulnerability that is not shared with other IT security solutions"[123] is called spoofing. In this type of an attack "intruders use some type of synthetically produced artefact (e.g., face mask, gummy finger or printed iris image) or try to mimic the behaviour of genuine users (e.g., gait, signature), to fraudulently access the biometric system".[124] Spoofing can be done on more types of biometrics. Attackers can fake for instance fingerprints or even voice by presenting a signal that contains respective vocal characteristics. Technical research states that "the signal does not even need to be understandable by a human, as long as it exhibits the deterministic vocal features of the attacked identity".[125] The ability of controllers to set up a resistant system are significantly reduced by overall availability of certain types of data[126] as well as tutorials on how to fake biometric data.

There are of course methods how to protect biometric systems, for instance methods of biometric cryptosystems or concealable biometrics.[127] Controllers can use techniques to secure biometric templates, such as biohashing. Biohashing can be defined as a "transformation-based [method], in which the biometric template of the user is transformed into a protected binary string through multiplication with a pseudo-random projection matrix and quantization".[128] However, this method is not fool proof as there are methods how to reverse a biohash of a person in case a secret key of

[120] MIT claims breakthrough in ending biometric bias. *Biometric Technology Today*. 2019, Vol. 2019, No. 2, p. 12 [2019-12-15]. Available at: <https://doi.org/10.1016/S0969-4765(19)30028-1>.

[121] '1m fingerprint' data leak raises doubts over biometric security. *Biometric Technology Today*. 2019, Vol. 209, No. 8, pp. 1–2 [2019-12-08]. Available at: <https://doi.org/10.1016/S0969-4765(19)30104-3>.

[122] GHOUZALI, S. et al. Trace Attack against Biometric Mobile Applications. *Mobile Information Systems.* 2016 [2019-12-08]. Available at: <https://www.hindawi.com/journals/misy/2016/2065948/>.

[123] GALBALLY, J. – MARCEL, S. – FIERREZ, J. Biometric Antispoofing Methods: A Survey in Face Recognition. *IEEE Access*. 2014, Vol. 2 [2019-12-08]. Available at: <https://ieeexplore-ieee-org.ezproxy.techlib.cz/document/6990726>.

[124] Ibid.

[125] CHINGOVSKA, I. – RABELLO DOS ANJOS, A. – MARCEL, S. Biometrics Evaluation Under Spoofing Attacks. *IEEE Transactions on Information Forensics and Security.* 2014, Vol. 9, No. 12, pp. 2264–2276 [2019-12-08]. Available at: <https://ieeexplore-ieee-org.ezproxy.techlib.cz/document/6879440>.

[126] One can think of images, videos, recording of voice of a person etc. that are available online by various actors (data subjects themselves, family and friends, journalists, etc.).

[127] RATHGEB, Ch. – UHL, A. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security.* 2011, Vol. 2011, No. 3, pp. 1–25 [2019-12-08]. Available at: <https://search-proquest-com.ezproxy.techlib.cz/docview/1323854588/fulltextPDF/91CADB9B1F374FD2PQ/3?accountid=119841>.

[128] TOPCU, B. et al. Practical security and privacy attacks against biometric hashing using sparse recovery. *EURASIP Journal on Advances in Signal Processing*. 2016, Vol. 2016, pp. 1–20 [2019-12-08]. Available at: <https://search-proquest-com.ezproxy.techlib.cz/docview/1819663613?pq-origsite=summon>.

a respective data subject is compromised or known. Revering a biohash then results in obtaining a rather exact original biometric template (for instance an image of a person).[129]

Specific risks are connected with using biometric data for authentication to access a cloud, as these data are also stored in a cloud and are subject to various threats and most importantly reduced control over the data.[130]

Recently, blockchain technology was suggested as a solution for storing and securing biometric data.[131] Unfortunately, storing biometric data in blockchain also poses a special type of risk. This risk is related to quality of data that is inserted into the system as it is extremely difficult or even impossible to get bad data out of the blockchain system later. Such risk could corrupt the whole system.[132]

1.3.2 Risks Related to Attacks on Biometric Systems

Biometric systems are information and communication systems and, therefore, are prone to comparable vulnerabilities and cyber-attacks just as any other systems. Biometric systems can be attacked in various stages of their operation.

Scientific literature distinguished eight such stages: attack at the sensor/acquisition device (destruction of the device or inserting false data); attack at the passage amongst the sensor and the sample feature extractor; attack on the extractor module; attack at the passage amongst the feature extractor and a matcher; attack on the matcher; attack on the system database; attack between the system database and the matcher; and attack at the passage amongst the matcher and the application.[133]

An attack on a biometric service can result in an overall denial of service, in circumventing the system that does not then provide access to authorised users, in interference with integrity of stored biometric data and their potential compromising or loss, in modifying parameters of a biometric system or in forcing an authorised user to provide access to an unauthorized user.[134]

1.3.3 Risks Related to Legal Regulation of Biometric Systems

As it has been already mentioned, biometric data are considered a special category of data and are, thus, subject to much stricter legal regulation. As opposed to normal types of personal data, processing of biometric data is in the EU in principle prohibited.[135]

---

[129] Ibid.

[130] BHATTASALI, T. et al. A Survey of Security and Privacy Issues for Biometrics Based Remote Authentication in Cloud. In: *13th IFIP International Conference on Computer Information Systems and Industrial Management (CISIM)*. 2014 [2019-12-08]. Available at: <https://hal.inria.fr/hal-01405569/document>.

[131] BLOSFIELD, E. Data Privacy Risks as Digital Identity Moves to Biometrics, Blockchain. *Insurance Journal*. 21. 5. 2018 [2019-12-08]. Available at: <https://search-proquest-com.ezproxy.techlib.cz/docview/2041724444/fulltext/A7B188C363E7486APQ/1?accountid=119841>.

[132] Ibid.

[133] HABIBU, T. – SAM, A. E. Assessment of vulnerabilities of the biometric template protection mechanism. *International Journal of Advanced Technology and Engineering Exploration*. 2018, Vol. 5, No. 45, pp. 243–254 [2019-12-08]. Available at: <https://search-proquest-com.ezproxy.techlib.cz/docview/2126783210?pq-origsite=summon>.

[134] Ibid.

[135] Art. 9 (1) of the GDPR.

However, the strict regulation of the GDPR does not apply to certain cases. According to Art. 2 (2), the GDPR “does not apply to the processing of personal data: (a) in the course of an activity which falls outside the scope of Union law; (b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU; (c) by a natural person in the course of a purely personal or household activity; (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.”

More loose rules then can apply that will not provide sufficient protection to individuals with regard to their personal data.

2. Biometrics from the Perspective of International and EU Law

2.1 International Law

Biometric data are not regulated by any international convention that is considered as an important international legal instrument. Art. 17 of the International Covenant on Civil and Political Rights[136] adopted by the United Nations (hereinafter UN) in 1966 declares the right not to be subjected to arbitrary or unlawful interference with privacy. The First Protocol allows victims of human rights violation to be heard by the Human Rights Committee. If there was interference with the right to privacy due to biometric data processing, an individual can complain to the Committee.

The right to private life is guaranteed by Art. 8 of the European Convention on Human Rights.[137] In case of an infringement to the right to private life by biometric data processing, an individual may address the European Court of Human Rights (hereinafter "ECHR") providing that he or she has exhausted all domestic legal remedies. In general, The ECHR ranks the right to protection of personal data, that implies also biometric data, under Art. 8 of the Convention. In the case of *Cemalettin Canlı against Turkey*[138] the ECHR adjudicated that the notion of private life has to be interpreted in accordance with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[139] (hereinafter "Convention 108").

The Convention 108 was adopted by the Council of Europe in 1981. The Convention 108 lays down basic principles of personal data protection such as fairness and transparency of the processing, collection of data for explicit, specified and legitimate purposes, processing of adequate, relevant and not excessive data in relation to that purposes, accuracy of data and processing of the data not longer than necessary for the purposes. The Convention 108 did not contain the protection of biometric data that was criticized by Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data.[140]

The Council of Europe prepared a modernization of the Convention 108 (hereinafter "Convention 108+").[141] The objective of the Convention 108+ should address privacy risks linked with new

[136] International Covenant on Civil and Political Rights. In: *United Nations* [online]. [2019-12-14]. Available at: <https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf>.

[137] European Convention on Human Rights. In: *Council of Europe* [online]. [2019-12-14]. Available at: <https://www.echr.coe.int/Documents/Convention_ENG.pdf>.

[138] Judgement of the ECHR of 18 November 2008, No. 22427/04, *Cemalettin Canlı against Turkey*.

[139] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. In: *Council of Europe* [online]. [2019-12-14]. Available at: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>.

[140] DE HERT, P. – CHRISTIANEN, K. Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data. In: *Council of Europe* [online]. 2013 [2019-09-15]. Available at: <https://rm.coe.int/progress-report-on-the-application-of-the-principles-of-convention-108/1680744d81>.

[141] Convention 108+. Convention for the protection of individuals with regard to the processing of personal data. In: *Council of Europe* [online]. 2018 [2019-09-15]. Available at: <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1>.

information and communication technologies. Art. 6 of the Convention 108+ treats biometric data uniquely identifying a person as a special category of data. Those data may be processed only if appropriate safeguards are enshrined in law. The safeguards should eliminate the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, in particular a risk of discrimination. In the Convention 108+ a scope of rights of data subject is enshrined in order to provide them more legal instruments to protect their personal data against unlawful processing.

Besides the Convention 108, there exist more documents mentioning biometric data. However, these documents have a character of recommendation and therefore are not legally binding. They sketch out a direction where the legal regulation will go.

The Organisation for Economic Co-operation and Development (hereinafter "OECD"), Working Party on Information Security and Privacy issued in 2004 a document on biometric-based technologies.[142] The document provides a general introduction to biometric technologies. The document describes risk linked to biometric-based technologies (e.g. privacy, security, user's control), gives an overview of basic technologies (finger geometry, facial recognition, voice recognition, etc.) and recommends certain steps when designing a biometric-based project. The stakeholders should strive for transparency, privacy and security, supervision of individuals interacting with biometric systems, accuracy or, if possible, an opt-in enrolment systems.

The UN is also active in the field of biometric data and technologies. In 2018, the UN published United Nations Compendium Of Recommended Practices for the Responsible Use & Sharing of Biometrics in Counter-Terrorism.[143] Besides an overview of biometric technologies, identity management and regulatory requirements for biometric technologies, the compendium provides information about the counter terrorism biometric systems and databases used by law enforcement authorities, border controller and military. "States should adopt a human rights-based approach to the use of counter terrorism biometric technology that includes the use of procedural safeguards and effective oversight of its application."[144] The safeguards should include oversight bodies, effective remedies and ethical review processes. The use of biometrics should be in compliance with human rights as well as technical standards. According to the UN, the states should counter the terrorism by means of biometric systems in order to protect their border security. The compendium provides the states with recommendation about verification techniques, databases and sharing of the biometric data at the international level.[145]

The abovementioned compendium is, however, criticized by the Privacy International (an organization of privacy advocates).[146] The Privacy International points out that the compendium supports the expansion of biometric systems and international sharing of biometric data, as well as an expanding access of the law enforcement authorities and security agencies to the biometric databases.[147]

---

[142] OECD. Working Party on Information Security and Privacy. Biometric-based Technologies. In: *OECD* [online]. 2004 [2019-12-04]. Available at: <https://www.oecd-ilibrary.org/docserver/232075642747.pdf?expires=1575372645&id=id&accname=guest&checksum=FF00B8A8B118873A62B7857A864A3A71>.

[143] UN. United Nations Compendium of Recommended Practices for the Responsible Use & Sharing of Biometrics in Counter-Terrorism. In: *UN* [online]. 2018 [2019-12-04]. Available at: <https://www.unodc.org/pdf/terrorism/Compendium-Biometrics/Compendium-biometrics-final-version-LATEST_18_JUNE_2018_optimized.pdf>.

[144] Ibid., p. 51.

[145] Ibid., p. 81.

[146] PRIVACY INTERNATIONAL. Briefing to the UN Counter-Terrorism Executive Directorate on the responsible use and sharing of biometric data to tackle terrorism. In: *Privacy International* [online]. 2019 [2019-12-04]. Available at: <https://www.privacyinternational.org/sites/default/files/2019-07/PI%20briefing%20on%20biometrics%20final.pdf>.

[147] Ibid., p. 14.

2.2 EU Law

2.2.1 GDPR and Its Ancestors

2.2.1.1 Evolution from the Data Protection Directive to the GDPR

The Data Protection Directive (hereinafter "DPD") effective until 24 May 2018 did not recognised biometric data as a special category of data, or in the other word, the DPD did not contain any definition or special reference to biometric data at all. The definition of biometric data was set down by Opinion 4/2007 of the Article 29 Data Protection Working Party (hereinafter "WP29") on the concept of personal data.[148] WP 29 in its working document on biometrics stressed that biometric data should have been considered as sensitive data pursuant to Art. 8 of Directive if raw data reveal information that could have been regarded as such data.[149]

Pursuant to Art. 8 Section 1 of the DPD, sensitive data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. According to the DPD, biometric data did not need to serve for unique identification of the data subject to be considered as sensitive data. In 2012, WP 29 reflected on special character of biometric data and introduced guidelines for processing of particular biometric data.[150] According to this opinion, data controllers should have implemented privacy by design,[151] privacy impact assessment,[152] and should have taken technical and organizational measures reflecting the sensitiveness of such data.[153]

2.2.1.2 GDPR and Biometrics

The DPD was replaced by 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 – the GDPR.

Pursuant to Art. 4 (1) of the GDPR "personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who 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."

In contrast to the DPD, the GDPR specifically mentions the term biometric data and regulates their processing. Pursuant to Art. 4 (14) "biometric data means 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".

---

[148] ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 4/2007 on the concept of personal data (WP 136), p. 8. *European Commission* [online] 2007 [2019-09-15]. Available from: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>.

[149] ARTICLE 29 DATA PROTECTION WORKING PARTY. Working document on biometrics (WP 80), p. 10. *European Commission* [online] 2003 [2019-09-15]. Available from: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf> .

[150] ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 3/2012 on developments in biometric technologies (WP 193). *European Commission* [online] 2012 [2019-09-15]. Available from: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf>.

[151] Ibid., p. 28.

[152] Ibid., p. 29.

[153] Ibid., p. 31.

The GDPR recognizes six lawful grounds for processing (Art. 6 GDPR). That means that a controller[154] can process personal data only if there exists one or more lawful grounds for processing. Those grounds are the following:

"a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

c) processing is necessary for compliance with a legal obligation to which the controller is subject;

d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

f) processing is necessary 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 which require protection of personal data."

Biometric data pertain to the so-called special category of personal data and as such, they are subject to the special rules referred to in Art. 9 of the GDPR. According to the Recital 51 of the GDPR, only those data that are "processed through a specific technical means allowing the unique identification or authentication of a natural person" are considered biometric data. Biometric data are characterized by the fact that they can be read relatively easily from the body of a person and recorded, for example, in a photograph, video or voice recording. At the moment, however, these data are considered raw data, i.e. the data that are not processed and as such they are not considered biometric data according to the GDPR. Biometric data in the sense of the GDPR, so called biometric templates, are created only after processing of raw data. This type of personal data is then subject to special rules.

Art. 9 (1) contains a general clause prohibiting the processing of biometric data for the purpose of the unique identification of a natural person. The article, however, also lays down exceptions to this prohibition (see below). In this context, it is interesting that the article omits the term "authentication" used in the Recital 51. Authentication can be understood as confirmation of identity (one-to-one) versus its determination (one-to-many). This may give the impression that the GDPR excludes from the abovementioned clause the prohibition of processing biometric data, such as verifying the identity of the phone owner with the fingerprint reader, since in doing so the phone compares the already stored template with the submitted identifier (fingerprint) in order to determine whether or not he or she is the same person. Thus, the system itself does not search the fingerprint database and does not determine the identity of the person presenting the fingerprint. On the other hand, the very definition of biometric data in Art. 4 (14), which states that the biometric data allows or confirms unique identification, it may be concluded that the Art. 9 does not specify how unique identification should be achieved. Thus, Art. 9 (1) covers both cases, i.e. both authentication and identification.

Although processing of biometric data is generally prohibited, Art. 9 (2) provides for ten exceptions to that prohibition. Biometric data referred to in Art. 9 (2) (a) may be processed if "the data subject has

[154] A controller is "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" (Art. 4 (7) of the GDPR).

given explicit consent to processing of such personal data for one or more specified purposes, except where Union or Member State law provides that the prohibition referred to in paragraph 1 cannot be lifted by the data subject". The conditions for granting consent are further specified in Art. 7 of the GDPR and its recitals. The controller processing biometric data on the basis of consent must always be able to demonstrate that such consent has been given. The consent of the data subject must be requested in such a way that the data subject is genuinely and clearly acquainted with the fact that he or she gives his or her consent to the processing of his or her data. A request for consent should not be part of long arrangements where the granting of consent is not clear. The consent must be an active confirmation of the data subject, in the other words silence or a pre-marked consent in the electronic form are invalid.[155] The consent with processing of the biometric data must be explicit. WP29 in its guidelines defined the explicit consent as the consent that is expressed by the data subject, in other words an express statement of consent given by the data subject. The express statement could be a written statement or "statement by filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, or by using an electronic signature."[156]

Other cases in which the controller may process biometric data for unique identification purposes are the following:

"a) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in providing that the law provides for appropriate safeguards for the fundamental rights and the interests of the data subject,

b) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent,

c) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

d) processing relates to personal data which are manifestly made public by the data subject,

e) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

f) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject,

g) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards of professional secrecy,

[155] ARTICLE 29 WORKING PARTY. Guidelines on consent under Regulation 2016/679. In: *European Data Protection Board* [online]. 10. 4. 2018 [2019-09-30]. Available at: <https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en>. See p. 16.

[156] Ibid., p. 18.

h) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy,

i) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Art. 89 (1) of the GDPR based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject."[157]

Compared to the Data Protection Directive, the GDPR provides Member States with very limited space for derogations in national legislation. In case of the processing of biometric data, Member States may maintain or introduce further conditions, including limitations of such processing (Art. 9 (4) of the GDPR).

When processing biometric data, a controller must adhere to general principles relating to processing of personal data that are set out in Art. 5 of the GDPR. A controller must comply with criteria of lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability. With regard to biometric data, it is important to highlight the principle of purpose limitation. According to this principle, personal data must not be processed in a manner that is incompatible with initially specified purposes. However, the GDPR allows for processing for other than originally defined purpose in Art. 6 (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. Further processing of personal data for scientific or historical research purposes or statistical purposes are not considered to be incompatible with the initial purposes. However, processing for scientific or historical research purposes or statistical purposes must be subject to implementation of appropriate technical and organizational measures in order to safeguard the rights and freedoms of data subjects.

Data subjects have specific rights defined in Chapter III. of the GDPR. Data subjects have right to transparent information and communication (Art. 12); right to information (Art. 13 and 14); right of access (Art. 15); right to rectification (Art. 16); right to erasure – also called the right to be forgotten (Art. 17); right to restriction of processing (Art. 18); right to be notified about rectification, erasure of personal data, or restriction of processing (Art. 19); right to data portability (Art. 20); right to object (Art. 21); and right not to be subject to automated decision-making including profiling (Art. 22).

The right to transparent information and communication 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. In order to provide clear explanation of this right, the WP29 issued specific guidelines on how to fulfil transparency requirements properly.[158] 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.[159] Only those who truly understand what processing of their personal data entails are able to decide whether and under which conditions they are willing to give

[157] Art. 9 (2) of the GDPR.
[158] ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on transparency under Regulation 2016/679. In: *European Commission* [online]. 2017 [2019-12-02]. Available at: <http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850>.
[159] Ibid.

consent to such processing to a controller, to enter into contractual relationship with a controller. The controller has to inform data subjects among others about the purposes of the processing for which the personal data are intended as well as the legal basis for the processing, the recipients or categories of recipients of the personal data, data transfer, retention period, rights of the data subjects, incl. their right to withdraw a consent. The information has to be provided at the time when personal data are obtained, or where personal data have not been obtained from the data subject, the controller provides the data subject with the information at the latest within one month. Moreover, data subjects have to be provided with information whenever they claim their right of access. In case when the controller applies automated decision-making, including profiling, the controller has to provide meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. 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, controllers might avoid informing the data subject by design while calculating risk of the probability that such practice would ever be revealed. It is difficult, if not impossible, for data subjects to verify information about the processing.

With regard to the right to erasure, the GDPR enumerates situations in which data subjects can exercise this right, e.g. if the personal data are no longer necessary in relation to the purposes, a data subject withdraws their consent, or the personal data have been unlawfully processed. The right to erasure is not absolute. The data subject cannot claim the right when for instance processing is necessary for compliance with a legal obligation of the controller, for reasons of public interest in the area of public health in accordance with Art. 9(2) and (3), or for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes.

The right to data portability is the right to transfer the data between the controllers. This right is applicable only when data are processed on the basis of consent or contract and the processing is carried out by automated means. When biometric data are processed under the aforementioned lawful grounds, the controller has to hand over the data to the data subject in a structured, commonly used and machine-readable format and/or to transmit those data to another controller.

The right to object is applicable when the controller processes the personal data on the grounds of the legitimate interest or for the performance of a task carried out in the public interest. The controller may no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. Where personal data are processed for direct marketing purposes, the data subject has the right to object at any time to processing of personal data. The controller may not process the personal data for direct marketing after receiving such an objection.

Data subjects are also guaranteed the right not to be subject to an automated decision-making[160] including profiling. According to Art. 22 (1) “the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her”. However, processing of biometric data is always inherently automated. The question is then whether the data subject is significantly affected by a situation in which for instance a possible refusal of access to either a particular service or a certain space based on analysis of biometric data would occur. Guidelines of WP29 state that effects of such data processing “must be sufficiently great or important to be worthy of attention. In other words, the decision must have the potential to significantly affect the circumstances, behaviour

[160] 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.

or choices of the individuals concerned, have a prolonged or permanent impact on the data subject, or at its most extreme, lead to the exclusion or discrimination of individuals."[161] If that were the case, biometric data could only be processed on condition that the data subject had given his explicit consent, the processing is necessary for entering into, or performance of, a contract between the data subject and a data controller; or that the processing was necessary for reasons of significant public interest under Union or Member State law. At the same time, rights, freedoms and legitimate interests of data subjects must be safeguarded.

In the GDPR, automated decision-making is tightly connected with profiling. Biometrics as such is a broad term including information about "individual aspects of constitution or functioning or behaviour of a biological organism".[162] 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.[163]

The dangers and risks of using biometric data for profiling have already been summarized in literature. [164] Merging unique identifiers of a person with profiling techniques can violate the right of information self-determination, enslave the humankind and result in discrimination.[165] 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".[166]

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".[167] 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.

It is important to note that 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,[168] it is questionable if deriving additional

---

[161] ARTICLE 29 WORKING PARTY. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. In: *European Data Protection Board* [online]. 6. 2. 2018 [2019-09-30]. Available at: <https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en>. See p. 21.

[162] 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>.

[163] KINDT, E. J. *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis*, p. 349.

[164] For instance, HILDEBRANDT, M. – GUTWIRTH, S. (eds). *Profiling the European 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: SYNODINOU, T.E. et al. (eds). *EU Internet Law. Regulation and Enforcement*. Cham: Springer, 2017.

[165] Ibid., p. 351–352.

[166] Art. 4 (4) of the GDPR.

[167] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on consent under Regulation 2016/679*.

[168] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*.

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.

Finally, it must be noted that automated decisions, including profiling, which would have legal effects or otherwise have a significant impact on the data subject should not be based on biometric data although there might be exceptions to this rule if conditions of Art. 22 (4) of the GDPR are met (for details on processing biometric data related to online behaviour and profiling see Section 2.2.1.3).

Apart from obligations corresponding to data subjects' rights, controllers have also other specific obligations. One of these obligations is to ensure integrity and confidentiality of the personal data. Pursuant to Art. 32 of the GDPR the controller has to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk for the rights and freedoms of natural persons. The higher the risk of interference with fundamental rights and freedoms, the stricter measures should be taken by the controller. This implies that when a controller processes biometric data, it should take measures that specifically guarantee security and integrity so that the privacy of the data subject is effectively protected.

In case when personal data leak, an unauthorized person gets access to the data or the data are compromised otherwise, the controller has to without undue delay and later than 72 hours after having become aware of the data breach, notify the personal data breach to a data protection authority (Art. 33 GDPR). The notification is not necessary if only the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. The breach of biometric data in most cases presumably lead to that risk. It implies that in case of the breach of such data the controller will be obliged to notify the breach to the authority. Moreover, the controller has to communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons (Art. 34 GDPR).

Another important duty of a controller in processing biometric data is the obligation to carry out a Data Protection Impact Assessment (hereinafter "DPIA") pursuant to Art. 35 of the GDPR. Where a type of processing especially using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller will, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A data protection impact assessment is in particular required in case that the controller processes special categories of data on a large scale. According to Guidelines on Data Protection Impact Assessment the controller, when assessing whether the processing is carried out on a large scale, has to consider factors such as "the number of data subjects concerned, either as a specific number or as a proportion of the relevant population; the volume of data and/or the range of different data items being processed; the duration, or permanence, of the data processing activity; the geographical extent of the processing activity."[169] It can be assumed that the large part of controllers processing biometric data is obliged to carry out the personal data impact assessment before commencing processing due to processing such data on a large scale or due to application of new technologies or/and the presence of high risk to rights and freedoms of data subjects, i.e. the right to privacy or prohibition of discrimination.

Where the principal activity of the controller or processor consists of large scale processing of biometric data, the controller has to appoint a data protection officer (hereinafter "DPO") in accordance with Art. 37 of the GDPR. Data protection officer is entitled to have access to all information related to

[169] ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. In: *European Data Protection Board* [online]. 2018 [2019-12-02]. Available at: <https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en>. See p. 10.

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.

2.2.1.3 Biometrics and Profiling of Online Behaviour under the GDPR[170]

According to Eurostat, 76 % of European citizens use the Internet on a daily basis.[171] Their activity leaves traces about their online behaviour. Identity of these individuals can be verified[172] or determined with the help of cookies, i. e. pieces of data stored in a device that provides information to servers with which a device is communicating.[173] Determination and verification of users' identities with the help of cookies is called explicit tracking and it relies on the cooperation of either users or their web browsers.[174] However, Internet users can be identified also based solely on their online behaviour with behaviour-based tracking techniques that do not need cookies or any other explicit identifiers.[175] Such identification happens unobtrusively and, in principle, without the knowledge of people whose behaviour is being monitored. This technique exploits methods of pattern recognition and applies them either on web surfing behaviour, activity of applications installed on a device, or environmental peculiarities.[176] With regard to its purpose, behaviour-based tracking partly corresponds to the definition of behavioural biometrics that seeks "to quantify behavioral traits exhibited by users and use resulting feature profiles to successfully verify identity".[177]

The term behavioural characteristic is not defined in the GDPR. Behavioural-based biometric data are considered dynamic while still having general characteristics of being universal to all people, unique for each person, and permanent.[178] According to WP29 that was replaced by European Data Protection Board (hereinafter "EDPB") but whose opinions stay valid, typical behavioural biometric data "include hand-written signature verification, keystroke analysis, gait analysis, way of walking or moving, patterns indicating some subconscious thinking like telling a lie, etc."[179] As this definition refers to patterns of

[170] This subsection was published in KRAUSOVÁ, A. Online Behavior Recognition: Can We Consider It Biometric Data Under GDPR? *Masaryk University Journal of Law and Technology*. 2018, Vol. 12, No. 2 [2019-12-08]. Available at: <https://journals.muni.cz/mujlt/article/view/8803>.

[171] EUROSTAT. Internet usage. Eurostat (isoc_ci_ifp_iu) and (isoc_ci_ifp_fu). In: *European Commission*. [online]. 2018 [2019-09-30]. Available at: <https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals#Internet_usage>.

[172] See Recital 25 of ePrivacy directive. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[173] EUROPEAN COMMISSION. Cookies. In: *European Commission* [online]. 2016 [2017-12-22] Available at: <http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm>.

[174] BANSE, C. – HERRMAN, D. – FEDERRATH, H. Tracking Users on the Internet with Behavioral Patterns: Evaluation of its Practical Feasibility. In: GRITZALIS, D. – FURNELL, S. – THEOHARIDOU, M. (eds). *27th IFIP TC 11 Information Security and Privacy Conference, SEC 2012* Heraklion, Crete, 4–6 June 2012, Berlin: Springer, p. 235.

[175] Ibid., p. 235 and 246.

[176] Ibid., p. 242.

[177] YAMPOLSKIY, R. V. – GOVINDARAJU, V. Taxonomy of Behavioral Biometrics. In: LIANG, W. – XIN, G. (eds). *Behavioral Biometrics for Human Identification: Intelligent Applications*. IGI Global, 2010. Available at: <https://www.researchgate.net/publication/254217766_Taxonomy_of_Behavioural_Biometrics>.

[178] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Working document on biometrics*, p. 3.

[179] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 3/2012 on developments in biometric technologies*, p. 4.

thinking and moving that are then manifested and recorded in an objectively perceivable manner, online behaviour of a person perceivable through her specific usage of devices or contents searching patterns should also fall under the definition of behavioural data if it serves as a means for unique identification.

Unique identification is the key term of the definition that determines whether behavioural data will fall in the category of biometrics. The term unique identification is used only at two places in the GDPR – in the very definition of biometric data in Art. 4 (14) and in the Recital 51. However, the GDPR does not provide any explanation as to the meaning of unique identification.

From a semantic point of view, "unique identification" can refer to recognizing someone as being the one and only person.[180] According to WP29, however, this term is relative as it "depends on different factors including the size of the database and the type of biometrics used".[181] Moreover, it is generally known that no type of biometrics is fully reliable. Biometric accuracy differs with regard to the technology used. In order to achieve a higher degree of accuracy, dual biometrics is sometimes recommended.[182] Nevertheless, if no biometric system can guarantee unique identification in all cases, it is then questionable what degree of probability would be sufficient to classify a technology as processing biometric data within the meaning of the GDPR. As the Recital 15 of the GDPR states that "the protection of natural persons should be technologically neutral and should not depend on the techniques used," various biometric technologies should not be discriminated against with regard to their performance. In an opposite case, this might lead to circumvention of obligations set out in the GDPR and result in harm to data subjects, i. e. natural persons whose personal data is processed. Determining acceptability of an accuracy level is then a different question that should not influence classification of a system as being a biometric system.[183]

Technological neutrality is crucial also in determining whether mere monitoring users' online behaviour, its analysis for creating identification profiles, and consequent application of these profiles qualifies as biometrics. Traditional biometric systems use sensors, such as cameras (facial recognition) or microphone (voice recognition), that directly measure some natural property of a human and modify it into an electric signal.[184] Biometric systems monitoring users' online behaviour utilize devices of these users as sensors and apply own remote analytics upon the gathered data. Utilization of a keyboard, mouse or touchpad in fact provides information about behaviour that is converted into an electric signal. Identity of users is digitalized[185] such as with any other type of biometrics. Specific templates can be created based on these data as well.

The term biometric data within the meaning of the GDPR then includes any data resulting from electronic processing of data gathered based on physical, physiological or behavioural characteristics of a person regardless of sensors used if such resulting data are used for the purpose of unique identification. Errors in accuracy should not per se discriminate a system from being considered

[180] According to a dictionary the term "to identify" means "to recognize or establish as being a particular person or thing", while "unique" can be understood as "existing as the only one or as the sole example; single; solitary in type or characteristics". See *Webster's Encyclopedic Unabridged Dictionary of the English Language*. New York: Random House, 1996, p. 950 and 2074.

[181] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Working document on biometrics*, p. 2.

[182] WILSON, C. R. Biometric Accuracy Standards. In: *National Institute of Standards and Technology* [online]. 2003 [2017-11-20] Available at: <https://csrc.nist.gov/CSRC/media/Events/ISPAB-MARCH-2003-MEETING/documents/March2003-Biometric-Accuracy-Standards.pdf>.

[183] WP 29 formulated several criteria for assessing acceptability of accuracy: the purpose of processing, false accept rate (probability of incorrect identification), false reject rate (probability of incorrect rejection during identification), population size, and "the ability to detect a live sample". ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 3/2012 on developments in biometric technologies*, p. 6.

[184] MORDINI, E. – TZOVARAS, D. – ASHTON, H. Introduction. In: MORDINI, E. – TZOVARAS, D. (eds). *Second Generation Biometrics: The Ethical, Legal and Social Context*, p. 7.

[185] GHILARDI, G. – KELLER, F. Epistemological Foundation of Biometrics. In: MORDINI, E. – TZOVARAS, D. (eds). *Second Generation Biometrics: The Ethical, Legal and Social Context*, p. 40.

as processing biometric data. The resulting data become biometric data at the moment when they enable a system to recognize a person from all other people enrolled in the system.[186]

Online behaviour recognition in the meaning of determining or verifying identity falls under the category of behavioural biometrics defined from a technical point of view. In general, there are five categories of behavioural biometrics and each of them is based on analysis of different features.[187] Online behaviour recognition is based on monitoring the activity of a device. This activity can be caused either by a user (active use of applications as well as regular breaks and switching between applications that may result in identification of original patterns of behaviour) or by the device itself.

With regard to the very nature of biometrics and the purpose of protecting personality of humans, only templates based on activity originating from a natural person can be considered as biometric data within the meaning of the GDPR. Behavioural patterns are expressions of one's own identity and, therefore, deserve strict legal protection. These patterns can be observed also indirectly from "observable low-level actions of computer software" such as call traces, audit logs, program execution traces etc.[188] On the other hand, activity of a device itself does not constitute a link to a personality of their users. It could constitute such a link only with the help of additional information.

A complicated situation would arise when both user's activity as well as device's activity would be analysed together and such analysis would then result in a combined biometric template. How should one determine which data is biometric and which data is not? The technique of combining more types of input data typically happens in multi-modal biometric systems and is called information fusion.[189] The fusion can be performed at three levels – at the feature extraction level when the system merges data from all sensors, at the matching score level when the system combines values of matching scores from various sensors, and at the decision level when decisions based on matching scores (accept/reject decision) are combined.[190] From the legal point of view, the problem arises only when data from all sensors would be merged (at the feature extraction level) so the resulting identification data would not be based solely on "the physical, physiological or behavioural characteristics" as defined in the GDPR. There are already solutions utilizing so called hybrid information fusion that combine a biometric component with a numerical component.[191] In special environments, especially in the online behaviour recognition area, systems might start to utilize various types of data, including activity initiated solely by a device. Such identification data based on hybrid information fusion should be, however, considered as biometric data. The GDPR does not impose a requirement that specific technical processing needs to relate *solely* "to the physical, physiological or behavioural characteristics". It only need to relate to it and combination with a different kind of information should not prevent the data from being awarded a higher level of protection.

Creation of biometric behavioural templates relies on spotting patterns in behaviour as well as in analysis of psychological traits of a person. Psychological-based biometric techniques measure individual's "response to concrete situations or specific tests to conform to a psychological profile".[192]

---

[186] According to WP29 "a natural person can be considered as ''identified'' when, within a group of persons, he or she is ''distinguished'' from all other members of the group". ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 4/2007 on the concept of personal data*, p. 12.

[187] These are authorship-based biometrics, biometrics based on monitoring human-computer interaction, indirect biometrics based on monitoring low level actions of SW, kinetics based on monitoring motor skills of people, and purely behavioural biometrics based on monitoring a human while performing mentally demanding tasks. For details see YAMPOLSKIY, R. V. – GOVINDARAJU, V. *Taxonomy of Behavioral Biometrics*.

[188] Ibid, p. 2–3.

[189] ROSS, A. – JAIN, A. Information Fusion in Biometrics. *Pattern Recognition Letters*. 2003, Vol. 24, No. 13, pp. 2115–2125 [2017-11-02]. Available at: <https://www.sciencedirect.com/science/article/pii/S0167865503000795?via%3Dihub>. See p. 2117.

[190] Ibid.

[191] IOVANE, G. – BISOGNI, C. – DE MAIO, L. – NAPPI, M. An encryption approach using Information Fusion techniques involving prime numbers and Face Biometrics. *IEEE Transactions on Sustainable Computing*. 2018 [2018-01-15]. Available at: <http://ieeexplore.ieee.org/document/8259031/>.

[192] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 3/2012 on developments in biometric technologies*, p. 4.

Therefore, utilization of such techniques might be also considered as profiling[193] within the meaning of the GDPR. As it has been already mentioned, profiling is defined in its Art. 14 (4) of the GDPR 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".

In general, the difference of profiling and biometrics lies in their purpose. Biometrics is used for determining or verifying an identity of a person, while profiling aims at evaluation of a natural person and possibly placing that person in a certain group or category. Profiling can be even based on biometric data themselves as a special category of personal data. In such case special obligations apply.[194] However, even the GDPR uses the term "profile" as a means of possible identification of a person.[195] The question is whether profiling itself can result in creation of biometric data, i. e. if a specific profile of a person based on her behaviour that enables her identification is created, should it be considered as biometric data even if the initial intention of a controller was not to process biometric data?

The answer is yes. Information about online behaviour of a person relates to her physical, physiological, behavioural, or psychological characteristics as it refers to her state of mind (typically search for specific contents) or her ability and manners in using a device that serves as a sensor. Combination of such gathered information leads to creation of a profile that can be compared to a biometric template created based on multi-modal biometrics. It is worth to note that even though the main purpose of profiling is evaluation, profiling does not need to include inference, i. e. any judgment based on the data.[196] Moreover, identification is typically achieved based on evaluation of data through their comparison.

However, the condition for a profile to qualify as biometric data depends on its ability to distinguish a person to whom it relates from a group of people. The profile can be associated with a certain group (as in biometric systems there are for instance groups of users with different access rights) but in order to be considered as biometric data, it must be possible to exclude the profile from that group (requirement of unique identification). On the other hand, the exact identity of a person does not need to be determined. The reason is that biometric data can be used also only "to verify the identity without actually identifying the individual".[197]

The fact that a profile of a person based on her online behaviour allowing her unique identification has legal consequences both for controllers as well as data subjects. The most important obligation of controllers relates to respecting principles relating to processing personal data. In order to comply with the GDPR requirements, controllers must continually examine their data and profiles based on the data in order to determine whether they process biometric data or not. The crucial element here is the potential of the data to allow unique identification.[198] However, processing of biometric profiles needs to fulfil requirements for processing special categories of data under Art. 9 of the GDPR only if a controller uses the profile among other to distinguish a particular person from others. Especially in the context

[193] Profiling is based on the use of algorithms "to locate unexpected correlations and patterns". See HILDEBRANDT, M. *Smart Technologies and the End(s) of Law*. Cheltenham: Edward Elgar Publishing, 2015, p. 241.

[194] See Art. 22 of the GDPR and for details ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*.

[195] Recital 30 of the GDPR stipulates the following: "Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them."

[196] ARTICLE 29 WORKING PARTY. *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, p. 9

[197] Ibid., p. 10.

[198] This can be perceived as parallel to the very definition of personal data as any information relating to an identifiable natural person.

of an online environment where exceptions for processing biometric data other than explicit consent, controllers need to make sure to be able to prove that a data subject granted them an explicit consent.[199]

The profiles composed fully or partially from the biometric data may be used for automated decision making. On the basis of the profile, the individual may be automatically denied access to certain places, for instance due to his non-standard behaviour or a contract may not be concluded, e.g. if the individual's profile refers to a poor physical condition, the insurance company may automatically decide not to enter into an insurance contract with such individual. The GDPR regulates the automated individual decision-making in Art. 22. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. From the text of the regulation it was not clear whether the GDPR forbid the automated decision-making or the data subject solely had a right to object such processing. The WP29 in its guidelines speaks about a general prohibition of automated decision-making with exemptions.[200]

The prohibition of automated decision-making does not apply if the decision is necessary for entering into, or performance of, a contract between the data subject and a data controller, paragraph 1 shall not apply if the decision is necessary for entering into, or performance of, a contract between the data subject and a data controller,

such processing is authorised by the EU or member state law on condition that the law lay down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, or

the automated decision-making is based on the explicit consent (Art. 22 (2) of the GDPR).

Besides the abovementioned conditions the automated decision-making based on the special categories of data is subject to the second limitation. The special categories of data may not be used for such decisions with exemption of the processing based on the explicit consent (Art. 9 (2) a) GDPR) or in case that the processing necessary for reasons of substantial public interest (Art. 9 (2) g) GDPR). Moreover, suitable measures to safeguard the data subject's rights and freedoms and legitimate interests must be in place.

When the controller processes the personal data by automated decision-making, he/she has some specific obligation according to the GDPR. The controller has to inform the data subject about the existence of automated decision-making, including profiling and provide to the data subject with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject (Art. 13 (2) f), Art. 14 (2) g), Art. 15 (1) h) of the GDPR). According to the WP29 "The controller should find simple ways to tell the data subject about the rationale behind, or the criteria relied on in reaching the decision. The GDPR requires the controller to provide meaningful information about the logic involved, not necessarily a complex explanation of the algorithms used or disclosure of the full algorithm. The information provided should, however, be sufficiently comprehensive for the data subject to understand the reasons for the decision."[201]

In the case of automated decision-making the controller has to carry out the data protection impact assessment (DPIA), since the DPIA is obligatory when the processing involves a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated

[199] For details about requirements on explicit consent see ARTICLE 29 WORKING PARTY. *Guidelines on Consent under Regulation 2016/679*.
[200] ARTICLE 29 WORKING PARTY. *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, p. 19.
[201] Ibid., p. 25.

processing, including profiling, and on which decisions are based that produce legal or similar effects. Moreover, the controller has to designate the data protection officer when the core activities of the controller or the processor consist of processing (e.g. by automated decision-making) on a large scale of special categories of data.

2.2.2 National Derogations of Selected Member States to the GDPR and the Data Protection Directive for Police and Criminal Justice Authorities with Regard to Biometrics

Despite the GDPR sets out a common standard for processing special categories of personal data, according to Art. 9 (4) of the GDPR "Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health". Moreover, Member States may also introduce national derogations from certain rights of data subjects in cases when biometric data are processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.[202]

With regard to the GDPR, a number of Member States have already introduced national laws reacting to this regulation. These national laws mainly complement the rules of personal data processing set out in the GDPR and provide for national derogations. Some of them also implement a directive published together with the GDPR – the Data Protection Directive for Police and Criminal Justice Authorities (hereinafter "DPDCJA").[203]

2.2.2.1 Belgium

An act adapting the GDPR in Belgium of 30 July 2018 was officially published on 5 September 2018.[204] This act provides a number of specific rules regarding processing biometric data. In Art. 8. § 1. the act specifies what can be considered as a necessary processing for reasons of substantial public interest in the sense of Art. 9 par. 2 (g) of the GDPR. In Art. 8. § 1. 3° the act specifies conditions for processing personal data regarding sexual life by associations and foundations whose primary objective of existence is to evaluate and provide counselling and treatment for people whose sexual behaviour can be qualified as crime. Except for special legal provisions, this particular provision prohibits processing of genetic and biometric data with the aim to uniquely identify a person by these organizations.

In TITLE 2, the act implements the DPDCJA. In Art. 26. 13° the definition of biometric data is provided. This definition corresponds to the definition in the DPDCJA. Art. 34 of the act implements Art. 10 of the DPDCJA (Processing of special categories of personal data). Further conditions for processing

[202] Conditions for these derogations are set out in Art. 89 (2) – (4) of the GDPR.

[203] This shortened title is used in an official summary of EU Legislation in EUR-Lex. See Protecting personal data when being used by police and criminal justice authorities. In: *EUR-Lex* [online]. 2017 [2019-01-30]. Available at: <https://eur-lex.europa.eu/legal-content/ENG/TXT/?uri=LEGISSUM:310401_3>. British Data Protection Act 2018 refers to this directive as to Law Enforcement Directive (Art. 1 (4)). Some resources refer to the directive as the Data Protection Directive on Police Matters. See LAURI, J. p. *The Data Protection Directive on Police Matters 2016/680 protects privacy – The evolution of EU's data protection law and its compatibility with the right to privacy*. Master's thesis, University of Helsinki 2017. The official resource is Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89.

[204] Wet 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, *BS* 5 september 2018, C-2018/40581.

biometric data are set out in Art. 34. § 2: a competent authority or a processing authority must keep a list of categories of persons who have access to the personal data, with a description of their status relative to the processing of the intended data. This list must be made available to the competent supervisory authority. These persons must be bound to keep the data confidential either through statutory obligation or an equivalent contractual obligation.

In TITLE 3 (Processing of personal data by other authorities), Subtitle 1, the act provides rules for processing personal data by intelligence and security services. Art. 76 entitles the intelligence and security services to process all categories of personal data including biometric data. In Subtitle 2, the act provides rules for processing personal data by armed forces. Art. 105. 1° entitles the armed forces to process all categories of personal data including biometric data as well. This applies, however, only in periods when armed forces are deployed or are supposed to be deployed. Even then, principle such as purpose limitation, lawfulness and fairness of processing, etc. apply (Art. 105. 2°, 3°, 4°, 5°, 6°). Certain rights of data subjects can be limited (Art. 105. 9°). In Subtitle 3, the act provides rules for processing personal data in the context of Act of 11 December 1998 concerning the classification and security clearances, safety certificates and safety advice. Governments, authorities, and subjects specified in Art. 107 are entitled to process all categories of personal data including biometric data. This applies also for the Coordinating body for the threat analysis (Subtitle 4, Art. 142). Special authorisation for processing biometric data is provided also for public authorities specified in Art. 185.

2.2.2.2 Croatia

Croatia adopted the Act on Implementation of the General Data Protection Regulation on 27 April 2018.[205] This act, however, does not implement the DPDCJA (Art. 1(2)). The act adopts definitions set out in the GDPR by referencing to its text (Art. 3(1)). Part IV. of the act focuses on processing personal data in special cases. Processing of biometric data is regulated in Art. 21 – Art. 24.

Art. 21 regulates processing biometric data by public authorities. According to Art. 21(1) processing is allowed only in cases provided for by law or, if necessary, also for the protection of persons, property, classified information or business secrets if interests of a data subject do not prevail. According to Art. 21(2) processing of biometric data shall be considered in accordance with the law if it is necessary for the fulfilment of obligations under international treaties regarding the identification of an individual in the crossing of the state border.

Art. 22 regulates processing biometric data in private sector. According to Art. 22(1) processing is allowed only in cases provided for by law or, if necessary, also for the protection of persons, property, classified information, business secrets, or for individual and safe identification of users of services if interests of a data subject do not prevail. According to Art. 22(2) when biometric data is processed for the purpose of safe identification of users of services, these users must provide an explicit consent compliant with the GDPR.

Art. 23 regulates processing of biometric data of employees for the purpose of recording of working hours and for entering and leaving the premises. Such processing is possible if it is prescribed by law or if such processing is carried out as an alternative to another solution for recording the working time or entering and leaving the premises and an employee has given an explicit consent compliant with the GDPR.

Art. 24 regulates applicability of the provisions on processing biometric data and declares that provisions of this act on the processing of biometric data shall not affect the obligation to carry out an assessment

[205] Zakon o provedbi Opće uredbe o zaštiti podataka (Narodne novine, br. 42/2018).

of performance in accordance with Article 35 of the GDPR. Moreover, it stipulates that these provisions shall not apply to the area of defense, national security and a security-intelligence system.

2.2.2.3 The Czech Republic

The Czech Republic adopted the Act No. 110/2019 Coll., on Personal Data Processing (hereinafter Personal Data Processing Act or PDPA)[206] that implemented some provisions of the GDPR and the DPDCJA. The act regulates, besides other things, the processing of personal data by public authorities, however, it does not contain any special regulation according Art. 9 (4) GDPR. The act provides in Section 16 that the special categories data processed for scientific or historical research purposes or statistical purposes should be anonymized, unless this is prevented by legitimate interests of the data subject. The act does not contain any specific provision regarding to biometric data.

2.2.2.4 France

French law reacted to the GDPR and the DPDCJA by amending the existing act on data, files and freedoms of 1978[207] by an act of 20 June 2018 on the protection of personal data.[208]

Art. 8 of the act on data, files and freedoms roughly corresponds to Art. 9 of the GDPR and in general prohibits processing of special categories of personal data including biometric data for the purposes of unique identification of a person. However, there are certain differences. For instance, the French law uses the term “consentment exprès” instead of “consentement explicite”. The legal basis for processing special categories of personal data is structured differently than in the GDPR. Art. 8 II. 9° allows employers and administrators to process biometric data that are strictly necessary for the control of the access to the work places as well as for devices and applications used in the context of the tasks entrusted to employees, agents, trainees or service providers. However, this processing must comply with regulations put in place by the National Commission for Informatics and Liberties.

According to Art. 11 I. 2° b) this Commission is entitled to draw up and publish model regulations to ensure the security of personal data processing systems and to regulate the processing of biometric, genetic and health in consultation with the public and private bodies representing the actors concerned. As such, except for the treatments implemented on behalf of the State acting in the exercise of its prerogatives of public authority, the Commission may prescribe additional technical, organizational and other measures for the processing of biometric, genetic and health data pursuant to Art. 9 par. 4 of the GDPR.

2.2.2.5 Germany

Germany was the first EU Member State that adopted a new act to both react on the GDPR as well as to implement the DPDCJA.[209] This act was adopted already in July 2017. Biometric data are expressly mentioned in this act only in Part 3 that implements the DPDCJA. Art. 46 defines biometric data in par. 12 and in par. 14 stipulates that biometric data for the purpose of uniquely identifying a natural person belong to the category of special categories of personal data.

---

206 In Czech Zákon č. 110/2019 Sb., o zpracování osobních údajů.
207 *Loi* n° 78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés.
208 *Loi* n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.
209 Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) vom 30. Juni 2017 (BGBl. I v. 5.7.2017, S. 2097).

However, what regards special categories of personal data as defined in the GDPR in Art. 9 (1), the German act contains detailed rules and derogations of the GDPR in Art. 22 – 28. These provisions focus on processing of special categories of personal data and processing for other purposes.

According to Art. 22 (1) the processing of special categories of personal data as referred to in Article 9 (1) of the GDPR shall be permitted by public and private bodies if processing is necessary to exercise the rights derived from the right of social security and social protection and to meet the related obligations; processing is necessary for the purposes of preventive medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services or pursuant to the data subject's contract with a health professional and if these data are processed by health professionals or other persons subject to the obligation of professional secrecy or under their supervision; processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices; in addition to the measures referred to in subsection 2, in particular occupational and criminal law provisions to ensure professional secrecy shall be complied with. Processing of special categories of personal data shall also be permitted by public bodies if processing is urgently necessary for reasons of substantial public interest; processing is necessary to prevent a substantial threat to public security; processing is urgently necessary to prevent substantial harm to the common good or to safeguard substantial concerns of the common good; or processing is necessary for urgent reasons of defence or to fulfil supra- or inter-governmental obligations of a public body of the Federation in the field of crisis management or conflict prevention or for humanitarian measures.

Art. 22 (2) provides a number of examples of appropriate measures how to safeguard interests of a data subjects. These measures include technical organizational measures to ensure that processing complies with the GDPR; measures to ensure that it is subsequently possible to verify and establish whether and by whom personal data were input, altered or removed; measures to increase awareness of staff involved in processing operations; designation of a data protection officer; restrictions on access to personal data within the controller and by processors; the pseudonymisation of personal data; the encryption of personal data; measures to ensure the ability, confidentiality, integrity, availability and resilience of processing systems and services related to the processing of personal data, including the ability to rapidly restore availability and access in the event of a physical or technical incident; a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing; specific rules of procedure to ensure compliance with this Act and with the GDPR in the event of transfer or processing for other purposes.

Art. 23 deals with processing of personal data for other purposes by public bodies. Art. 23 (2) defines conditions for processing special categories of data for other purposes. Such processing by public bodies is allowed if one of the conditions specified in Art. 23 par. 1 is met (processing in the interest of data subject, checking supposedly incorrect information, preventing substantial harm to the common good or threat to public security, prosecution of an administrative or criminal offence, preventing serious harm to another person, or exercising powers of supervision and monitoring) and at the same time an exception pursuant to Art. 9 (2) of the GDPR or to Art. 22 of the German act applies.

Art. 24 deals with processing of personal data for other purposes by private bodies. Its second paragraph is the same as at Art. 23. However, the conditions in Art. 24 (1) are much more limited compared to conditions in Art. 23 (1). Private bodies can process personal data for other purposes only if its purpose is to prevent threats to state or public security, or to prosecute criminal offences, or to establish, exercise or defend legal claims. At such cases the test of proportionality must be conducted to assess whether a data subject does not have an overriding interest.

Art. 25 deals with transfer of data by public bodies and in par. 3 stipulates comparable conditions as Art. 23 (2) and Art. 24 (2). There are different conditions for transferring personal data to public and private bodies.

Art. 26 (3) and (4) deal with processing special categories of data for employment purposes. Such processing can be done only if labour law, social security law and social protection laws allow to do so and at the same time the data subject does not have an overriding interest in prohibiting processing such data. Collective agreements can allow processing special categories of personal data as well.

Art. 27 also provides for derogations from Art. 9 (1) of the GDPR and specifies conditions for processing data for the purposes of scientific or historical research and for statistical purposes. Such data can be processed without consent if interests of a controller substantially outweigh interests of data subjects. This provision also limits rights of data subjects and sets out special conditions for rendering the data anonymous as well as keeping certain data separate from others. Publishing such data is also regulated. It can be done either with a consent of a respective data subject or if it is necessary to present research findings on contemporary events.

Finally, Art. 28 deals with processing special categories of personal data for purposes in public interest. The provision limits certain rights of data subjects.

2.2.2.6 Netherlands

In Netherlands, an act of 16 May 2018 was adopted to implement the GDPR in the national law.[210] This act, however, does not mention the DPDCJA. Processing of special categories of data is regulated in Art. 22 – 30.

Art. 23 specifies what can be considered as processing for reasons of substantial public interest in the light of Art. 9 (2) (g) of the GDPR: a) the processing is necessary to satisfy an international law obligation; b) the data are processed by the Authority for personal data or an ombudsman as referred to in Section 9:17 of the General Administrative Law Act, and to the extent that the processing is necessary for the performance of the tasks assigned to them by law, provided that such execution is provided for in such guarantees that the personal privacy of the data subject is not disproportionately harmed; or c) the processing is necessary in addition to the processing of personal data of a criminal nature for the purposes for which this data is processed.

Art. 24 specifies exceptions for scientific or historical research or statistical purposes in the light of Art. 9 (2) (j) of the GDPR: a) the processing is necessary for scientific or historical research or statistical purposes in accordance with Article 89 (1) of the GDPR; b) the investigation referred to in part a serves a general interest; c) asking for explicit consent is impossible or requires a disproportionate effort; and d) the performance shall be provided in such a way that the personal privacy of the data subject is not disproportionately harmed.

Art. 29 specifies exceptions for processing biometric data while also referring to Art. 9 (2) (g) of the GDPR. According to this provision the prohibition to process biometric data for the unique identification of a person does not apply if the processing is necessary for authentication or security purposes.

[210] Wet van 16 mei 2018, houdende regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119) (Uitvoeringswet Algemene verordening gegevensbescherming). *Stb*. 2018, 144.

2.2.2.7 Poland

In Poland, an act of 10 May 2018[211] was adopted to introduce specific rules in connection with the GDPR as well as to implement the DPDCJA. The Polish act does not contain any specific derogations of the GDPR with regard to biometric data. Processing of this data is mentioned only in Chapter 11 titled "Regulations on administrative fines and criminal provisions". Art. 107 regulated unlawful processing of personal data and as a punishment for such processing sets out a penalty of a fine or imprisonment of up to two years. If biometric data are processed unlawfully, the penalty is a fine or imprisonment of up to three years.

2.2.2.8 Romania

In Romania, the GDPR has been implemented mainly by an act 190/2018.[212] Art. 3(1) regulates processing of biometric data. According to this provision "processing of genetic, biometric or health-related data, for the purpose of achieving an automated decision-making process or creating profiles, is allowed with the explicit consent of the data subjects or, if the processing is based on express legal provisions, with the application of appropriate measures for the protection of the rights, freedoms and legitimate interests of the data subject".[213]

This act does not contain any further references to biometric data. However, Art. 6 specifies conditions for processing special categories of personal data for reasons of substantial public interest and refers directly to Art. 9, par. 2 (g) of the GDPR. The following safeguards must be in place: "a) application of adequate technical and organisational measures to observe the principles listed under Art. 5 of the General Data Protection Regulation, especially in terms of data minimisation and the principle of integrity and confidentiality, respectively; b) nomination of a data protection officer, if required as per Art. 10 of the present law; c) setting out storage periods according to the nature of the data and the processing purpose, as well as specific deadlines for deleting personal data or revising them for deletion purposes".[214]

The English translation also mentions that other implementation measures can also be found in Act No. 129/2018. Unfortunately, due to a language barrier we were not able to locate and review this document.

2.2.2.9 Slovakia

Slovakia adopted a special act on personal data protection on 30 January 2018.[215] This act provides for national derogations as well as implements the DPDCJA. In § 5 c) the act provides a definition of biometric data that corresponds to the definition in the GDPR. Part four of the act is devoted to specific situations of lawful processing of personal data. Biometric data are expressly mentioned in this part in § 78 (5). According to this provision a controller may process biometric data also based on a specific regulation or an international treaty by which the Slovak Republic is bound.

---

[211] Ustawa z dnia 10 maja 2018 r. – o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000).

[212] Information presented in this section is based on an unofficial translation of this act into English. See Law No. 190/2018 on measures for the application of Regulation (EU) 2016/679 of the European Parliament and 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). (Unofficial translation from Romanian language prepared by PrivacyOne). In: *IAPP* [online]. [2019-01-30]. Available at: <https://iapp.org/media/pdf/resource_center/Romanian_Data_Protection_Law_English_Translation.pdf>.

[213] Ibid.

[214] Ibid.

[215] Zákon č. 18/2017 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

This act also amends Slovak Nuclear Act and requires obligatory use of biometric identification when entering certain nuclear facilities.[216] This processing is considered as processing for reasons of substantial public interest according to Art. 9 (2) (g) of the GDPR.

2.2.2.10 United Kingdom

On 23 May 2018, the United Kingdom adopted Data Protection Act[217] that supplements the GDPR in its Part 2 and in its Part 3 implements the DPDCJA. The term biometric data is defined in Art. 205 (1). This definition corresponds to the definition in the GDPR.

For the purposes of law enforcement, the act defines in Art. 35 (8) (b) processing of biometric data for the purpose of uniquely identifying an individual as sensitive processing. Sensitive processing is permitted according to Art. 35 (5) only in two cases.

In the first case the two following conditions must be fulfilled: the data subject has given consent to the processing for the law enforcement purpose, and at the time when the processing is carried out, the controller has an appropriate policy document in place. This document must explain how the controller secures compliance with the data protection principles as well as what are the policies regarding the retention and erasure of personal data and namely provide an indication of the retention period.

In the second case the three following conditions must be fulfilled: processing is strictly necessary for the law enforcement purpose, it meets at least one of the conditions in Schedule 8 (These conditions are specified as statutory etc. purposes, administration of justice, protecting individual's vital interests, safeguarding of children and of individuals at risk, personal data already in the public domain, legal claims, judicial acts, preventing fraud, and archiving etc.), and at the time when the processing is carried out, the controller has an appropriate policy document in place (see above). Schedule 8 is a flexible tool for changing conditions of biometric data processing as it can be amended by the Secretary of State.

Schedule 1 of the act provides special rules for special categories of personal data. Part 2 of this Schedule specifies what are the conditions of substantial public interest. Biometric data can be processed with regard to support for individuals with a particular disability or medical condition.

2.2.3 Other EU Legislation

2.2.3.1 Travel Documents

Passports and travel documents are subject to unified rules in the European Union which set minimum security standards for such documents.[218] Biometric features, such as facial images and fingerprints, are mandatory in passports and documents. Fingerprints shall be included in interoperable formats. This data must be secured and stored on the data storage medium. This medium "shall have sufficient capacity and capacity to guarantee the integrity, authenticity and confidentiality of the data" (Art. 1 (2) of the Regulation). The biometric data contained in the document can only be used to verify

[216] See § 26(6) of Zákon č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon) a o zmene a doplnení niektorých zákonov.
[217] Data Protection Act 2018.
[218] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States.

the “authenticity of the document” and “the identity of the holder using directly available comparable features when the passport or other travel documents are required to be produced by law” (Art. 4 (3) of the Regulation). Persons have the right “to verify the personal data contained in the passport or travel document and, where appropriate, to ask for rectification or erasure” (Art. 4 (1) of the Regulation). The Regulation lays down specific rules and measures in the Annex which should be adopted and respected in the production of passports and documents. However, this applies in particular to the page with biographical data.

2.2.3.2 Documents Issued by the EU

Members of the institutions of the European Union and their servants receive a special document called *laissez-passer* issued pursuant to a separate regulation; the document is recognized as a travel document.[219] The document must comply with the above-mentioned Council Regulation 2252/2004. It contains both biographical and biometric data. Biometric features are facial image and two digital fingerprints. The holders of the document have specific rights defined in Art. 5 of the Regulation.[220] In particular, the document holders have the right “to verify the personal data contained in it […] and, where appropriate, to ask for its rectification or erasure”. The biometric features in the document may only be used to verify the “authenticity of the document” and “the identity of the holder by means of directly available comparable features”.

2.2.3.3 Driving Licences with Microchip

A national driving license is introduced in the European Union on the basis of the Driving License Directive.[221] Optionally, Member States may introduce a microchip containing harmonized data as part of the driving license. Biometric data relating to fingerprint or iris are additional data groups for these licenses.[222] The inclusion of these data groups is at the choice of each EU Member State.

2.2.4 EU Policies on Artificial Intelligence and Potential Future Requirements on Processing of Biometric Data

Biometric data is involved in artificial intelligence. For the purposes of this publication, we use the following definition of artificial intelligence. “Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals.”[223]

[219] Council Regulation (EU) No 1417/2013 of 17 December 2013 laying down the form of the laissez-passer issued by the European Union.

[220] Ibid.

[221] Directive 2006/126/EC of the European Parliament and of the Council of 20 December 2006 on driving licences (Recast) (Text with EEA relevance).

[222] Commission Regulation (EU) No 383/2012 of 4 May 2012 laying down technical requirements with regard to driving licences which include a storage medium (microchip) (Text with EEA relevance).

[223] EUROPEAN COMMISSION. Communication from The Commission to the European Parliament, The European Council, The Council, The European Economic and Social Committee and the Committee of the Regions. Artificial Intelligence for Europe. In: *European Commission* [online]. 25. 4. 2018 [2019-10-19]. Available at: <https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe>. See p. 2.

For instance, the facial recognition systems make use of artificial intelligence in order to identify the individual and subsequently to assure security by analysing his/her behaviour.[224] The artificial intelligence could be also used for identification in the basis of voice record and emotion analysis. This use of artificial intelligence is conceivable for example in a bank – client relation.

In April 2018, the European Commission issued a communication Building Trust in Human-Centric Artificial Intelligence.[225] In its communication the European Commission declares that "the ethical dimension of AI is not a luxury feature or an add-on: it needs to be an integral part of AI development. By striving towards human-centric AI based on trust, we safeguard the respect for our core societal values and carve out a distinctive trademark for Europe and its industry as a leader in cutting-edge AI that can be trusted throughout the world."[226] Since the AI cause concerns about opacity, unexplainably or lack of ethics, the High-Level Expert Group on Artificial Intelligence set up by the European Commission issued the Ethics Guidelines for Trustworthy AI.[227] Concerning AI and biometric data, the guidelines mentions face recognition technology and involuntary methods of identification as a critical concerns raised by AI.[228]

In according to the guidelines, the trustworthy AI has three components: lawfulness, ethicity and robustness. The ethical principles of the trustworthiness, respect for human autonomy, prevention of harm, fairness and explicability. Developers and deployers as well as end-users and the broader society have to meet certain requirements to ensure the trustworthy AI. These requirements are i.e. human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination and fairness, societal and environmental wellbeing and accountability. "To implement the above requirements, both technical and non-technical methods can be employed. These encompass all stages of an AI system's life cycle."[229] The guidelines offers a non-exhaustive trustworthy AI assessment list for developers and deployers of AI system.[230]

The requirement of transparency and the rationale behind decisions made AI is laid down in Civil Law Rules on Robotics adopted by the European Parliament.[231] Besides the transparency, the European Parliament stresses the importance of lawful data processing and safety and security of technology of robotics.

[224] KITE-POWELL, J. Making Facial Recognition Smarter With Artificial Intelligence. In: *Forbes* [online]. 30. 9. 2018 [2019-10-19]. Available at: <https://www.forbes.com/sites/jenniferhicks/2018/09/30/making-facial-recognition-smarter-with-artificial-intelligence/#66442807c8f1>.

[225] EUROPEAN COMMISSION. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Building Trust in Human-Centric Artificial Intelligence. In: *European Commission* [online]. 8. 4. 2019 [2019-10-19]. Available at: <https://ec.europa.eu/digital-single-market/en/news/communication-building-trust-human-centric-artificial-intelligence>.

[226] Ibid., p. 9.

[227] High-Level Expert Group on Artificial Intelligence. Ethics Guidelines for Trustworthy AI. In: *European Commission* [online]. 8. 4. 2019 [2019-10-19]. Available at: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>.

[228] Ibid., p. 33.

[229] Ibid., p. 20.

[230] Ibid., p. 31.

[231] EUROPEAN PARLIAMENT. Civil Law Rules on Robotics. In: *European Parliament* [online]. 16. 2. 2017 [2019-10-20]. Available at: <http://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.pdf>.

3. Czech Legislation on Biometrics

3.1 Social and Constitutional Aspects of the Biometrics

3.1.1 Introduction

There are only few law domains typical of a high level of dynamics and, at the same time, relative stability, with a strong element of discontinuity. The technological development and globalization are indisputable synonyms of today. Despite a relatively short period of their existence, they bring about economic and social changes. The speed of the development of technologies has an exponential character. It is assumed that over the upcoming twenty years, automation, robotisation, artificial intelligence, and other technologies will be introduced in the manufacture and services and in the method of their management. Experts' opinions differ as to how fast these changes will occur and how essential they will be.

In any case, according to the experts, technological progress is a big opportunity to increase the efficiency of manufacture and services and facilitate work. The work procedures, forms and conditions and the requirements for workers' knowledge and skills are about to change. New technologies should lead, in particular, to replacing routine activities that can be algorithmised. According to the OECD's estimates, about one tenth of jobs in the Czech Republic will be jeopardized by the automation in the course of the next 10–20 years, which would constitute a decrease in the number of jobs by more than 400 thousand.[232] However, new jobs, mainly in services, are expected to be created. In relation to these changes, the experts speak about the need for strengthening the key competencies of people and preparing both existing and new generations for the upcoming changes and the different reality of work and their personal life. It is obvious that the changes will affect personal data and privacy, as well as other fundamental rights.

The current technologies frequently employ, or are directly based on, the processing of personal and other data. The quick pace of technological changes and the globalization have changed from scratch the extent and method of collecting, using and transferring personal information and the access to it. Data is also used extensively in business and public administration. Oftentimes, it is collected without knowledge or consent of the affected persons. If bulky data does not contain personal information, has been anonymized, encoded or at least pseudonymized, it does not need to constitute any or any major risks in terms of privacy and personal data. However, most currently generated data includes personal data, and extensive data files increase a risk to privacy and personal data protection. Data leakages often take place, which the affected subjects do not even find out. The risks relate, in particular, to special categories of personal data. There are also technologies making use of

[232] Průmysl 4.0 významně ovlivní budoucnost profesí, změny čekají i vzdělávací systém. In: *EkonTech.cz* [online]. 25. 5. 2018 [2019-12-15]. Available at: <https://www.ekontech.cz/clanek/prumysl-40-vyznamne-ovlivni-budoucnost-profesi-zmeny-cekaji-vzdelavaci-system>.

biometric data directly for personal identification, such as the use of fingerprints or face recognition. Even in these cases, personal data is collected, so legitimate privacy and personal data protection issues arise. The law should be prepared for these changes.

The tool that covers serious issues of the relationship between technological development and personal data protection or sets the criteria for assessing the extent of a reasonable intervention in privacy is, in particular, the GDPR or, possibly, other related regulations.[233] In this context, it seems indispensable to examine new technologies in the sphere of biometrics and to consider the specific consequences of their impact on privacy and family life. For biometric data processing purposes, the GDPR requires a significantly higher standard of protection than the previous legislation, i.e. the DPD, since it classifies biometric data as special categories of personal data, i.e. data subject to a specific legal regime. Along with the GDPR, many other related regulations have been adopted, such as the Data Protection Directive for Police and Criminal Justice Authorities and the Directive concerning the use of name record of air passengers (the so-called PNR).[234]

The GDPR newly applies directly in all Member States of the European Union. It has a stronger legal force than a domestic regulation. Hence, if these regulations contradicted each other, e.g. if the Czech law stipulated that the security of personal data in a certain sector can be less strict than as pursuant to the GDPR, the European regulation would take priority. Even this fact is, of course, associated with a number of other issues concerning the future trust in the Czech law since certain aspects of some methods of processing data in a given sector are subject to special legislation at the statutory level.[235] However, the GDPR contains a section related to the position and competencies of the supervisory authority and certain procedural aspects of its procedure, which are not specific enough to fully replace the supervision-related legislation in the Personal Data Processing Act and in the Czech procedural laws.[236] Likewise, the GDPR orders or allows Member States to regulate certain aspect in more detail.[237] Therefore, in this respect, it is possible to expect probably the most significant amendments in this legislative sphere since its beginning, within the meaning of the position and the implementation of certain competencies of the supervisory body, or possible sector modifications in the processing of personal data where necessary with regard to the GDPR and other Czech laws (such as, as they already stand today, the provisions of Section 5 (5) to (9) of Act No. 480/2004 Coll., on certain information society services, regulating the conditions of targeted marketing operated through postal service operators). For this reason, it will be necessary to identify possible problematic points of the new concept of the Czech legislation, i.e. points where the current regulation is contrary to the GDPR, to adapt the Czech laws to the new legal regime, and to apply a prudent and reasonable concept respecting the key principles of foreseeability of administrative decision-making, legal certainty, and proportionality.

[233] In this context, from the systematic perspective, it is necessary to, at least, moderate the so-called security directive which completes the legal framework of the today's European personal data protection, i.e. the Directive of the European Parliament and of the Council (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[234] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

[235] As an example, it is possible to refer to Act No. 372/2011 Coll., on health services and conditions of their provision (Health Services Act), which specifically regulates the processing of data in medical documentation, or Act No. 262/2006 Coll., the Labour Code, which separately regulates several methods of processing personal data of employees.

[236] Especially Act No. 500/2004 Coll., Code of Administrative Procedure, and Act No. 255/2012 Coll., on inspection (Inspection Code).

[237] For example, Art. 37 (4) of the GDPR allows Member States to extend the obligation to appoint a personal data officer to include other categories of controllers and processers than the ones referred to in the first paragraph of this Article.

3.1.2 An Individual's Biometric Data and Basic Structure of Its Protection

The term 'biometrics' can be understood, with certain reservations, as a technology or system enabling machine (electronic) identification of an individual or the confirmation of a given user's identification. Thus, biometric systems constitute, in essence, recognition systems ensuring the identification or verification (authentication) of certain characteristics (features) of an individual; these are derived either directly from the physiological data, such as fingerprints, facial characteristics, irises, retinas, hand (finger or palm) geometry, geometry of bloodstream, iris and face, body smell, etc. or from an individual's behaviour where we speak about the so-called behavioural data, such as voice characteristics, handwriting, signature, dynamics of keyboard writing, and others. Therefore, the key concept here is identification on the basis of biometric characteristics of a human body, including specific or presumed characteristics of its manifestations (the so-called behavioural characteristics), where we distinguish between an individual's physical appearance and social behaviour and what specific roles he or she performs (profile). It is an approach to identifying individuals based on their physical, biological, genetic, behavioural, or other similar characteristics where, depending on the time, it is necessary to consider an inexhaustible number of related characteristics (i.e. partial elements or significant indications and the specific features of such characteristics). For the purposes of such identification, several methods, procedures, and algorithms can be used, including related categorization and indexation elements that can simply be referred to as biometric systems.

In this respect, biometric systems serve two main purposes: identification of individuals on the one hand and their verification (authentication) on the other.[238] The term 'biometric data' can be understood as a basic building unit of biometric system of its kind. No legal definition of biometric data is contained in the Czech law as such. It can be found in the GDPR.[239] The previous DPD did not recognize the concept of biometric data either. As the interpretational rule in this respect, the definition formulated by the WP29 was used.[240]

Biometric data is unique and usually represents physiological (physical or behavioural) characteristics through which individuals differ from one another. The key factor here is, in particular, the possibility of identifying individuals, with an extremely high level of reliability, based on their physical, biological or genetic characteristics.

Of course, an individual can also be identified based on numerous other (standard), though oftentimes similar, criteria, for example, based on his/her physical appearance, social behaviour, or interaction with people around him or her or based on how he or she is referred to by others (by surname, name, a nickname) in his or her family or work environment (where he or she holds a certain position / performs a particular role) and among his or her friends. An individual can also be identified based on what he or she owns, knows, does, etc. From the medical and criminalistics perspectives, an individual is also identifiable by means of certain illnesses, injuries and medical interventions suffered and their consequences (teeth condition, types of fractures, medical interventions leaving typical and irremovable traces – implant bones, joints, vessels, etc. or surgical introduction of electronic elements into the body, such as pacemakers, other technical or electronic appliances for improving or substituting original biological functions, post-surgery scars, etc.).[241]

---

[238] For details see Section 1.1 or ARTICLE 29 – DATA PROTECTION WORKING PARTY. *Working document on biometrics*.
[239] See Art. 4 (14) of the GDPR.
[240] See ARTICLE 29 – DATA PROTECTION WORKING PARTY. *Opinion 4/2007 on the concept of personal data*, p. 8.
[241] For more details, see RAK, R. – MATYÁŠ, V. – ŘÍHA, Z. *Biometrie a identita člověka: ve forenzních a komerčních aplikacích*. Praha: Grada, 2008.

Given the identification (verification) potential of this data, biometric data can usually be considered as personal data within the meaning of the applicable legislation, taking into account that this data may constitute a special category of sensitive personal data subject to a special (privileged) legal regime.[242]

In relation to the development of new technologies and their options, it is necessary to remind that the issue of biometric data and the systems related to it represent a highly dynamic industry the commercial potential and the present and future analytical options of which are not good to underestimate. Although any predictions here are extraordinarily problematic, foreign literature[243] considers the so-called second generation of biometrics, or, more precisely, systems enabling personality identification (i.e. profiling) on the basis of the dynamics of an individual's behaviour, as highly problematic, both legally and factually. The thing is that the goal of the systems so designed is not to identify an individual, but rather to "read his or her mind" and predict his or her future behaviour. The second generation of biometric data focuses on the categorization of individuals, and unjustified or unjust selection may result in discrimination where the stigmatization affects individual's future. Hence, a question arises as to what the future technological progress will make possible.[244] With all possible consequences thought through, the indicated goals of the second generation of biometrics would deny the substance of an individual's freedom itself and would create a dangerous priority role of not only the state and its authorities towards individuals but also significant out-of-state groups (economic and others) which an individual could not compete with.

3.1.3 Right to Privacy and its Relation to Other Fundamental Rights in the Context of Protection of Biometric Data

The supporting pillar of any deliberation of this kind is the persuasion of all authors of this monograph about the inalienability, illimitability, and irrepealibility of fundamental rights as relatively complex and delicate cultural structures of advanced human societies, which, without exaggerating, form a single common basis of the legal and political thinking of the today's world. Therefore, the underlying idea of this book is the need to ensure appropriate protection of fundamental human rights and freedoms, in particular, of the fundamental right to human dignity, although sufficient legal protection of biometric data at the level of civil law (see below) cannot be omitted. The main method of examining the relation between biometric data and an individual's fundamental rights and freedoms – as already stated above – is, in particular, the principle of proportionality and its prudent and adequate use.

An attempt at analysing the relation between the right to privacy and other fundamental rights must draw from the general right to protection of privacy since – as obvious in the European area – this right is necessarily affected by the collection, processing and storage of biometric data. This fundamental right to private life is regulated in the Czech Republic mainly in the following laws:

– Charter of Fundamental Rights and Freedoms[245] in Article 7

[242] However, it is necessary to differentiate between biometric data the purpose of which is to verify a user (e.g. verification of an individual solely as a member of a certain group) and biometric systems the purpose of which is to identify an individual based on his or her physiological or behavioural characteristics.

[243] CAMPISI, P. (ed). *Security and Privacy in Biometrics*. 2nd Vol. London: Springer-Verlag, 2013, pp. 405–406.

[244] See, for example, MATEJKA, J. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. Praha: CZ.NIC, 2013.

[245] Czech National Council's Resolution No. 2/1993 Coll., On the Declaration of the Charter of Fundamental Rights and Freedoms as part of the constitutional order of the Czech Republic.

– Convention for the Protection of Human Rights and Fundamental Freedoms[246] in Article 8

– Personal Data Processing Act

– New Civil Code, mainly in Section 81 (2) and Section 86

– Charter of Fundamental Rights of the European Union in Article 7 (solely where the Union law applies)

The biometric data collection, processing and storage intervening in the fundamental right to private life are strongly limited in these laws. The European courts (and also the Constitutional Court of the Czech Republic) carry out a three-tier test assessing whether the restrictions relating to the right to private life are justifiable. They concern the following questions:

a) whether the intervention follows the law; law should be of certain quality and should be available and accurate and have foreseeable consequences; this also applies with regard to the gravity and extent of an intervention in a fundamental right (compare the Finding of the Constitutional Court of 22 March 2011, ref. number Pl. ÚS 24/10);
b) whether the intervention has pursued a legitimate goal (e.g. protection of public safety, life, health, third-party property);
c) whether the intervention has been indispensable in a democratic society (i.e. whether there has been an urgent social need for such an intervention);

The last prerequisite requires an analysis by means of the proportionality test. It consists in the following criteria:

a) criterion of appropriateness of an intervention for achieving a particular goal;
b) criterion of necessity of an intervention compared to other (less restrictive) measures enabling the achievement of a particular goal; and
c) criterion of proportionality in the narrower sense of the word, i.e. consideration of whether the extent (sense) of an intervention is sufficiently serious to outweigh an individual's interest in the protection of his or her fundamental human right (for more compare point 4 below).

The fundamental right to private life includes, among other things, the right to informational self-determination; in essence, an individual has the right to determine which details of his or her private life to disclose to other entities. In this respect, it is possible to refer, for example, to the Finding of the Constitutional Court of 17 July 2007, file number IV. ÚS 23/05, and of 1 December 2008, file number I. ÚS 705/06, and the Decision of the Federal Constitutional Court of Germany BVerfg GE 65 where the German Constitutional Court drew, among other things, from the judicature of the European Court of Human Rights, in particular, from the case *Malone vs. United Kingdom* (Judgment No. 8691/79 of 2 August 1984), which inferred the right to informational self-determination from Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms.

The essential significance of the protection of the fundamental right to private life was also stressed in the Judgment of the Supreme Administrative Court of 28 June 2013, file number 5 As 1/2011 – 156. It stated, among other things, the following: "For the protection of another fundamental right or freedom to prevail over the protection of privacy, the situation must be such that otherwise equal fundamental rights and freedoms are in conflict and it must be thoroughly considered whether

[246] European Convention on Human Rights. In: *Council of Europe* [online]. [2019-12-14]. Available at: <https://www.echr.coe.int/Documents/Convention_ENG.pdf>.

in the particular situation the interest protected by another fundamental right and freedom is serious and jeopardized enough to allow intervention in privacy and, therefore, partial or complete limitation of the fundamental human right to privacy or private and family life and, hence, to human dignity."[247]

At the general level, it can be stated that the fundamental right to private life (compare, particularly, Article 7 of the Charter of Fundamental Rights and Freedoms and Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms) is of such a wide impact that it often overlaps other fundamental rights regulated in other Articles of the Charter, the Convention, and international pacts. According to recognized literature, "In most situations, the Court [understand the European Court of Human Rights] then examines the case against a more specific Article rather than against Article 8 [of the Convention] which is general in this regard".[248] The relation of the fundamental rights referred to below, if affected by the collection, processing and storage of personal (including biometric) data, is then obvious.

What fundamental rights overlap most frequently or may overlap the fundamental right to private life? They are, in particular:

a) fundamental right to human dignity,[249] personal honour and good reputation (can also be included under the fundamental right to private life in a broader sense)

The thing is that 'human dignity' alone may be affected by the collection, processing and storage of biometric data, for example, during thorough personal searches and controls, in particular, at airports; this will also relate to other fundamental rights stated below. Let's leave aside that by far not every check of this type constitutes an inadmissible violation of the given fundamental right (Article 7 of the Charter and Article 8 of the Convention) since the public interest or the protection of third-party rights and freedoms oftentimes prevails. When it comes to the protection of good reputation, it is categorized under the concept of private life even by the European Court of Human Rights (compare *Pfeifer vs. Austria*, Judgment No. 12556/03 of 15 November 2007). Controls carried out at airports by state authorities or other comparable controls are often associated with the collection of biometric data, for example, in the form of fingerprints or in other, more invasive forms (compare the European Court of Human Rights, *S. and Marper vs. United Kingdom*, Judgment No. 30562/04 of 4 December 2008).[250]

b) fundamental right to the protection of personal data

Even this fundamental right undoubtedly affects an individual's private life. When it comes to biometric data, it is collected or processed, for example, already in the issuance of personal or travel documents or their check (fingerprints, photos, etc.). The storage of personal data is then incorporated in the protection of private life even by the European Court of Human Rights (compare *Amanna vs. Switzerland*, Judgment No. 27798/95 of 16 February 2000).

[247] In the given case, the matter related to the admission of a camera system for protecting the safety of people and property of the property owner and hotel guests, to the check of accesses to the property, and to the prevention of vandalism.

[248] Cf. KMEC, J. – KOSAŘ, D. – KRATOCHVÍL, J. – BOBEK, M. *Evropská úmluva o lidských právech. Komentář.* Praha: C. H. Beck, 2012, p. 866.

[249] See CAMPISI, p. (ed). *Security and Privacy in Biometrics*, p. 393: The report of the Council of Europe refers to the integrity of human body as to an aspect of human dignity; the 'use of your body' as an identification tool may encroach on what we call our information privacy. However, the publication infers that biometrics is "in its nappies" and there is only little knowledge of its possible drawbacks; hence, a development of unpredictable consequences may be started up.

[250] Cf. KMEC, J. – KOSAŘ, D. – KRATOCHVÍL, J. – BOBEK, M. *Evropská úmluva o lidských právech. Komentář*, p. 871, 884.

c) fundamental right to personal freedom (e.g. in the arrest of a suspect)

This fundamental right may, in comparable cases, also be affected. It may, for example, be a short-term detention for verifying a passenger's identity or a long-term detention of immigrants by the authorities of the given state. Controls by means of biometric data, especially in countries endangered by a flow of immigrants, suggest themselves. It is possible to mention, for example, the stopping of a passenger at a national border within the Schengen area without stating a reason. Here, however, it is not possible to overlook the current condition where the states have found themselves in the centre of a new phenomenon and are trying to face the immigration wave through means that would hardly be thinkable a short time back. The calling for breaking through the Schengen system or modifying it newly is being very loud in Europe.

d) fundamental right to the freedom of movement

e) fundamental right to the inviolability of home (house freedom)

Even this right is undoubtedly related to the fundamental right to private life and usually affects the protection of biometric data of a particular individual; for example, the collection of fingerprints is a common phenomenon in a house search. In this respect, it is appropriate to refer to the Decision of the European Court of Human Rights in the case *S. and Marper vs. United Kingdom*[251] where the Court speaks about the danger of stigmatization (in particular, in adolescents) in relation to the collection of DNA. The storage of DNA without a time limitation may, thoroughly taken, affect the presumption of innocence. A similar effect could have resulted from the proposal of the French Government in 2004 for registering biometric data of foreigners whose visas have been denied; this case may, however, seem disputable.

f) fundamental right to the privacy of correspondence and to the privacy of other written documents, records and other messages

This concerns, in essence, the communication operation, including the so-called e-mails, etc. (see, for example, the Judgment of the European Court of Human Rights No. 62617/00 of 3 April 2007 in the case *Coplad vs. United Kingdom* or the Judgment of the Constitutional Court of the Czech Republic No. Pl. ÚS 24/10 of 22 March 2011, point 32). A specific action is the recording of voice, which also indisputably amounts to biometric data (compare the Judgment of the European Court of Human Rights No. 44787/98 of 25 September 2001 in the case *p. G. and J. H. vs. United Kingdom*).

g) fundamental right to the freedom of thinking, conscience and religious belief

This right has recently been a significant issue in Europe, in particular, in connection to the flow of (oftentimes illegal) immigrants from Muslim countries. After all, many such individuals had lived in some European states before the recent immigration wave began (United Kingdom, France or Germany). The states more or less defend themselves and refer to both the public interest and the necessity of the protection of third-party rights and freedoms, in particular those of their own citizens. In this respect, it is appropriate to mention the problems relating to the so-called covered Muslim women, whether they use burqa, niqab, chador, hijab or Shayla; burqa and niqab prevent, in essence, the optical identification of the person whose body and face are covered. A question arises here as to how to deal with the necessary collection (processing) of biometric data through an automated recognition of facial characteristics (the so-called facial recognition), whether for public purposes (a check of personal documents and verification of identity) or private purposes (e.g. access to a company's building). At present, it is a question of the legislation of the respective state.

[251] Ibid, p. 916.

h) In a broader sense of the word, this group also comprises the fundamental right to the prohibition of discrimination.

The protection of biometric data – if it is part of the right to the protection of personal data – and the protection of the fundamental right to private life are associated, as a possible antipode, with the constitutional right to the freedom of speech and the right to information (Article 17 of the Charter of Fundamental Rights and Freedoms). However, rather than strictly contradicting each other, the fundamental right to private life and the fundamental right to information co-exist. Even here it is necessary to draw from the circumstances of a particular case and to measure through the proportionality test whether the protection of a particular fundamental right prevails in the particular case (compare the Finding of the Constitutional Court published under number 405/2002 Coll.).

A possible limitation of fundamental rights in the form of collection, processing and storage of biometric data requires the existence of appropriate security guarantees ensuring that personal data (biometric data here) is effectively protected from incorrect use and misuse. It is necessary, among other things, that biometric data is used in a form allowing the identification of a subject for the purpose for which it is stored and for a period not longer than as required to achieve the given purpose.

Legal guarantees require that the national law prevents the use of personal data which could be inconsistent with the guarantees provided in Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms. The national law must ensure that the collection and the storage of personal data are relevant rather than excessive in relation to the purpose for which the personal data is stored and that their form allows the identification of a personal data subject for a period not longer than as required to achieve the purpose for which the personal data is stored. The stated postulates were expressed by the European Court of Human Rights already in the mentioned case *S. and Marper vs. United Kingdom*; however, in this respect, it is also possible to refer to other cases heard by the European Court of Human Rights, such as the case *Leander vs. Sweden*, Judgment No. 9248181 of 26 March 1987, the case *Turek vs. Slovakia*, Judgment No. 57986/00 of 14 February 2006, or the case *Gardel vs. France*, Judgment of 17 December 2009, Application No. 16428/05.

The common elements (features) of guarantees are identified by a significant Oxford study[252] as follows:

a) Specification of the purpose: data must be collected for a specified, explicit and legitimate purpose

b) Quality of data: collected data should be relevant and necessary to achieve the legitimate purposes for which it is collected

c) Collection of data: data should be provided with the consent or knowledge of data subjects

d) Notices: data subjects should be informed of the purposes for which their data is collected, of the office allowing the collection of data, of whether the disclosure is mandatory or voluntary, and of the consequences of the failure to provide it

e) Limitation of use: data should be used for originally specified purposes or for purposes compatible with original purposes; restrictions also apply to the transfer of data among state authorities and between the state and private organizations or individuals

[252] See ERDOS, D. et al. Biometric Identification and Privacy. In: *Oxford Human Rights Hub* [online]. 2013 [2019-07-15]. Available at: <http://ohrh.law.ox.ac.uk/wordpress/wp-content/uploads/2018/02/4.-Indian-Biometric-Identification-and-Privacy.pdf>. The summary part of this report titled as 'Safeguards for the Protection of Biometric Data' recognizes legal guarantees, common elements (features) of guarantees (i.e. in multiple states), and challenges to biometric identification schemes.

f) Security: appropriate security measures ensuring the security, integrity and confidentiality of personal data should be in place

g) Access: data subjects should have the right of access to their personal data contained in databases

h) Correction: data subjects should have the right to update and correct their data

i) Independent data protection office: all jurisdictions in the study secures for independent data protection offices the right to monitor compliance with data confidentiality guarantees and the right to investigate and hear complaints

Regarding the issue of current challenges of biometric systems, the Oxford study[253] referred to three legal cases. It first examined the already cited case *S. and Marper* (European Court of Human Rights) and then the case *Nahon vs. Knesset* (Supreme Court of Israel). Although the Supreme Court rejected the application for its prematurity, judges criticised the matter and considered whether it was really necessary to store biometric data of the entire Israeli population in a single centralized database; they concerned fingerprints and computerized facial details. The third case was heard by the Constitutional Board of France; they also concerned fingerprints and facial details as parts of the national database serving to prevent thefts of identity. However, in the opinion of the Constitutional Board, it was an intervention which disproportionately limited the data subject's right to private life.

Biometric data and its collection, processing and storage do limit the fundamental right to private life (or, possibly, other fundamental rights), but also serve or may serve to protect other fundamental rights – in particular, in relation to third parties. They concern, in particular:

a) fundamental right to life;
b) fundamental right to own property; and
c) other fundamental rights referred to above, which, on the one hand, are limited in a particular person but, on the other, and as already stated, are (may be) protected in relation to third parties (e.g. the fundamental right to private life or human dignity and other fundamental rights referred to above)

When it comes to biometric data serving to protect third-party fundamental rights, it cannot be overlooked that public interest may also be affected in certain cases. However, public interest is a broader concept comprising, in particular, the protection of national security and public security, the protection of economic well-being of the country, the prevention of disorder and crime, the protection of health and morals, etc. (compare, for example, Article 8 (2) of the Convention for the Protection of Human Rights and Fundamental Freedoms[254]). These are not fundamental rights (state has no fundamental rights) but values that need to be reflected on within the proportionality test and where it is necessary to consider whether an interest in the protection of a certain fundamental right of a particular person (e.g. the right to private life) outweighs the attributes fulfilling the public interest in comparison to such a fundamental right. It is, however, always necessary to draw from the circumstances of a particular case as there is no general manual available.[255]

[253] Ibid., specifically, in the part titled as 'Challenges to Biometric Identification Schemes'.
[254] European Convention on Human Rights. In: *Council of Europe* [online]. [2019-12-14]. Available at: <https://www.echr.coe.int/Documents/Convention_ENG.pdf>.
[255] As an example, it is possible to state the massive controls of passengers and their personal searches at many airports; they are often the collection and processing of their biometric data and an intervention in their private life and other fundamental rights referred to above (for example, in the right to human dignity).

3.1.4 Risks Related to Processing Biometric Data and their Categorization

Some of the risks (referred to below) may be of not only a legal but also technical or social nature; sometimes it is *promiscue*, not easy to separate.

First of all, it needs to be emphasized again that biometric data is very vulnerable as a consequence of its specific nature since it is unique, permanent and universal. For this reason, it is necessary to ensure a data control enabling the identification of possible risks and to adopt security measures drawing, among other things, from the proportionality test. The proportionality test is aimed at finding the appropriate security data level enabling the assessment of risks associated with the processing of the specific type of data and with the introduction of specific measures corresponding to the degrees of vulnerability of this data. This, however, gives rise to a problem since the Czech legislation lacks a consistent approach to biometric data; in other words, legal uncertainty, that is, not completely clear legal state, exists in the Czech Republic in the matter of processing of biometric data, which results in the social need for revising the complicated and rigid approach to biometric data which often constitutes sensitive data.

The risk of collecting, processing and storing biometric data means, in essence, a possibility of biometric data being misused. This applies, in particular, to the fundamental right to private life, which is usually the most serious risk. However, the misuse of biometric data may also relate to other fundamental rights as they are stated in the previous text. In this respect, identity thefts, blackmail, destruction of personal reputation, or an attack at human dignity are usually referred to as classical examples. This may lead to harm of a personal or financial nature. Nevertheless, an essential problem seems to be, sometimes optically, sometimes actually, the conflict among the below fundamental rights (in particular, the right to private life) on the one side and third-party fundamental rights or the public interest on the other.

Given the risks associated with biometric data in general – in the attempt at minimizing their impact, it is not possible to avoid the existing statutory instruments aimed at the given goal. These include, in particular, the special obligations resulting from the GDPR since biometric data is usually considered as personal data. Hence, the stated obligations assume that the controller must create the necessary guarantees in personnel and technical spheres (e.g. security of the place of processing of biometric data) and – in the narrower sense – in the sphere of use of computer technology in general. The thing is that the system may be hacked or used by unauthorized persons or for other purposes than for which it is intended. It is, therefore, obvious that the assessment of risks associated with the processing of personal data is an issue of evaluation of a particular situation by the respective controller or processor, in particular, an issue of the employed or set means and method of processing personal data, the type and extent of this data, and, for example, the specifics or location of the processing or the building where the processing takes place.

There are many methods of processing biometric data; however, absolute majority of them are associated with the need for storing sensitive personal data, in particular, such data which people commonly and intentionally conceal from others (usually fingerprints, retina or iris picture, etc.).[256] This leads to real risks of misuse of such data towards its originators (biometric falsification for unauthorized access, production of falsified evidence for courts, access to sensitive medical details, etc.). For this reason, certain systems do not store in their databases any visual patterns of individual

[256] For more see, for example, ŠČUREK, R. Biometrické metody identifikace osob v bezpečnostní praxi. Studijní text. In: *Rucnepsanypodpis.cz* [online]. 2008 [2019-12-15]. Available at: <http://www.rucnepsanypodpis.cz/PDF/biometricke_metody.pdf>.

users, but only the measured distances of their facial characteristics (they usually concern the characteristic parts of face – mouth edges, eye ends, etc.). In the event of a possible attack of the system, the attacker (hacker) does not obtain access to photos but only to a matrix of numerical data. However, even this data needs to be considered as biometric within the meaning of its statutory regime (it is sensitive personal data). In this respect, it is necessary to refuse the opinions of professional literature[257] that this data is not subject to the statutory regulation resulting from the specific regime of sensitive personal data.

The risks of misuse of biometric data may be eliminated in cases identified as the so-called statutory licence as referred to in Sections 88 and 89 of the new Civil Code which stipulate in detail the cases where no consent, for example, to an intervention in private life, is necessary. However, in this respect, it is not possible to overlook the exception from statutory licence stipulated in Section 90 of the new Civil Code, which stipulates that no statutory reason for intervening in private life or using an individual's photo, written documents of a personal nature, or audio or visual records must be used inappropriately and contrary to the individual's legitimate interests. Therefore, the cited provision needs to be applied very carefully and it is always necessary to consider the circumstances of a particular case appropriately.

The following remarks need to be stated in relation to certain special cases of working with biometric data:

– Fingerprints belong among highly specific biometric data since they are easy to transfer and their falsification cannot be completely excluded; they concern, for example, the transmission of a fingerprint from glass and the creation of a similar print in a wax on the relevant medium.

– The existence of the so-called blacklists of troublemakers (e.g. in shops or restaurants) is problematic because it does not seem proportional to record all customers to eliminate only some of them (e.g. processing of facial characteristics or fingerprints for the purpose of excluding a certain customer from further contracting, etc.).

– A completely specific is the risk of using biometric data towards possible discrimination where individuals not able to use the biometric system, for example, owing to their mental or physical defects, are excluded.

Hard to categorize are risks associated with the so-called second generation of biometric data which is a rather pro future deliberation. The thing is that it aims at identifying individuals on the basis of their behaviour. The goal of this may be the attempt at 'reading a human mind', which, however, may lead – as already stated above – to the stigmatization, the categorization of people, the deindividualization, and, thus, discrimination (as an example – the categorization of people may cause that people may be approached on the street or examined in a check at borders just because they fall within a certain 'categorized' profile). In this respect, it is, however, necessary to point out that ethical requirements relating to these risks must be respected – not only in the biometric data of the second generation – from the very beginning of work with biometric data.

Hence, it is obvious that there is a 'considerable tension between the processing of biometric data of the second generation and the principle of an individual's participation in this process'[258]; it is not easy to minimize the general risk of the system being used by other persons and for other than foreseeable purposes without a traditional option of individual participation.

[257] See, for example, VALER, T. Biometrie obličeje pro autentizaci osob. *Data Security Management*. 2014, Vol. XVIII, No. 2, p. 19.
[258] Cf. CAMPISI, P. (ed). *Security and Privacy in Biometrics*, p. 406, 407.

The assessment of risks resulting from statutory obligations (e.g. border controls), both overall and individually, is very difficult. First of all, it needs to be stated that the systems and work with them are not fully developed yet, which may also affect the examination of proportionality between work with biometric data on the one side and the intervention in the fundamental right to private life or another fundamental right on the other. In essence, biometric data only represents a certain degree of probability and, hence, no results of the work with them can be absolutized. As already stated above, biometric data is unique, permanent and highly vulnerable. This is supported by the legal uncertainty in the sphere of work with biometric data since the legal rules are not clear enough.

Assessing the risks associated with biometric data more closely and considering the necessary guarantees, it is appropriate to refer, for example, to the resolution of the 27th International Conference for Data and Privacy Protection held in 2005[259]. The conference pleaded, among other things, strict distinction between biometric data collected and stored for public purposes (e.g. border controls) on the basis of a statutory obligation and for contractual purposes on the basis of a consent; the extent and gravity of the risk in terms of the public interest seem obvious.

Another aspect comes into play and enables the assessment of risk of the particular biometric data that is to be used. It is the choice between biometric data leaving tracks (e.g. DNA samples, fingerprints) and biometric data that does not do so (e.g. iris). The risk of intervention in the private life is considerably smaller here. However, it is always a matter of a particular case which biometric data can be used as adequate at all. A completely specific biometric data is then the human face (or, more precisely, the geometry of face itself) which is of the nature of public information and, therefore, the accidental or occasional recognition of which does not, obviously, bear any risk inducing possible misuse of personal identifiers against a particular person. However, a completely different situation is the one when such recognition is carried out in an automated way through sophisticated technology for the purpose of the further indexation and cataloguing of human data although the potential rate of the total effects of the data so processed is not and, with regard to the current development, cannot even be, known at the time of such processing.[260]

Naturally, special attention needs to be paid to biometric data which is strongly invasive and disturbing by nature because it brings information, for example, on an individual's health condition or racial or ethnical origin.

[259] Ibid, p. 399.

[260] An example of a sophisticated device for scanning the geometry of face is, for example, technology Broadway 3D of the Russian company Artec. According to the manufacturer, it is the first device capable of identifying an individual at a speed comparable to how people recognize each other (about one second). The device consists of two parts – a reader (camera) and a computer unit. If the camera detects a person passing by, the reader starts projecting a clearly defined pattern on the face at quick intervals. Then it records the points of the projected patterns in the person passing by and the computer unit determines the change of their location depending on the time, which results in identification. The manufacturer's special algorithms can detect the absence of subtle mimics in the face and carry out the identification based on that. There are also many software tools on the market enabling the use of common cameras for 3D authentication. For more information, see VALER, T. *Biometrie obličeje pro autentizaci osob*, p. 18.

3.1.5 Social Specifics of Using Biometrics in the Czech Republic – results of statistical research titled 'Biometrics and its Use from the Perspective of the Czechs'

The Public Opinion Research Centre of the Institute of Sociology of the Academy of Sciences of the Czech Republic (acronym "CVVM") carried out in September 2018, on the initiative and order of the research team of the project referred to above (GA ČR No. 16-26910S), research with working title 'Biometrics and its Use from the Perspective of the Czechs'. The research itself took place between 8 and 20 September 2018 and was carried out methodologically in the form of personal interviews between an interviewer and a respondent[261] on a sample of Czech people over 15 years of age; 1230 people were approached, of whom 1037 were interviewed.[262] This representative group of respondents was asked questions focused on the issue of biometrics and its more and more frequent use in various departments, in particular, information technologies. The research dealt specifically with whether and how much the Czechs were aware of what biometric data was, whether they knew that this data was often recorded, registered, processed and used by means of various technologies and applications in an automated way and independent of individuals' consents, and whether, in relation to the use of biometric data, the people preferred user convenience to the protection of their privacy, which biometrics-based technologies undoubtedly violate. The end of the interview contained questions relating to the phenomena associated with the monitoring and use of biometric data in common life.

At first, the respondents were asked about their awareness of biometric data, whether they had already heard of this concept and knew what it meant. The results show that approximately seven out of ten people over 15 years of age (71 %) at least heard of biometric data and that almost a half of them (47 %) had, according to them, at least an approximate idea of what biometric data was. A more detailed analysis showed that more men than women – people between 30 and 44 years of age, with the highest level of completed education, with a favourable evaluation of the living standard of their household and Internet users – declared their awareness of biometric data. A higher awareness of biometric data was also expressed by people in towns with more than 80 thousand inhabitants and in Prague. In terms of employment, a higher awareness of biometric data was shown by highly qualified professional or leading workers.

Another question explored whether the people knew that modern technologies enabled the collection, processing and use in various ways a large amount of data on every individual, both with his or her knowledge and consent and absolutely independent of him or her. The research showed that 70 % of the people knew that modern technologies enabled such processing and that 30 % did not know that. The share of those who had this knowledge corresponded, in essence, to the knowledge of what biometric data was. The sociodemographic differences in the answers to the given question did not differ much from the differences recorded in the first question examining the concept of biometric data.

Subsequently, the respondents were asked whether, in using various technologies, they preferred user convenience at the expense of their personal data being used or whether they preferred the protection of their privacy at the expense of certain user inconvenience or, possibly, a limitation of certain services tailored to individual users. The results referred to the fact that, in the Czech

[261] The combination of PAPI (71 %) and CAPI (29 %) interviews was chosen for the form of this interview; the research tool was then a standardized questionnaire with 60 variables.

[262] ČERVENKA, J. *Biometrika a její využívání z pohledu české veřejnosti*. Research report. Centrum pro výzkum veřejného mínění, Sociologický ústav AV ČR, v. v. i., 2018.

population over 15 years of age, there were more of those (three to one) preferring the protection of their privacy to the maximum user convenience which modern technologies might possibly offer with the use of personal data. The opinion that it was important that the used technologies provided maximum user convenience and customized services even despite of the information available on their person being used was expressed by approximately one fifth (21 %) of the respondents, while the share of those preferring the protection of their privacy despite compromised convenience and despite the limitation of customized services exceeded three fifths (63 %). About one sixth (16 %) of the respondents were not able to decide. A statistically significant difference in the preferences of user convenience at the expense of the share of those who could not decide could be noticed between Bohemia and Moravia where user convenience was preferred by 24 % of the respondents, with 13 % of those who could not decide, in Bohemia and by only 16 % of the respondents, with 20 % of those who could not decide, in Moravia.

A rather interesting difference could be seen in terms of religious belief among the Catholics, who less frequently preferred user convenience (9 %) and, conversely, preferred, to an increased extent, the protection of privacy (72 %), while people without a confession preferred, to an increased extent, user convenience (25 %) less frequently than the average. In terms of the left-wing to right-wing political orientation, similar opinions to the ones of the Catholics were expressed by people categorizing themselves as 'centre-left'. In evaluating the respondents' answers, the PORC interpreted these differences by inferring that one of the differentiating factors for an approach to the given issue might be a value approach on the conservatism – liberalism axis; conservative approaches might combine with the tendency to prefer the protection of privacy and refuse modern technologies based on the use of personal data, while liberal approaches might be inclined, to an increased extent, to accept new technologies with the optimistic view that they were going to cause positive things and prevent misuse or negative impacts, among other things, on privacy.

Other questions focused, in more detail, on some common situations occurring in relation to technologies making use of the collection of data. They concerned the total of nine pairs of statements where the respondents answered questions on the basis of a five-point scale. The prevailing answers were that (1) in the purchase on the Internet customers minded the collection of data on their behaviour and (2) they minded when websites were adapting to their personal preferences. (3) Opinions were quite similar when it came to whether the respondents preferred access passwords and verification codes to an automated identification on the basis of biometric data; the statement preferring automated identification on the basis of biometrics was supported by 29 % of the respondents, while the statement preferring access passwords and verification codes was supported by 31 % of the respondents. (4) In the question about whether customers were, in new services, interested in what data was collected on them, the statement that they were always interested clearly prevailed (42 %). (5) In the question about whether or not, in searching for goods and services on the Internet, the respondents minded stating their personal data capable of leading to their direct identification, the opinions were quite similar. (6) In the pair of statements of whether or not, in purchasing goods and services on the Internet, the respondents minded stating personal data leading to their identification, the most frequent answer was that they did (36 %). (7) In the question about whether a user could or could not influence how the application or website he or she was using collected data on his or her behaviour and preferences, the sceptical option that it could not be influenced slightly prevailed. (8) In the pair of statements of whether technologies predicated on the use of biometric data and data on individuals' behaviour in private and commercial spheres should be prohibited or allowed (because they allowed improving the offer of services), the respondents (two fifths of them) clearly took the side that they should be prohibited. (9) In the last pair of statements relating to an option of safeguarding from the possible leakage and misuse of an individual's data and data on his or her behaviour stored on the Internet and on electronic appliances, the Czechs clearly supported the sceptical option that this could not be safeguarded (46 %).

To sum up, it was the first and exclusive research of the opinion of the people in the Czech Republic on biometrics, focused on the awareness of biometric data, the awareness of the processing of data through modern technologies, and the respondents' preferences in the event of conflict between the protection of privacy and user convenience. It informed on the fact that a majority of the people had knowledge of what biometric technologies and modern technologies in general were, and depicted the prevailing public opinion towards the preference for privacy protection at the expense of user convenience. On top of that, the research referred to the wide range of not only sociodemographic and geographic factors but also to other facts allowing differentiating the public's attitudes more sensitively. What can be considered as important are the details of the high number of indecisive answers. The relevance of the implemented research is given, in particular, by the fact that opinions of natural persons, for the protection of whom the current data protection laws are intended, were explored. Overall, the conclusions of the research can be summed up as follows:

- About seven people out of ten (71 %) over 15 years of age had at least heard of biometric data and almost a half of the respondents (47 %) had at least an approximate idea of what biometric data was.

- 70 % of the respondents knew that modern technologies enabled the collection, processing and use of data on every individual, even without his or her knowledge and consent.

- In the Czech population (three to one), those people prevailed who preferred the protection of their privacy to the maximum user convenience offered by modern technologies with the use of personal data.

The conclusions referred to above show that the currency of, and the need for, a simultaneous increased standard of protection of personal data and privacy of natural persons were indirectly confirmed.

3.1.6 Solutions in Constitutional and Human Rights Spheres

A solution at the constitutional level exists. For several years, the Constitutional Court of the Czech Republic has been accentuating the constitutional significance of international commitments, in particular, of the proclaimed and ratified international agreements (treaties) within the meaning of Article 10 of the Constitution. In this respect, it is possible to rely, in particular, on Article 1 (2) of the Constitution pursuant to which the Czech Republic shall adhere to the obligations resulting from the international law; therefore, such obligations are, at the same time, of a constitutional nature. Here, it is, for example, possible to refer to the obligations stipulated in the Convention for the Protection of Human Rights and Fundamental Freedoms, the International Covenant on Civil and Political Rights, and the International Covenant on Economic, Social and Cultural Rights, which are agreements pursuant to Article 10 of the Constitution.

From the legal perspective, when it comes to biometric data, the right to protection of personality overlaps with the right to protection of personal data.[263] The thing is that the right to protection of personality works with the concept of expressions of personal nature, which, similarly to the concept of personal data, is closely associated with a particular person. Professional literature is of the opinion that "every expression of personal nature which can be ascribed to a particular person constitutes personal data; nevertheless, personal data may also be information of a different

[263] KUČEROVÁ, A. – NOVÁKOVÁ, L. – FOLDOVÁ, V. – NONNEMANN, F. – POSPÍŠIL, D. *Zákon o ochraně osobních údajů. Komentář.* Praha: C. H. Beck, 2012., p. 47 et seq.

nature, independent of an individual's personality, such as personal identification number or bank account number".[264] The concept of personal data is then broader than the concept of the manifestation of a personal nature; semantically, this concept is connected to the human right concept of an individual's personality[265] or his or her family life. Thus, biometric data is closely related to the concept of protection of personality. An individual's personality then constitutes, in essence, specific characteristics and differences in every individual's nature, appearance and behaviour. It is the natural individuality of a person which is the value protected by the Charter of Fundamental Rights and Freedoms in Article 10[266] and by the provisions of the Civil Code pertaining to the protection of personality (Sections 81–117).[267] The personality of an individual "comprises everything through which an individual expresses himself or herself towards people around him or her from physical, spiritual and mental perspectives".[268]

When it comes to the home right, the fundamental rights to privacy protection and to private life are regulated, in the first place, in the Charter of Fundamental Rights and Freedoms in Article 7 (1) and Article 10 (2), in the new Civil Code, in particular, in Section 81 (2) and Section 86, and also in several provisions of the Data Protection Act. The international law (in a broader sense) anchors the protection of privacy or protection of private life, in particular, in the Convention for the Protection of Human Rights and Fundamental Freedoms in Article 8 (1), in the International Covenant for Civil and Political Rights in Article 17 (1), and, for completeness, in the Charter of Fundamental Rights of the European Union in Article 7 (solely where EU law applies).

Naturally, the fundamental right to protection of privacy (private life) is or may be intervened in through biometric data, i.e. through its collection, processing and storage. An intervention in an individual's privacy must meet the requirement for proportionality (see below). In the judicial practice, whether national (constitutional courts) or European (European Court of Human Rights[269]), it is examined whether an intervention in privacy is violating the relevant provisions pertaining to the protection of the fundamental right to private and family life (breach of Article 8 of the European Convention on Human Rights). As already stated more briefly above, the courts usually use the proportionality test as a standard procedure, which includes the assessment of appropriateness, necessity and comparison of gravity of both colliding fundamental rights (for a more detailed look, see chapter 3.1.3).

Let's get back to the problems experienced in the solution of the existing legal situation (risks) in the field of special legal protection of biometric data. It concerns, in particular (also generally on case-by-case basis), a possible or actual conflict between the public interest, or, possibly, between the individuals' fundamental rights to the protection of life, health, safety and property through the collection, processing and storage of biometric data on the one side and the protection of fundamental rights to personal freedom, human dignity and private life of data subjects (persons under examination) on the other. There are two groups of constitutionally anchored values which conflict each other. The recognized methods of dealing with such a conflict are the proportionality principle and the proportionality test, as already stated elsewhere herein.[270]

---

[264] Ibid.

[265] Hence, the concept of an individual's personality is closely related to the concept of privacy or, more precisely, it overlaps the concept of private and family life. The concept of privacy is then inseparable from an individual's personality and can thus be viewed as a universal value which is granted general protection.

[266] Resolution of the Presidium of the Czech National Council of 16 December 1992 on the declaration of the CHARTER OF FUNDAMENTAL RIGHTS AND FREEDOMS as a part of the constitutional order of the Czech Republic. In: *Ústavní soud* [online]. [2019-12-15]. Available at: <http://www.usoud.cz/fileadmin/user_upload/ustavni_soud_www/prilohy/Listina_English_version.pdf>.

[267] Act No. 89/2012 Coll., the Civil Code, as amended.

[268] Lavický, p. et al. *Občanský zákoník I. Obecná část (§ 1−654). Komentář.* Prague: C. H. Beck, 2014, p. 392.

[269] Judgment of the ECHR of 2 September 2010, Application No. 35623/05, Uzun vs. Germany.

[270] It is possible here to also refer to the Czech constitutional judicature, in particular, to the Judgments of the Constitutional Court No. Pl. ÚS 4/94, Pl. ÚS 15/96, Pl. ÚS 16/98, and Pl. ÚS 40/08.

Considering the existing legal situation, it is not possible to avoid the laws of the Council of Europe and of the European Union (compare the Introduction) which regulate in detail the protection of individual persons although, in Convention No. 108 cited above, it is protection with regard to the automated processing of personal data. In Convention No. 108, it is significant that such processing of the so-called sensitive personal data (disclosing the racial origin, political opinions, religious or other belief, as well as personal data relating to health or sexual life) is linked to the fact that the national legislation sets appropriate guarantees (Article 6 of the cited Convention). However, are these 'appropriate guarantees' actually and effectively anchored in the legislation of the Czech Republic? It is a big question.

In examining the current legal state, it is appropriate to also deal with the aspects of the general law although it is, naturally, necessary to interpret the general (civil) law by means of constitutional principles and vice versa. Constitutional, but also civil, aspects associated with special legal protection of biometric data can also be found in professional literature,[271] which shows that neither *case law* nor the existing legal *framework* provide a clear answer to the questions associated with the use of biometric data. The author stated therein (de Hert) also deals with the argument of human dignity and emphasizes that human dignity should be fully respected during "the collection and processing of physical characteristics". Another author (Niels Christian Juul) draws, in particular, from the recommendation of the Danish Personal Data Protection Office; he states that "privacy impact assessment" (PIA or also the assessment of impact on the protection of personal data) ensures a reasonable balance among the purpose of the system, the possible level of identification, the storage of personal data, and the risk of its misuse and theft. Biometric systems should be used in a way so as to achieve a higher level of privacy and for users to have an option to check their own data.

Considering the solution to the existing situation in the field of special legal protection of biometric data, it is appropriate to reproduce certain crucial questions relating to the statutory aspects of its processing. They include, in particular, the following:

a) Legal uncertainty regarding the processing of biometric data

The Czech legal environment is formed through both the legislation of the European Union and the national law. As for the European Union, it is necessary to refer, in particular, to the GDPR, which, however, has not eliminated all problems; this includes, for example, the uncertainty regarding the exact limits within which biometric data can be recognized, the uncertainty regarding the special criteria in relation to the processing of biometric data as a special category, etc.[272]

b) Unknown social impact in the Czech Republic

This theme is closely related to the issue of risks, collection, processing and storage of biometric data, which is dealt with in more detail in point 3 of this text.

c) Ineffectiveness of general (present) legislation

The existing legislation lacks appropriate and complete clarity; the impacts and risks associated with the processing of biometric data are not clear either. It is not obvious to what degree the necessary level of protection is secured through the general legislation. However, a question arises as to what level of protection is desirable and what interests could be reflected for the needs and decisions of biometric data subjects to be respected and secured.

[271] CAMPISI, p. (ed). *Security and Privacy in Biometrics*, p. 385, point 15.5.3., p. 393, point 15.7.4., p. 423, point 16.3.1, 2.

[272] It is, of course, a question whether such exact limits can a priori be set at all. The answer to this question depends on the better and better data analysis methods and, naturally, on the circumstances of a particular case.

d) Problems related to biometric authentication

With regard to its specifics, biometric data is vulnerable since, as already stated above, it is unique, permanent and universal. The use of biometric data, for example, as general passwords, creates a risk of its compromising, without an option to change the password. Still, what biometric identification tool and processing form constitute the least risk? Are there effective methods mitigating the risks associated with biometric authentication? Is it necessary to apply the proportionality test to specific categories of biometric data in different ways? This, however, does not constitute an exhaustive list of problems.[273]

With regard to the aforementioned, it needs to be stated that, similar to other dynamically developing legal domains,[274] neither technological changes alone nor the tendency to legal and other risks associated with handling of biometric data intervene in the content of the present legal relations and their existing structures significantly enough to disrupt the actual substance of the functioning of these traditional legal structures. Nevertheless, it is obvious that these changes generate legal problems in many privacy protection spheres and regimes, which are very difficult to resolve on a normative basis; their solution can be found in the current constitutional principles and the interpretation methods related to them.

In this respect, it is becoming to remind that all co-authors of this monograph are aware of the individual parts of their text addressing frequently both the private law and the public law. Such a situation may sometimes make an impression of confusion of both spheres. It, however, cannot be overlooked that the actual constitutional case law in the form of Finding of the Plenum of the Constitutional Court of the Czech Republic declares that the legal order of the Czech Republic is, on the one hand, based on the dualism of public and private laws, but, on the other, the private and public laws are not currently divided by a 'Chinese wall'; hence, the closer overlapping and a mutual intensive influencing of private and public elements are occurring more and more frequently.[275] This situation needs to be counted on even in the future.

Hence, the normative basis of the solution should be, in particular, the better use and strengthening of the proportionality principle, including the appropriate weighing of the protection of the fundamental right to private life on the one side and the protection of public interest and third-party rights through the collection, processing and storage of biometric data on the other. The special legal protection of biometric data in contrast to the protection of, in particular, the fundamental right to private life (and related fundamental rights) are usually connected vessels; they can hardly be examined independent of each other.

The application of the proportionality principle should draw from the principle that biometric data can be collected, processed and stored only for such purposes which a prudent person considers as appropriate and indispensable under the particular circumstances. This can be identified as a test of prudency and appropriateness of its kind; the test should be predicated on four criteria related to, or associated with, the proportionality test (compare above). According to these criteria, prior to the collection or processing of biometric data, it should be examined and confirmed that the collection, control and processing of individuals' biometric data is indispensable to achieve the given goal or need, that it is the most effective method of achieving the given goal or need, that the loss of privacy associated with a particular method of processing particular biometric data is proportional (i.e. certain proportionality of intervention in the privacy is secured in contrast

[273] There are specific technological solutions (PET – Privacy Enhancing Technologies) enabling, for example, the taking of a sample of biometric data (e.g. a basal smear) and the subsequent processing of only a portion of it and the deletion of the original data. It is biometric data which is deprived of a part of its information value. The question is as to whether and to what extent it remains to be biometric data.

[274] For more see, for example, MATEJKA, J. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*, p. 187.

[275] Compare the Finding of the Constitutional Court of 10 January 2001 No. Pl. ÚS 33/2000.

to the contribution associated with such processing of biometric data) and that there is no other appropriate method of achieving the given goal which would constitute lesser intervention in the respective individuals' privacy.[276]

However, it is also necessary to strengthen the guarantees against misuse of biometric data. The relevant judicature in this respect is the one of the European Court of Human Rights. In case *Gardel vs. France*, Judgment of 17 December 2009, Application No. 16428/05[277], the court held that security guarantees should ensure that biometric data was relevant (in relation to the purpose for which it was stored) rather than excessive over the period not longer than as required by the given purpose and that other adequate guarantees against misuse of this data were adopted. The stated requirements then come to the fore, in particular, in young people. In the cited case *S. and Marper vs. United Kingdom* (where it came to the storage of DNA and fingerprints), the judicature of the European Court of Human Rights inferred that there had to be a time limitation since, otherwise, young people took the risk of stigmatization and the feeling of stigmatization.

Measures of a preventive nature should be adopted to prevent misuse of biometric data. They include, in particular:

1) strengthened liability of controllers and processors (i.e. including operators and possible providers) for possible damages and strengthening of their control by the competent independent authority;
2) a periodical audit of biometric systems and their certification and monitoring by an independent authority; such authority in the Czech Republic is the Personal Data Protection Office (Section 50 et seq. of the Personal Data Processing Act);
3) informative consent of a data subject to the processing of his or her personal data (biometric data); the necessary exceptions are stipulated in the given state's legislation

Moreover, it is necessary to strengthen the protection of special groups from discrimination. Alongside the classical cases of discrimination stated in Article 3 (1) of the Charter of Fundamental Rights and Freedoms (gender, race, etc.), this also includes possible discrimination for reasons such as a subject's mental weakness, physical handicap, etc. It is also necessary to further and appropriately check the compliance of the confidentiality obligation in relation to biometric data.

To conclude, it can be stated that the fundamental right to privacy or private life is closely related – and sometimes overlaps – with other fundamental rights regulated in other Articles of the Charter of Fundamental Rights and Freedoms, the Convention for the Protection of Human Rights and Fundamental Freedoms, and international covenants. It is appropriate here to state, in particular, the fundamental right to human dignity, personal honour and good reputation (compare Article 10 (1) of the Charter) and the fundamental right to the protection of personal data definitely affecting an individual's private life. The same conclusions were also adjudicated by the European Court of Human Rights in case *Amanna vs. Switzerland* No. 27798/95. General conclusions relating to the handling of biometric data result from the above text, of which the following can be recommended:

- The judgment brought significant changes in relation to biometric data. Biometric data belongs among personal data which is of a special sensitive nature in terms of fundamental rights and freedoms and which requires special protection in its processing. Its processing is prohibited unless there is an exception to its processing.

[276] Compare, for example, PARLAMENTNÍ INSTITUT. Odpověď na dotaz: Právní úprava biometriky. Červenec 2014, p. 6, 7 – Kanada. Personal Information Protection and Electronic Documents Act. S. C. 2000, p. 5

[277] RAINEY, B. – WICKS, E. – OVEY, C. *The European Convention on Human Rights*. 6th edition. Oxford: Oxford University Press, p. 378.

- Biometric data is of a special nature because it relates to behavioural and physiological characteristics of individuals and enables their unique identification. This is, however, associated with significant risks ensuing from the actual nature of biometric data. This data may be misused for discrimination, stigmatization or confrontation. Unlike other identification data, no individual can be provided with a new identification if it has been disrupted.

- Biometric data needs to be always understood in the context of knowledge of biometric technologies. The assessment of biometric data is newly based on the principle of technological neutrality, which, in practice, means that differentiation predicated on the direct and indirect identification of data subjects is going to be abandoned and a broader concept of biometric data is going to apply.

- In considering the processing of biometric data, it is always necessary to consider first whether the processing of personal data through biometric technologies is necessary and there are no other solutions not using biometric data.

- In certain situations, the only possible legal regime for using biometric data will be the consent, which, however, must be free and informed. However, even in these cases, an option without biometric data being used should be offered. Only an informed user should decide whether to provide his or her personal data for the purposes of its processing in biometric systems or whether to pick another option of which he or she has been informed in advance. The general rule that individuals who cannot or do not want to use biometric data should be offered other options, for example, a card, name tag, chip, etc., should be introduced.

- The use of biometric data needs to take into account, for example, that children, employees, seniors or handicapped persons may lose sensitivity in relation to the use of biometric data, in particular, in its excessive use. It is a fact that, for instance, children do not realize the risk of using biometric data and prefer a simple verification form. In this respect, it is necessary to provide sufficient, transparent and intelligible information on the use of biometrics, including possible risks. This task of an essential significance should be fulfilled by both the family and educational institutions.

Given the reasons referred to above, it is also necessary to insist on a thorough application of all related legal and technological guarantees against misuse of these categories of data with regard to the legal framework resulting from the Regulation and the constitutional laws where the protection of the fundamental right to human dignity, i.e. a right at the fulfilment of which almost all other human rights directly or indirectly are aimed, always comes first.[278]

3.2 Current Czech Personal Data Protection Legislation

The Czech Republic adopted a new Act on Personal Data Processing[279] on 12 March 2019. The act provides from derogations from the GDPR and implements the DPDCJA.

[278] For more details of the issue of human rights in relation to biometrics see GÜTTLER, V. – MATEJKA, J. K otázkám některých základních lidských práv a svobod v souvislosti s právní ochranou biometrických údajů. *Právník*. 2016, No. 12, p. 1055.

[279] Act No. 110/2019 Coll., on Personal Data Processing (zákon č. 110/2019 Sb., o zpracování osobních údajů).

The act does not explicitly refer to biometric data in the sense of Art. 9 par. 4 of the GDPR. Rather it refers to special categories of personal data as specified in Art. 9 par. 1 of the GDPR. According to § 16 par. 2 of the Czech act, processing of special categories of personal data for the purposes of scientific or historic research or for statistical purposes should be done only in a manner that does not allow for identification of data subjects, unless the data subject's legitimate interests prevent it. Unfortunately, the Explanatory report does not provide clear clarification of this provision[280] and elaborates only on the next provisions that relate to processing for journalistic purposes or academic, artistic or literary expression defined in § 17–23. The act implies in § 17 that special categories of personal data can be processed for the above mentioned purposes if such processing is proportional. Moreover, such processing of personal data is not subject to the authorization or approval of the national Data Protection Authority and enjoys the right to source protection and protection of the content of the information including processing of personal data in a manner allowing remote access. The Explanatory report stipulates that this provision aims to preserve the same standard and space of the freedom of the press and refers to other relevant provisions such as Civil Code or constitutional norms. A test of proportionality must be made before data is published. Special categories of data cannot be published for instance only for the purposes of having sensational front-page news as this cannot be considered as a lawful purpose. It is worth to note that the Explanatory report does not limit processing special categories of data in so called "preparatory stage" in which data is collected for further investigative work and making conclusions.

The Act on Personal Data Processing implements the DPDCJA in Section III. in § 24–42. For the purposes of this Section, § 24 par. 2 refers to the relevant definitions of the GDPR, including the definition of biometric data. However, the Act does not contain any specific derogations from the DPDCJA with regard to this category of personal data.

3.3 Other Legislation with Specific Rules on Biometrics

3.3.1 Travel Documents

The issue of travel documents is also regulated in the Czech law. Pursuant to the Travel Documents Act,[281] facial recognition and fingerprints are entered in the document in machine-readable form. In certain people, only facial recognition is recorded [see Section 5 (4)]. The Act regulates the collection of biometric data (Section 21a) and the verification of the functioning of a data carrier containing biometric data (Section 21b). Biometric data is also recorded in service and diplomatic passports.

Travel document holders are entitled to *"*ask for verification of the functioning of a data carrier and of the correctness of their biometric data contained in it*"* and, in the event of discrepancies, they are entitled to be issued a new travel document (Section 32a). Unauthorized processing of personal data from a biometric data carrier is considered a misdemeanour. Other details relating to biometric data in public documents and travel documents are stipulated in other laws.[282]

[280] Explanatory report to Act No. 110/2019 Coll., on Personal Data Processing. In: *Beck-online* [online]. 2019 [2019-04-30]. Available at: <https://www.beck-online.cz/bo/chapterview-document.seam?documentId=oz5f6mrqge4v6mjrgbpwi6q&rowIndex=0>.

[281] Act No. 329/1999 Coll., on Travel Documents, as amended.

[282] See Act No. 197/2009 Coll., on the certification of public documents containing biometric data and the amendments to certain Acts, as amended; Decree No. 415/2006 Coll., laying down the technical conditions and procedure in the collection and further processing of biometric data contained in travel document data carriers; Decree No. 400/2011 Coll., implementing the Identity Cards Act, as amended, and the Travel Documents Act, as amended; Methodological

3.3.2 Biometric Data of Foreigners

Biometric data is also used for identifying foreigners entering the territory of the Czech Republic. The fundamental legislation in this respect is the Act on the Residence of Foreigners,[283] laying down the obligation of foreigners to acquiesce to the verification of their biometric data in entering the territory of the Czech Republic (Section 5 (2) b) or to the collection of their biometric data in filing an application for long-term residence (Section 44) or for permanent residence (Section 74). In general, foreigners are obliged to acquiesce to the collection of their current biometric data for the purpose of verifying the authenticity of their passes (Section 103 t). Special rules apply to the issuance of alien's passports (Section 113). Foreigners are issued residence permits based on their residence permit applications. A residence permit bears a data carrier containing biometric data – facial recognition and fingerprints. A residence permit containing biometric data is also issued pursuant to Section 35 of the Act on Temporary Protection of Foreigners[284] and Section 59 of the Asylum Act[285]. The latter Act is implemented through a special Decree laying down the conditions of collection of biometric data in the form of facial recognition, fingerprints, and signature.[286]

3.3.3 Processing of Biometric Data by the Czech Police

The Police of the Czech Republic process information and personal data in compliance with the Act on the Police of the Czech Republic[287] (hereinafter "PCRA"). Work with information is regulated in Sections 60–80 of the PCRA. The PCRA does not use the term 'biometric data' as such, but allows the Police to "take fingerprints, ascertain physical characteristics, measure an individual's body, make visual, audio and similar records, and take biological samples enabling the detection of genetic information" (Section 65 (1) of the PCRA) in individuals accused of an intentional offence, individuals notified of being suspected of an intentional offence, individuals serving a prison sentence for the commission of an intentional offence, individuals ordered to undertake protective in-patient treatment or detention proceedings, or missing and found individuals a search for whom was launched and whose legal capacity is limited (Section 65 (1) of the PCRA). However, such data can be collected only for the purpose of a future identification. Save for situations when the individual's physical integrity could be violated (e.g. in the blood taking), a police officer may, after a futile request for being allowed to collect an individual's data, collect the data despite the individual's resistance to its collection. The Police of the Czech Republic may also collect information from registers operated on the basis of a special law (Section 66 of the PCRA), including the register of travel documents containing personal biometric data. The legislation allows the Police of the Czech Republic to process personal data, including sensitive data, without an individual's consent provided that they are doing so to fulfil their tasks (Section 79 of the PCRA).

Instruction of the Ministry of the Interior ref. No. SC-243/2006 of 6 September 2006, regulating the procedure of municipal authorities with extended competencies in the processing of applications for, and the issuance of, passports containing machine-readable data and biometric data carriers; Directive of the Ministry of the Interior concerning Act No. 133/2000 Coll., on the resident register and personal identification numbers and on the amendments to certain Acts (Resident Registration Act), as amended; Act No. 328/1999 Coll., on identity cards, as amended; and Act No. 329/1999 Coll., on travel documents and on the amendment to Act No. 283/1991 Coll., on the Police of the Czech Republic, as amended, (Travel Documents Act), as amended.

283 Act No. 326/1999 Coll., on the Residence of Foreigners in the Czech Republic and on the Amendments to Certain Acts.

284 Act No. 221/2003 Coll., on Temporary Protection of Foreigners, as amended.

285 Act No. 325/1999 Coll., on Asylum, as amended.

286 Act No. 88/2011 Coll., on the technical conditions and procedure in collecting foreigners' biometric data and signatures for issuing their residence permits, as amended.

287 Act No. 273/2008 Coll., on the Police of the Czech Republic, as amended.

Biometric data plays a role even in the execution proceedings anchored in the Criminal Procedure Code (hereinafter "CPC")[288]. Where house arrest is ordered and compliance with this sentence is inspected, *"*the convicted individuals shall be obliged to allow the inspection authority upon request to enter their places of sentence and to acquiesce to the collection of their biometric data, in the commencement and during the execution of an electronic inspection, if they are suspected of being in breach of the obligations subject to inspection. The collected biometric data comprises fingerprints, facial characteristics, and voice record*"* (Section 334 (1) of the CPC).

Accused individuals shall be obliged to acquiesce to the collection of their biometric data even during the electronic inspection of the fulfilment of their obligations imposed as measures replacing the custody (Section 360a (2) of the CPC). Even in this respect, biometric data means fingerprints, facial characteristics, and voice record. The actual procedure of collecting and verifying biometric data is described in detail in the Explanatory Report on the amendment to the CPC of April 2016[289]. According to the Report, biometric data should be taken either for the purpose of *"*a double verification of identity or for the purpose of a subsequent measurement of blood alcohol content in breath (in relation to a possible order to refrain from drinking alcohol)*"*.

The concept of biometric data is also recognized in the Criminal Register Act[290] (hereinafter "CRA"). Pursuant to Section 10 (5) of the CRA, no biometric data shall be specified in the special section of a transcript of the Criminal Register, which, pursuant to Section 4a, is intended for *"*details of final convictions of Czech nationals entered in criminal proceedings in courts of another Member State of the European Union and data relating to such convictions on the basis of information sent by other Member States of the European Union*"*. Given the enactment of the DPDCJA, the regulation referred to will have to be revised and, possibly, made compliant with the rules of this Directive by 6 May 2019.

3.3.4 Processing of Biometric Data by the Czech Military Police

Personal data is also processed by the Military Police pursuant to a special Act.[291] The handling of information is regulated in Sections 10–20 of the Military Police Act (hereinafter "MPA"). Pursuant to the MPA, the Military Police shall be entitled, in particular, to make audio, visual and other records from publicly accessible locations (Section 11), solicit information from designated information systems (Section 12), or process personal data, including sensitive, without a data subject's consent (Section 13). Special rules apply to the processing of personal data in the prevention and revelation of crimes (Section 14) and in the search for soldiers (Section 15). An amendment to the MPA,[292] expressly devoted, among other things, to the processing of biometric data, is being heard by the Government.

Based on the amendment referred to above, Section 11a should be incorporated in the Act and should allow the Military Police to collect personal data for the purposes of future identification of natural persons accused of an intentional criminal offence or persons suspected of an intentional criminal offence. In essence, the cited Section copies, to an extent, Section 65 of the PCRA, pursuant to which

[288] Act No. 141/1961 Coll., on Criminal Proceedings (Criminal Procedure Code), as amended.

[289] Explanatory Report on Act No. 150/2016 Coll. amending Act No. 141/1961 Coll., on criminal proceedings (Criminal Procedure Code), as amended, Act No. 218/2003 Coll., on youth responsibility for unlawful acts and the judiciary in suits of youth and on the amendments to certain Acts (Youth Judiciary Act), as amended, and Act No. 40/2009 Coll., the Criminal Code, as amended.

[290] Act No. 269/1994 Coll., on the Criminal Register, as amended.

[291] Act No. 300/2013 Coll., on the Military Police and on the Amendments to Certain Acts, as amended.

[292] Parliamentary Press No. 973/0 of 29 November 2016, a government bill amending Act No. 300/2013 Coll., on the Military Police and on the Amendments to Certain Acts (Military Police Act), as amended.

the Military Police would be entitled *"*to take fingerprints, ascertain physical characteristics, measure an individual's body, make visual, audio and similar records, take biological samples enabling the detection of genetic information of a natural person, and process this data further*"* despite an individual's resistance. A military police officer would be allowed to surmount the resistance to an extent commensurate to its intensity, except in situations when the individual's integrity could be violated, e.g. in the blood taking.

3.3.5 Obligatory Biometric Identification or Authentication

The Czech legislation specifically requires biometric identification of people entering delimited and demarcated premises of nuclear facilities. These premises have four concentric levels *"*differing by the type of protective measures*"*[293] and comprise the guarded area, the protected area, the inner area, and the vital area.[294] Pursuant to the implementing Decree to the Nuclear Act,[295] *"*anyone authorized to enter the guarded, protected, inner or vital areas must be equipped with an identification card enabling automated check of their access. Biometric identification must be used for checking the access of natural persons, at least in the access to the inner area or the vital area. The current database of accesses must be available for at least 1 month and its permanent storage must be ensured*"* [Section 11 (2)]. Section 11 of the Decree lays down the conditions of storage of information concerning identification cards, accesses and passages of people, recorded voice communication of workers, and people's movement monitored in the event of an extraordinary radiation accident. The biometric identification obligation is also stipulated in Section 13 (1) and (4) of the Decree relating only to the inner area and the vital area. These areas are also furnished with a mandatory system detecting disturbances and with an industrial television system.

Another sphere where biometric identification shall be required are payment transactions. On 21 March 2017, the Government submitted to the Chamber of Deputies of the Parliament of the Czech Republic a payment bill as Parliamentary Press No. 1059/0.[296] Section 223 of the bill counts on the so-called strong verification of a user by an entity authorized to provide payment services, in cases when, for example, a user accesses his account through the Internet or enters an electronic payment order. The strong verification is then defined in Section 223 (3) of the bill, pursuant to which it shall mean *"*a verification predicated on the use of at least 2 of the following elements: a) a detail known only to the user, b) property which the user has in his possession, c) user's biometric data*"*.

Hence, biometric data is only one of the verification options and does not necessarily need to be mandatory. On 16 October 2017, the bill was delivered to the President of the Czech Republic for signature and should come into effect on 13 January 2018. Biometric data is recognized, by the way, also in the Accounting Act.[297] Section 33 (2) c) of the Accounting Act counts on the so-called combined form of an accounting record, being *"*a record in paper form, also containing information in technical form not legible for natural persons and enabling its translation into a form in which its content is legible for natural persons*"*. A passport containing biometric data is stated in the Explanatory Report on the amendment as an example of such a combined form.[298]

---

293 Explanatory Report on Act No. 263/2016 Coll., the Nuclear Act, Section 161.
294 Act No. 263/2016 Coll., the Nuclear Act, as amended, Section 161 (1).
295 Decree No. 361/2016 Coll., on Security of Nuclear Installation and Nuclear Material.
296 Parliamentary Press No. 1059/0 of 21 March 2017, a government payment bill; In: *Poslanecká sněmovna Parlamentu České republiky* [online]. 16. 10. 2017 [cit. 2017-10-16]. Available at: http://www.psp.cz/sqw/historie.sqw?o=7&t=1059
297 Act No. 563/1991 Coll., on Accounting, as amended.
298 Explanatory Report on Act No. 304/2008 Coll. amending Act No. 563/1991 Coll., on Accounting, as amended, and certain Acts. See as for Articles 32–34.

Mandatory biometric identification was also considered in the Explanatory Report on Gaming Act[299] where biometric identification of players was to be included in the so-called *pre-commitment* system and was to ensure the observance of gaming limits. However, this requirement was abandoned in the end.

3.4 Special Cases of Processing Biometric Data

3.4.1 Dynamic Biometric Signature

A highly significant group of the behavioural biometric methods[300] through which the identity or the authentication of a particular person can be determined is, in particular, the analysis of the handwriting and the signature.

The thing is that the current technologies, or, more precisely, their applications, enable a detailed evaluation of not only the resulting static image of handwriting but also the highly sophisticated and detailed process of creating (writing) a signature. We speak about the so-called dynamic signature verification methods evaluating, in real time, the speed of writing a signature, the pen pressure in the individual phases of handwriting, etc. What is also evaluated are the direction and the sequence of writing certain elements, such as striking out, accentuation of certain parts, writing periods, etc. Some people, for example, write diacritics only at the end, while others continuously. Someone underlines or strikes out from left to right, while another the other way around. All this is missing in the static evaluation of the final signature like we all visually evaluate it today in day-to-day practice. Similar to dactyloscopy, two absolutely identical signatures (their graphical images) are understood today as the possible results of forgery or falsification rather than an ideal sameness of the signature and its original specimen, absolutely regardless of the fact that nobody ever provides an absolutely identical signature at all times. From the application analytical perspective, it is possible to discern a certain determinant uniqueness within the meaning of the overall logical, time, grammar or other behaviourally determinant sequence of the individual lines of a pen in its overall context.[301] These technologically relatively new signature verification methods then logically lead to the search for new and promising ways of unambiguously anchoring this specific type of signature at legal and general levels.

A signature at the general legal level represents a summary issue significantly overlapping a number of legal domains, both public and private. While, in the domain of public procedural law, it is an issue that has already been resolved in substantial part[302] or, more precisely, is associated, on a judicature basis, with the use of either handwritten or electronic[303] signature or with the use of fiction signature

[299] Explanatory Report on Act No. 186/2016 Coll., on Gambling, as amended.

[300] Biometrics, as a field devoted to the observation of living organisms, is divided into two spheres – physical biometrics and behavioural biometrics (also known as behaviometrics). While physical biometrics monitors specific physical attributes of living organisms (for example, in the event of people, voice, fingerprints, palm bloodstream map, face shape or eye cornea), behavioural biometrics focuses on monitoring their behaviour.

[301] For more details, see, for example, RAK, R. – MATYÁŠ, V. – ŘÍHA, Z. *Biometrie a identita člověka: ve forenzních a komerčních aplikacích*, p. 134.

[302] See, for example, the opinion of the Supreme Court's plenum of 5 January 2017 on the filings made electronically and the delivery of documents electronically issued by the court through public data network (Opinion No. Plsn 1/2015).

[303] As in the event of signing an electronic document expressing a legal act towards a public signatory or another person in relation to the exercising of their competencies pursuant to Section 6 et seq. of Act No. 297/2016 Coll., on trust services for electronic transactions, as amended.

in acts undertaken through a data box,[304] the public regulation of the processing of dynamic biometric signatures provides numerous yet unsolved legal application and purely security practical problems.

The solution to these problems needs be found, in particular, both in the current practice and the analysis of related provisions of the Czech and European legislations, specifically, in Regulation of the European Parliament and of the Council (EU) No. 910/2014, on electronic identification and trust services for electronic transactions in the internal market ("eIDAS"), in Act No. 297/2016 Coll., on trust services for electronic transactions, as amended ("ETTSA"), and the provisions of Act No. 89/2012 Coll., the Civil Code, as amended ("CC"). With regard to the essence and the meaning of the dynamic verification methods of this type, it is also necessary to responsibly consider the associated obligations for further processing of such behavioural personal data in accordance with the GDPR guidelines. It is not possible either to set apart the important related issue of the evidentiary reliability of these signatures, in particular, in comparison with the other traditionally used alternatives of electronic or handwritten signatures.

Private law is traditionally predicated on relatively unchanging legal principles entailing certain limits for both the legislator and the permissible interpretation application scope of the legislation. These principles undoubtedly include the principle of the directory nature of legislation and the principle of legal certainty, including the related postulates, such as the prohibition of retroactivity, protection of acquired rights, foreseeability of the decision-making, etc. Both these principles are thoroughly reflected in Sections 559–564 of the CC, regulating the forms of legal action, including the so-called electronic legal acts as specific written documents implemented through electronic means, including the requirement for their signature.

In principle, a legal act may take any form, unless written form is required pursuant to the laws (Section 559 of the CC), in general, in cases when the meaning and the nature of such act so require. Hence, in this respect, it is possible to differentiate between an informal legal act, the form of which is not legally regulated, and a formal legal act, for which a particular (usually written) form is prescribed, fulfilling, at the same time, a certain warning function. The failure to observe such form may result in both relative[305] and absolute[306] invalidity of a legal act,[307] but not always. The judicial practice usually restricts the consequences of invalidity to cases where the sense and the purpose of the laws so require (NS 29 Cdo 3919/2014).

Where written form is required pursuant to the laws,[308] an act (undertaken in writing) has to be signed by the acting person to be valid. Through a blanket legal rule, the laws refer to another regulation stipulating the method of electronically signing a written document in a legal act undertaken through

[304] Pursuant to Section 18 (2) of Act No. 300/2008 Coll., on electronic acts and the authorized conversion of documents, as amended, an act undertaken by an authorized or designated person through a data box shall have the same effects as an act undertaken in writing and signed.

[305] In particular, in situations when the statutory requirement for legal form is set only to protect a certain person's interest, i.e. fulfils, in essence, only the warning function for the parties to such act (Section 586 of the CC).

[306] In particular, in situations when the chosen form seems to be contrary to good morals or the laws and evidently breaches the public order (Section 588 of the CC). The absolute invalidity is in place, in particular, when the requirement for the form does not fulfil only the warning function but also the security function to the benefit of third parties or in the public interest – see, for example, the transfer of a real right to real estate property pursuant to Section 560 of the CC), etc.

[307] We speak about an element of a legal act within the meaning of Section 545 of the CC. The prescribed form should be observed in relation to an entire legal act. Nevertheless, the judicature does not exclude that parts of a legal act be undertaken in various forms; compare decision NS 29 Odo 14/2001 or NS 2 Odon 76/97.

[308] The obligation of a written form may be prescribed in the laws or may be pre-agreed between the parties (Section 559 of the CC). Where no written form is prescribed, any form of an electronic act may be taken, even without electronic signature. Nobody can be forced to choose a form or accept it (Section 559 of the CC). Pursuant to the laws of the Czech Republic, no legal act the signature of which requires third-party certification (official certification) can be undertaken through electronic means, not even those legal acts for which the laws stipulate more elements rather than the written form, such as the requirement for a last will being handwritten pursuant to Section 1533 of the CC. For more details, see KMENT, V. Nahradí elektronický podpis prostý ten tradiční vlastnoruční? *Bulletin advokacie*. 2016, No. 12, p. 5.

electronic means (Section 561 (1) of the CC). Such law is, in particular, the ETTSA, the so-called adaptation regulation to the eIDAS stated above. In the event of electronic legal acts, the requirement for written form is fulfilled by attaching electronic signature to the content of a legal act within the meaning of the ETTSA.

However, the applicable legislation allows an exception to the stated requirement for signing a written legal act. It ensues from Section 562 (2) of the CC that written form shall be preserved in legal acts undertaken through electronic or other technical means enabling the depiction of the content of a legal act and the identification of the acting person, completely regardless of whether the legal act has been signed or not. It is a special regulation of electronic written instruments without signatures (lex specialis[309] in relation to Section 561 (1) of the CC), to which the laws ascribe the legal effects of written documents provided they enable the depiction of an act and the identification of an acting person.[310] On the one hand, the laws do not expressly require signature for these other forms, but, on the other, stipulate an essentially similar requirement for the acting person's identification, which can be considered as a legal alternative of a signature, the purpose and the main function of which is usually the actual identification. In this respect, it can be stated that this 'identification' requirement can be fulfilled, for example, through a biometric or other similar identifier which *stricto sensu* does not constitute a signature in the legal sense, but meets similar purpose and function. The stated concept both reflects the parties' autonomous intentions in private law and constitutes a step towards expanding electronic contracting and legal acting.[311]

As already stated above, the Civil Code stipulates the condition of attaching electronic signature to electronic legal acts within the meaning of the ETTSA, the only law stipulating the method of signing such written documents. The provision of Section 5 et seq. regulates the types of signature based on the signatory or, more precisely, on the public nature of a signature, as well the individual legally admissible types of electronic signature regulated in the eIDAS. It unambiguously ensues from Section 7 of this Act that "guaranteed electronic signature, recognized electronic signature, or, possibly, another type[312] of electronic signature can be used for electronic signing if the electronic document through which a legal act is undertaken is signed in a way other than the one stated in Section 5 or Section 6 (1)". The so-called 'another type of electronic signature' within the meaning of this provision is also the basic (common) electronic signature pursuant to the eIDAS, whereby the 'other way' shall be a legal act within the meaning of the CC, i.e., typically, the signing of private electronic written documents. Therefore, it ensues from the applicable legislation that, in essence, any type of electronic signature pursuant to the eIDAS is sufficient in private relationships to meet the formal elements.

---

309 A similar conclusion is also contained in the commentary literature MELZER, F. – TÉGL, P. a kol. *Občanský zákoník. Velký komentář. III. Svazek*. Praha: Leges, 2014, p. 637, or, possibly, also ŠVESTKA, J. a kol. *Občanský zákoník. Komentář. Svazek I*. Wolters Kluwer, 2014, p. 1387, or also PETROV, J. – VÝTISK, M. – BERAN, V. a kol. *Občanský zákoník. Komentář*. C. H. Beck, 2017, p. 597.

310 Nevertheless, the provision of Section 3026 (1) of the CC, stipulating that, unless the nature of a written document so enables, the provisions of this Act shall apply accordingly even to other written documents regardless of their form, seems problematic in this sense. Hence, the stated provision expressly allows using the analogy of the legal provisions regulating the form of a document even for other forms of written documents, i.e. including electronic written documents and other tests not portable on tangible carriers, etc.

311 In relation to the foregoing, it is also necessary to mention the related Section 562 (2) of the CC, regulating the so-called presumption of reliability of electronic records stating that records on legal acts in an electronic system shall be considered as reliable if undertaken systematically and gradually and protected against changes. If a record is made in the operation of an enterprise and the other party invokes it to his benefit, it shall be considered as reliable.

312 The Act considers as exceptions in this sense only the acting of the state or, more precisely, its organizational units and other public signatories pursuant to Section 5 (1) of the ETTSA, which requires qualified electronic signature within the meaning of eIDAS.

Perusing the relevant provisions of the eIDAS, we can notice that the basic form of electronic signature is defined in Article 3 (10), stipulating that electronic signature shall mean:

– data in electronic form;
– data attached to, or logically associated with, other data in electronic form;
– data used by a signatory for signing

Through a mere analysis of the definition stated above, it can be concluded that the respective defining provision does not per se contain any qualitative requirements towards the identification or determination of a signatory's identity. The only qualitative element is the highly general reference to the common usage of the signatory attaching 'the data used for signing', which, in essence, may be any data in electronic form. The stated non-restrictive provision obviously meets the principle contained in Art. 25 (1) of the eIDAS, pursuant to which electronic signature must not be denied legal effects and must not be rejected as a proof in court or administrative proceedings only because it is electronic or because it does not meet the requirements for qualified[313] electronic signatures[314]. The issue of electronic contracting and the individual elements and functions are discussed in more detail, though with different legal qualification, for example by J. Matejka,[315] R. Polčák,[316] F. Korbel with F. Melzer,[317] K. Čermák,[318] and V. Kment.[319] However, the actual issue of the legal admissibility and, hence, the validity or permission of electronic signature based on the attachment of, in essence, any *'data used for signing'* pursuant to the eIDAS or the procedure as per Section 562 (1) p) of the CC, constituting a special regulation of valid written documents without a signature (in contrast with the general regulation of written documents with signature in Section 561 (1) first and third sentences of the CC), does not and cannot even come as a surprise since similar conclusions were already deduced[320] in the past in relation to the previous legislation.

3.4.1.1 Signing of Electronic Written Documents through Physical or Behavioural Biometrics Data

As already stated above, the valid legislation allows an electronic document (i.e. a legal act in private electronic documents) being signed electronically, for example, by affixing, in essence, any 'data used for signing' to it. In terms of their significance, possible use and legal force, electronic written documents have a position equivalent to other traditional forms, including paper ones (typically paper record carriers).[321] Hence, this equivalency of paper and electronic forms has much broader impacts in many respects than just on written documents since, from the legal perspective, it relates not only to writing but also to image, sound or other records; therefore, these documents are limited, in

[313] Qualified electronic signature has legal effects identical to handwriting (Article 25 (2) of the eIDAS).
[314] Even the reasoning of the eIDAS (Article 48 et seq.) stipulates that, to ensure the mutual recognition of electronic signatures, a high level of security is necessary, but electronic signatures of a lower security level should also be accepted in special cases, for example, in the context of Commission Decision 2009/767/EC of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the points of single contact under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market (notified under document C(2009) 7806) (Text with EEA relevance)).
[315] MATEJKA, J. Úprava elektronického podpisu v právním řádu ČR. *Právník*. 2001, Vol. 140, No. 6, pp. 582–611.
[316] POLČÁK, R. Elektronické právní jednání: změny, problémy a nové možnosti v zákoně č. 89/2012 Sb. *Bulletin advokacie*. 2013, No. 10, pp. 34–40, p. 36, or also POLČÁK, R. Praxe elektronických dokumentů. *Bulletin advokacie*. 2011, No. 7–8, p. 55.
[317] KORBEL, F. – MELZER, F. Písemnost, elektronický a biometrický podpis v elektronickém právním jednání. *Bulletin advokacie*. 2014, No. 12, pp. 31–36, p. 32.
[318] ČERMÁK, K. jr. Elektronický podpis: pohled soukromoprávní. *Bulletin advokacie*. 2002, No. 11, pp. 64–77.
[319] KMENT, V. *Nahradí elektronický podpis prostý ten tradiční vlastnoruční?*, p. 5.
[320] For more details see, for example, MATEJKA, J. *Úprava elektronického podpisu v právním řádu ČR*.
[321] The stated principle is indirectly accentuated, among other things, in Section 2 e) of Act No. 499/2004 Coll., on Archival Science and the Filing Service, pursuant to which a document is any written, visual, audio or other recorded information, whether analogue or digital.

particular, by the existing technical possibilities of recording on paper rather than by legal limitations of their use.[322]

In the traditional (i.e. in particular, paper) form, a signature usually represents a handwritten name (autograph). Hence, it concerns a handwritten expression through characters amounting to letters. The specific nature of a signature is determined, primarily, by the legal usage, whereby the validity of a written legal act is not conditional upon the completeness (i.e. for example, the statement of full name and surname) or legibility of the signature; however, the acting person's identity needs to be obvious in the overall context. Regarding the place of the signature, the essence of a signature is something that 'constitutes a written deed', meaning that it typically 'completes' or 'confirms' the text or the act to which it relates.[323]

One of the consequences of the stated equivalency of the paper and electronic forms is the fact that not only a written electronic document but also an electronic written document containing, for example, a visual, audio or other similar record[324] may be signed electronically. An electronic written document may be signed electronically pursuant to the eIDAS (see above), for example, through the so-called biometric forms of electronic signature constituting 'data used for signing'. These biometric forms of signature conform not only to the characteristics of the (plain) electronic signature but also to the general definition of a signature, i.e. its traditional form (see above). In the event of biometric options, regardless of whether they concern dynamic biometric signature or other behavioural forms of signature, similar problems as in the electronic signature arise, in particular, when it comes to the attachment of this signature to an electronic written document. For this reason, requirements identical to those imposed on electronic signatures need to apply to this signature as well. In this respect, it is possible to admit that the mere attachment of a scanned signature, the entry of a specific password or code, or the fulfilment of another authentication procedure may constitute the signature of a written document in the form of (plain) electronic signature pursuant to Section 561 (1) third sentence of the Civil Code. The same applies to recorded voice attached to an electronic written document, the content of which is the confirmation of the respective legal act.[325]

The electronic forms of signing in the form of attachment of biometric (physical or behavioural) data to electronic written documents (legal acts) not only follow the traditional (i.e. in particular, graphical) form of signature but also constitute a seemingly ideal interconnection of the traditional and the electronic concepts of signing within the meaning of the applicable legislation. Hence, in many respects, the allowed use of these modern forms of signing not only strengthens the position of electronic written documents and their legal use but also undoubtedly leads to the standardization of new practical procedures combining biometric methods (as an ideal authentication or quasi-identification tool) and cryptologic methods (qualified electronic signature).

---

322 The CC does not, in essence, prefer deeds to other forms of written documents. For example, pursuant to Section 3026 (1), all provisions of the CC pertaining to deeds shall also apply to other written documents regardless of their form, unless the nature of the written documents excludes it.

323 However, even here it is necessary to consider the tradition. For example, in lawyer-signed documents, the lawyer, as a representative, is signed on the first page of a written document (usually in the identification of a party to the procedure with a supplement that the lawyer is his legal representative).

324 However, for a document to be considered as written, the content of a legal act needs to be depicted in a way constituting a graphical depiction of a group of characters representing writing. For more details, see HULMÁK, M. Commentary on Section 40. In: ŠVESTKA, J. – SPÁČIL, J. – ŠKÁROVÁ, M. – HULMÁK, M. et al. *Občanský zákoník. Komentář.* 2nd edition. Praha: C. H. Beck, 2009, p. 369.

325 However, with regard to Section 562 (1), the practical difference between both situations is minimal since, in electronic form, it is possible to validly undertake a written act without a signature if the used means allow depicting the content of the act and identifying the acting person.

3.4.1.2 Evidentiary Reliability of Electronic Written Documents Including Their Biometric Signatures

From the evidentiary procedural perspective, all forms of electronic written documents (including their signatures) can be considered as equal or equivalent (see above) and, thus, can serve as proofs within the meaning of all Czech procedural laws; however, the laws contain a relatively non-trivial procedure regulating the evidentiary reliability of certain related evidence, in particular, in Sections 565[326] and 566 of the CC[327] where the legislator relatively redundantly expressly speaks about a 'private document' rather than 'a private written document'. Nevertheless, with regard to the conclusions of the legal doctrine[328] and the provisions of Section 3026 (1) of the CC,[329] it is possible to arrive at the conclusion that these provisions apply also to private (electronic) written documents.

The stated provisions are relatively crucial in terms of the actual evidentiary reliability of the biometric forms of a signature, including dynamic biometric signature (see above). Considering that this technology of signing must, in some of its phases, gather the signatory's biometric characteristics (regardless of whether legitimately with the signatory's consent or illegitimately under a false pretext), it is not possible to exclude that this data may be misused in the future to develop other derivatives of the original signature. The thing is that biometric signatures exist 'per se' and are independent of the signed documents. Hence, on principle, it is not possible to exclude that they be removed from original electronic written documents and attached to other written documents.

For this reason, to practically use biometric signatures for signing electronic documents, we need some 'sufficiently reliable and firm' relation between a signature and a document that could not be severed and that immediately reveals any manipulation (alteration of the document or the actual signature). However, with regard to the development of neuron networks (artificial intelligence), these procedures are more and more non-trivial, but it is still possible to interconnect them with asymmetric cryptography methods (see below), where the obtained biometric data (dynamic biometric signature) is attached to the document to be signed, and, subsequently, the resulting signature is generated by the system in the form of qualified electronic signature.[330]

However, the stated procedure imposes major requirements on the quality and the functional properties of the relevant systems, adding the need for a sophisticated evaluation of biometric data (against the signature specimen) and, hence, the possible jeopardy of the entire system (the possibility of misuse of the signature specimen database), etc. These aspects have not yet been satisfactorily resolved.

However, from another perspective, it is, in particular, the provision of Section 562 (2) second sentence of the CC,[331] containing a clear presumption of evidentiary reliability (refutable legal

---

[326] It is up to the one seeking the validity of a private document to prove its genuineness and correctness. If a private document is used against a person who has obviously signed it or his heir or against a person who has acquired assets in the transformation of a legal entity as its legal successor, the genuineness and correctness of the document shall be considered as recognized.

[327] (1) If a private document is not signed, it is up to the one who has used it to prove that it comes from the person about whom he claims it. (2) It shall be assumed that written documents relating to legal facts associated with the common operation of an enterprise prove, if the other party is seeking their validity to his benefit, what is contained in them and that they were issued on the date stated in them, which shall also apply if they have not been signed.

[328] See, for example, MATEJKA, J. *Úprava elektronického podpisu v právním řádu ČR*.

[329] If the nature of a written document does not exclude so, the provisions of this Code pertaining to documents shall apply accordingly to other written documents regardless of their form.

[330] For more details, see PETERKA, J. Elektronický podpis na rozcestí. In: *LUPA* [online]. 6. 6. 2011 [2011-12-28]. Available at: <http://www.lupa.cz/clanky/elektronicky-podpis-na-rozcesti>.

[331] It shall be assumed that records on legal acts in electronic system are reliable if made systematically and consecutively and protected from alterations. If a record is made in the operation of an enterprise and the other party invokes it to his benefit, it shall be considered as reliable.

conjecture) which reflects on modern approaches to the essence of electronic written documents and, concurrently, considerably facilitates the use of typical and more and more frequent forms of electronic contracting,[332] that can be considered as crucial in terms of evidentiary reliability. This direction chosen by the Czech legislator is more convenient in many respects than reliance on various attempts aimed at preventing the known evidentiary reliability of electronic written documents by attaching other authentication mechanisms (usually, for example, other qualified signatures, marks and stamps) to a document. However, the trend of the electronic processing of documents unambiguously leads to their evidentiary reliability being established through the qualified method and procedure through which they have been developed or are saved on a long-time basis[333] rather than through the individual electronic signatures in them. Hence, it is the electronic system, or, more precisely, its functional properties, architecture and design, which provides guarantees through which the genuineness or the authenticity of the electronic written documents processed in it can be presumed or, subsequently, proven. If the one invoking a written document proves that the system in which the written document is saved has the stated parameters, the burden of proof passes to the one claiming its falseness.

3.4.1.3 Dynamic Biometric Signatures and Personal Data Protection

Comparing the traditional methods of signing electronic written documents through qualified signatures (i.e. based on asymmetric cryptography methods) with physical or behavioural biometrics methods, we must necessarily conclude on highly significant differences. The main difference is, in particular, the fact that, in the event of biometric methods, signature data cannot be invalidated or otherwise revoked. If the data is compromised for developing electronic signatures (private key), it can be easily and quickly invalidated by means of standard and well-known tools and a new key can be generated if needed. If a person's basic biometric characteristics are obtained illegitimately, whether by fraud in the way as described above or by theft from the referential database of biometric samples, it is very difficult to prevent their misuse. The affected user (if he even learns about it) may try to knowingly change his signature specimen, which, however, would contradict, to a certain extent, the basic idea of collection and comparison of a person's unconscious biometric characteristics and would undoubtedly involve a lengthy and uneasy phase of determining and getting used to another signature.

Therefore, biometric signature needs to be viewed as highly sensitive personal data within the meaning of both the current legislation (Personal Data Protection Act) and the GDPR, which pays special attention to biometric data. The GDPR defines and classifies biometric data as the so-called special category of personal data to which the special rules stipulated in Article 9 of the GDPR apply. Pursuant to the GDPR, data is covered by the definition of biometric data only 'when processed through a specific technical means allowing the unique identification or authentication of a natural person' (Recital 51 of the GDPR).[334]

---

[332] For more details, see, for example, MASON, S. *Electronic Signatures in Law*. Cambridge: Cambridge University Press, 2012, p. 259.

[333] For more details, see POLČÁK, R. *Elektronické právní jednání: změny, problémy a nové možnosti v zákoně č. 89/2012 Sb.* or, possibly, also VOLAREVIC, M. – STRASBERGER, V. – PACELAT, E. A philosophy of the electronic document management. In: *Proceedings of the 22nd International Conference on Information Technology Interfaces*. 2000 [2019-12-15]. Available at: <https://ieeexplore.ieee.org/document/915870>, p. 141.

[334] Biometric data is characterised as data that can be relatively easily read from a person's body and recorded, for example, in a photo, video or voice record. However, this data constitutes the so-called 'raw data', i.e. not yet processed data, and is not per se considered as biometric. Only after it is processed, biometric data, the so-called template, is developed within the meaning of the GDPR. Special processing rules then apply to this type of personal data.

Although the processing of biometric data is generally prohibited, Article 9 (2) of the GDPR provides ten exceptions to this prohibition. Pursuant to Article 9 (2) a) of the GDPR, biometric data can be processed if "the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject". The conditions of the granting of consent are then stipulated in Article 7 of the GDPR and the recitals.[335] Another related case when an administrator can process biometric data for the purposes of the unique identification is a case when the processing is necessary for "the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity" [Article 9 (2) f)].

Therefore, the normative basis of the solution should be, in particular, the better application and strengthening of the principle of proportionality, including the appropriate comparison of the protection of the fundamental right to private life, on the one side, and the protection of public interest and third-party rights through the collection, processing and saving of biometric data, on the other. The special legal protection of biometric data and, in contrast, the protection, in particular, of the fundamental right to private life (and to the related fundamental rights) are usually interconnected and can hardly be examined separate from each other.

The actual application of the principle of proportionality should draw from the principle that biometric data can be collected, processed and saved only for such purposes a reasonable person considers as appropriate and necessary under specific circumstances. This can be identified as a reasonableness and appropriateness test of its kind, which should be predicated on four criteria following or associated with the constitutional test of proportionality (compare above). According to these criteria, prior to collecting or processing biometric data, it should be examined and confirmed that the collection, administration and processing of biometric data of individuals is necessary to achieve the defined goal or need and that it is the most efficient method of achieving the given goal or need, that the loss of privacy associated with a particular method of processing biometric data is proportional (certain proportionality of the intervention in privacy in comparison with the benefit obtained through such processing of biometric data is ensured), and that there is no other suitable method of achieving the set goal that would constitute a smaller intervention in the affected individuals' privacy.[336] It is, however, necessary to strengthen the guarantees against the misuse of biometric data.

In other words, the personal data protection legislation (including the GDPR) requires that electronic documents are signed based on biometrics in compliance with its principles, both within the meaning of sufficient legal and technological guarantees against misuse and the existence of the legal title stated above. Hence, dynamic biometric signature needs to be viewed as sensitive personal data, whereby in the cases of its further automated processing (see the system above), it is necessary to proceed in compliance with the GDPR guidelines. The only legal title based on which such processing is generally implementable is the express and informed consent of each data subject pursuant to Art. 7 of the GDPR, which an administrator must be able to prove throughout the processing. Hence, the data subject must be duly informed about the processing of his sensitive data and the administrator has to fulfil other obligations relating to the processing of both personal and sensitive data pursuant to the GDPR. Increased attention needs to be paid, in particular, to the fulfilment of the information and notification duty and the safeguarding of biometric

[335] The special conditions relating to children's consent are stipulated in Article 8. The recitals relating to the granting of consent are recitals Nos. 32, 33, 38, 40, 42, 43, 50, 51, 65, 68, 71, 111, 112, 155, 161 and 171.

[336] Compare, for example, PARLAMENTNÍ INSTITUT. Odpověď na dotaz: Právní úprava biometriky. Červenec 2014, p. 6, 7 – Kanada. Personal Information Protection and Electronic Documents Act. S. C. 2000.

data.[337] With regard to the current development and new trends, it needs to be stated that the personal data protection rules stated above will apply accordingly even to other technologies that process biometric data enabling data subjects' identification and authentication.[338]

The crucial condition of functioning of the current legislation is, in particular, the fact that the law is able to flexibly and, particularly, efficiently react to the developed use of information and communication technologies. This prerequisite should constitute a completely natural and logical development in all legal domains, in particular, where there is no objective reason for public or mandatory legislation. This is undoubtedly the case even in the sphere of private law, which has recently been extensively re-codified. It is apt to question its efficiency, including the formal and material requirements imposed both on legal forms (written documents) and in relation to the evidentiary or other similar application problems.

As ensues from the analysis above**,** the solution to these problems needs to be found in both the application practice and the analysis of related provisions of the Czech and European legislations, specifically, the eIDAS, the GDPR and the related Czech legislation, including the Civil Code, the Trust Services Act, the Personal Data Protection Act, and others. In relation to the conclusions made above, it is necessary to deduce that the current legislation does not contain per se any qualitative requirements for a signatory's identification; the only qualitative element is the highly general reference to the signatory's per-se habit of attaching *'*data used for signing', which, in essence, may be any data in electronic form. Hence, this relatively liberal approach of the legislator not only fulfils the principle ensuing from the eIDAS but also confirms the traditional respect for the parties' autonomous will as an irreplaceable value for private law parties. Electronic signature, regardless of whether it is based on the methods of physical or behavioural biometrics, is not, therefore, denied legal effects and is not rejected as a proof in court proceedings.

For the communication through these modern forms to be efficient, the forms need to thoroughly draw from time-proven and established private law principles. The electronic forms of signing in the form of attachment of biometric (physical or behavioural) data to electronic written documents (through a legal act) not only thoroughly follow the traditional (i.e. in particular, graphical) concept of signature but also constitute a seemingly ideal interconnection of traditional and electronic concepts of signing aimed at the desirable natural development of law. Hence, the possible use of these modern forms of signing strengthens in many respects the position of electronic written documents and their legal use and undoubtedly leads to the standardization of new practical procedures combining biometric methods (as an ideal authentication or quasi-identification tool) and cryptologic methods (qualified electronic signature).

Despite the current liberal concept of this private-law matter, reflected in the CC, even the relatively essential limitations ensuing from personal data protection laws, stipulating that the signing of electronic documents in the simultaneous use of biometric methods (physical and behavioural biometrics) has to be implemented in compliance with all principles of personal data protection, need to be respected. For these reasons, it is also necessary to insist on the thorough application

[337] For completeness, it needs to be added that, if, for example, one-way hashing is used in signing based on biometrics, i.e. a certain numerical detail whose reverse reconstruction to biometric data (sample) is not possible is generated, this detail can no longer be considered as biometric and the use of such system may be admissible in certain cases even without a data subject's consent. For more details, see, for example, Opinion No. 1/2017 of the Office for Personal Data Protection – Biometric Identification or Authentication of Employees. In: *The Office for Personal Data Protection* [online]. 8. 6. 2017 [2017]. Available at: <https://www.uoou.cz/stanovisko-c-1-2017-biometricka-identifikace-nebo-autentizace-zamestnancu/d-23849>.

[338] Opinion No. 2/2014 of the Office for Personal Data Protection – Dynamic Biometric Signature pursuant to Personal Data Protection Act. In: *The Office for Personal Data Protection* [online]. 18. 7. 2014 [2017]. Available at: <https://www.uoou.cz/stanovisko-c-2-2014-dynamicky-biometricky-podpis-z-pohledu-zakona-o-ochrane-osobnich-udaju/d-11298>.

of all related legal and technological guarantees against the misuse of this sensitive data and on the simultaneous existence of a clear legal title (informed consent); all this with regard to the legal framework of public legislation and 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.[339]

3.4.2 Biometric Data in Health Applications

The "smart devices" for medical purposes are being increasingly used to assess the health condition of a user. The devices have a form of tokens, pendants or cloth. The device may be implanted even into a human body as a sensor regularly transmitting the data to a provider. Health applications are used by persons who intend to track their performance or physiological processes (i.e. Fitbit) or by patients with chronicle diseases (diabetes, hypertension, etc.). The providers of such applications process biometric data (heartbeat, blood pressure, glucose level or sleep habits) that are not intended to identify a data subject but to evaluate his or her health condition and behaviour. From the biometric data, the providers compile biometric profiles and subsequently on the basis of those profiles, as well as on the basis of data from selected medical studies, the application assesses the health of the users.

Since every user is unique and the biometric data can be influenced by many variable factors, the analysis performed by an algorithm may be inaccurate and the assessment of the health condition may be wrong. The incorrect assessment can be also a consequence of software faults or misinterpretation of medical staff who may believe in the objectivity of the device. The wrongful assessment may cause detriment to the user.

The application providers tend to exclude liability in their terms of use. This exclusion is questionable with regard to the European consumer law, especially to the unfair terms in consumer contracts and the liability for defective products. The injured person is required to prove the damage, the defect and the causal relationship between defect and damage. However, by "smart products" based on algorithmic assessment and machine learning capacity, it may be problematic or even impossible for the injured person to prove the defect of the product. In practice, the determination of the liable subject will be complicated, not only because of the uniqueness of an individual user but also due to an inconsistency of measured biometric data of the single user.

Besides the producer-customer relationship emerged from the liability, there are many other parties involved in the manufacturing and designing of the health applications. Those parties are authors of a medical study which is used as the source material for the health status evaluation, a software provider, or a provider of cloud-based analytics.

Another type of liability related to the health applications is the liability for the breach of data protection legislation and, as a corollary, the fundamental rights of the user. Even though the processed biometric data are not used for identification purposes, those data reveal the state of health of the user and thus they fall within the special category of data pursuant to Art. 9 of the GDPR. The GDPR stresses the risk-based approach. The risk for the data subject resides in the infringement of his or her fundamental rights, i.e. right to privacy or data protection.

[339] For more details of the issue of human rights with regard to biometrics see GÜTTLER, V. – MATEJKA, J. *K otázkám některých základních lidských práv a svobod v souvislosti* s právní *ochranou biometrických* údajů, p. 1055.

3.4.2.1 Biometric Data in Healthcare

Biometrics refers to the measurability since they focus on measurable physical and at the same time biological characteristics.[340] Mordini and Tzovaras distinguish first and second generation of biometrics. "Second generation biometrics progress from asking who you are (the focus of first generation biometrics) to asking how you are; they are less interested in permanent data relating to a pure identity, and more propelled by an individuals' relationship with their environment. What are your intentions and how do you manifest these?"[341]

The second generation of biometrics is capable of being used for elicit medical information and health status of an individual. The health status may be deduced from various biometric characteristics or by comparison of changes of one biometric feature. The medical information may be obtained overtly or even covertly without knowledge of the individual about the possible medical data retrieval.[342]

Based on first and second generation biometrics, we can make a distinction between biometric data on biometric data in a broader and a narrower sense. Biometric data in the broader sense are the output of a biometric-based system. These data do not necessarily identify individuals but show their behaviour, intention, status or physical condition. Biometric data in the narrower sense are data that allow identification of the person. Such biometric data is defined in Art. 4 (14) of the GDPR. Biometric data processed for the purpose of unique identification of a natural person are sensitive data pursuant to Art. 9 of the GDPR, or, according to the terminology of the regulation of specific categories of data.

If the data do not allow or confirm the unique identification of a person, this data will be personal, but not biometric in the narrower sense in the sense of GDPR. However, although the data that do not allow or confirm the unique identification are not a biometric data under GDPR, they are still personal data under Art. 4 (1) of this regulation since personal data is all information about an identified or identifiable natural person. Provided that the biometrical data in the broader sense refer to a health status of the individual, they fall within specific categories of data under GDPR.

There exist three types of healthcare applications. The first one focuses on a doctor – patient relation, the second one on personal motivation and self-tracking, and the third one on users or patients with specific needs. The first category of applications usually arranges a communication between the doctor and the patient. Those applications are e.g. *Medici* or *ZocDoc*. *Fitbit* and *Nokia health products* fall within the second category. As an example of the third category of applications can serve the applications for diabetes patients like *hedia* or *MedicSen*. ZocDoc states that it processes medical data and medical history data without further specification.[343] If the medical data includes data about biometric features of the users, we can speak about processing biometric data as well. Fitbit tracks personal habits and exercise of its user. The application collects data about food, weight, sleep, water and female health.[344] "Your device collects data to estimate a variety of metrics like the number of steps you take, your distance travelled, calories burned, weight, heart rate, sleep stages, active minutes and location."[345] Likewise, Nokia collects through its health products weight, height,

[340] MORDINI, E. – TZOVARAS, D. (eds). *Second Generation Biometrics: The Ethical, Legal and Social Context*, p. 7.
[341] Ibid., p. 11.
[342] MORDINI, E. – ASHTONS, H. The Transparent Body: Medical Information, Physical Privacy and Respect for Body Integrity. In: MORANDI, E. – TZOVARAS, D. *Second Generation Biometrics: The ethical, Legal and Social Context*, p. 259.
[343] Privacy Policy. In: *Zocdoc* [online]. [2018-08-16]. Available at: <https://www.zocdoc.com/about/privacypolicy/>, or Privacy & HIPAA. In: *Medici* [online]. [2018-08-16]. Available at: <https://medici.md/hipaa-privacy/>.
[344] FitBit Privacy Policy. In: *Fitbit* [online]. Available at: <https://www.fitbit.com/eu/legal/privacy-policy#info-we-collect>.
[345] Ibid.

muscle, body fat, heart rate, breathing rate, blood pressure and temperature of its user.[346] The third category of applications processes data relates to a particular disease. In the context of diabetes patients, the processed data refer to blood glucose value.[347]

On the basis of biometric data, the biometrical profiles may be compiled in order to determine the health status of the person or medical diagnosis.[348] The input information used for the profiles may originate from medical studies or/and from combination and comparison of data obtained from other users. The application provider does not usually have all data that are necessary for the determination of the health status of the individual at their disposal since the interpretation of the biometric data depends on the context, location and time of the collection. The existence of partial biometric profile requires generalisation and interpretation that need not be fitting to every individual who uses the application. Fitbit application uses the personal data to improve the accuracy of a daily exercise and activity statistics of its user as well as to track sleep patterns. The data are transferred to partners that provide Fitbit, Inc. among others with data analysis, research, and surveys.[349] For the same purposes are the biometric data shared with third parties by Nokia.[350]

3.4.2.2 Liability for Incorrect Results

The health application uses algorithms to assess and to interpret the processed data.[351] The feature of the biometric data of the second generation is that they may differ in context and time. If the application does not process all relevant data necessary for the assessment, the output won't reflect the real situation. In other words, the assessment of the algorithm does not need to reflect the actual physical condition or health status. Even though machine learning applications do not make a decision but rather provide data support for decision-making,[352] in case that the user of the application or the doctor regards the results as trustworthy, and acts according to the results, the user or the patient may be inflicted bodily harm. The same harmful consequence may be caused by a wrongfully chosen algorithm or incorrect evaluation of self-learning algorithm. Hazardous for the assessment of physical or health condition may be mistaking between causality and correlation when processing and evaluating the huge amount of data.[353]

Unlike products that are not based on the algorithmic assessment, the defective outputs are less probably to recognize due to the presumable objectivity of computer-based results.[354] The trust in the results may cause that the defect will be recognised until the damage emerges.

If the defective product causes the damage the injured person may claim damages for product liability. Pursuant to Art. 6 Directive 85/374/EEC on the approximation of the laws, regulations

[346] Your Privacy when Using Nokia Health Products and Services. In: *Nokia* [online]. [2018-08-16]. Available at: <https://health.nokia.com/cz/en/legal/privacy-policy-supplement>.

[347] Terms and conditions of web use. In: *Mediscan* [online]. [2018-08-16]. Available at: <https://www.medicsen.com/en/privacy_policy> or Terms and Conditions for your use of the Hedia Application. Available from: <http://hedia.dk/terms-and-conditions/>, or Terms and Conditions for your use of the Hedia Application. In: *Hedia.co* [online]. [2018-08-16]. Available at: <http://hedia.dk/terms-and-conditions/>.

[348] ANDRONIKOU, V. – YANNOPOULOS, A. – VARVARIGOU, T. Biometric Profiling: Opportunities and Risks. In: HILDEBRANDT, M. – SERGE, G. *Profiling the European Citizen. Cross-Disciplinary Perspectives*. Dordrecht: Springer, 2008, p. 132.

[349] FitBit Privacy Policy.

[350] Privacy Policy. In: *Nokia.com* [online]. Available at: <https://www.nokia.com/en_int/privacy>.

[351] STEWART, K. 10 Algorithms That Are Changing Healthcare. In: *University of Utah Health* [online]. Available at: <http://uofuhealth.utah.edu/innovation/blog/2015/10/10AlgorithmsChangingHealthCare.php>.

[352] HODSON, H. Google knows your ills. *New Scientist*. 2016, Vol. 230, No. 307, pp. 22–23, p. 23.

[353] MAYER-SCHÖNBERGER, V. – INGELSSON, E. Big Data and medicine: a big deal? *Journal of Internal Medicine*. 2018, Vol. 283, No. 5, p. 418–429. See p. 424.

[354] GILLESPIE, T. *The relevance of algorithms*. 2012. Available at: <http://www.tarletongillespie.org/essays/Gillespie – The Relevance of Algorithms.pdf>.

and administrative provisions of the Member States concerning liability for defective products (Product Liability Directive – hereinafter "PLD") a product is defective when it does not provide the safety which a person is entitled to expect, taking all circumstances into account, including the presentation of the product the use to which it could reasonably be expected that the product would be put, or the time when the product was put into circulation. The extra safety of the product is required by medical devices. According to the judgement of the Court of Justice of the European Union *Boston Scientific Medizintechnik* the safety which the public at large is entitled to expect, must be assessed by taking into account, inter alia, the intended purpose, the objective characteristics and properties of the product in question and the specific requirements of the group of users for whom the product is intended. When the medical device is used by patients in a vulnerable situation, the safety requirements for those devices which such patients are entitled to expect are particularly high.[355] Those safety requirements may be demanded in particular by health application intended for patients with an illness where an inaccuracy in the data assessment could be fatal.

The claim of product liability may not be successful in practice since the injured person is required to prove the damage, the defect and the causal relationship between defect and damage (Art. 4 of the PLD). For the injured person it is difficult if not impossible to prove the use of the inappropriate algorithm for the particular application or the wrong assessment of data. Even if the injured person proves the aforementioned, the manufacturer may allege non-liability on the grounds of a fact that the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered (Art. 7 e) of the PLD). Another problem with the current legal regulation of product liability resides in the self-learning algorithm and the damage caused by the product. Despite the fact that the liability regime laid down by the PLD is liability without fault, the question is whether the wrong assessment of the self-learning algorithm could be assessed as the defect. Provided that we come to a positive conclusion, the effective PLD would not apply as the manufacturer is pursuant to Art. 7 b) not liable for the damage if it is probable that the defect which caused the damage did not exist at the time when the product was put into circulation by him or that this defect came into being afterwards which is the case of self-learning algorithm.

Even though it is uneasy for the injured person to prove the defect of the product, providers of the health applications tend to exclude liability. "If you rely on any Fitbit Content or the Fitbit Service, you do so solely at your own risk. Our goal is to provide helpful and accurate information on the Fitbit Service, but we make no endorsement, representation, or warranty of any kind about any Fitbit Content, information, or services. The accuracy of the data collected and presented through the Fitbit Service is not intended to match that of medical devices or scientific measurement devices. [...] We are not responsible for the accuracy, reliability, availability, effectiveness, or correct use of information you receive through the Fitbit Service."[356]

"HealthTap is designed to support the health decisions and choices that you make. These decisions and choices are yours, and we believe that you are the best decision maker about your health and that these decisions should be made in connection with the advice you receive within a formal doctor-patient relationship. Always use common sense when making health decisions. HealthTap cannot make decisions for you. We can help you find good health information and, where available and appropriate, connect with doctors for care via HealthTap Prime or HealthTap Concierge or for in-person care."[357]

[355] Decision of the Court of Justice of the European Union from 5 March 2015 case no. C-503/13 and C-504/13 (Boston Scientific Medizintechnik).
[356] FitBit Terms of Service. In: *Fitbit* [online]. Available at: <https://www.fitbit.com/eu/legal/terms-of-service>.
[357] Terms of Use. In: *HealthTap.com* [online]. [2018-08-16]. Available at: <https://www.healthtap.com/terms>.

According to the PLD, the manufacturer may not limit the liability by any contractual clause. Pursuant to Art. 3 (1) of the Directive 93/13/EEC on unfair terms in consumer contracts,[358] a contractual term is regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer. The unfair contract term is not binding on the consumer. As the unfair contract term, it is regarded the exclusion or limitation of the legal liability of a seller or supplier in the event of the death of a consumer or personal injury to the latter resulting from an act or omission of that seller or supplier. Provided that the products are being offered or sold within the European Union, the manufacturer has to comply with the consumer protection legislation. Any exclusion or limitation of liability is null and void. However, such a disclaimer can discourage the consumer from claiming the damages.

The data generated by the algorithm may be misinterpreted by the user or by the doctor. In case that the outcome is misread by the user, he or she must face the consequences of the misinterpretation unless he or she had been misinformed or informed insufficiently.

In case that the health application is used by the doctor for diagnosis or treatment is the legal situation of the injured person regarding damages more favourable. The doctor or provider of healthcare will be liable for a thing used for the provision of service on the basis of the contract concluded with a doctor or healthcare service provider. Such liability is the strict liability without the existence of a fault on the side of the doctor. A subsequent recourse of the doctor healthcare towards the service provider will depend on the contract terms concluded between the application provider and the provider of healthcare services.

The recourse claim has also the provider of health application if it becomes apparent that the incorrect results of the algorithm are based on the erroneous medical study which the provider used as the source material for the evaluation of the data. In case that the provider of the health application engaged another party as a subcontractor (a software provider, or a provider of cloud-based analytics), the application provider has the recourse towards the aforementioned contracting party. The nature and extent of the recourse will depend on contractual terms.

3.4.2.3 Liability for Breach of Data Protection Legislation

The provider of the health application processes personal data. The provider who focuses the service directly on the consumers is the controller according to GDPR. If the application is offered and used by doctors, the provider will be in the position of the processor because the provider processes the personal data on behalf of the doctor who determines the purposes and means of the processing of personal data of his or her patients. Some obligations under GDPR are directed only to the controller, whereas others relate to the controller as well as the processor.

The provider of the application has to obey the European data protection legislation even if the provider is not established in a member state of the EU provided that data subjects are in the EU where the processing activities are related to the offering of goods or services to such data subjects in the EU or the monitoring of their behaviour as far as their behaviour takes place within the EU (Art. 3 of the GDPR). In case of the provider of the health application, both offering as well as monitoring of behaviour, will be present. When the provider is not established in the EU, the provider has to appoint a representative as a contact for data subjects and local data protection authorities (Art. 29 of the GDPR). The designated representative should be subject according to the Recital 80 to enforcement proceedings in the event of non-compliance by the controller.

[358] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.

Besides the designation of the representative in case of the controller who is not established in the EU GDPR laid down many obligations to the controller. Even though the data processed by the means of the application are not biometric data under the GDPR, the data still fall within the special categories of data relating to health. The controller who offers the application to the consumer has to process those data on the basis of explicit consent for a specific purpose (Art. 9 (2) a) of the GDPR). The explicit consent means an express statement of the consent.[359] When the application is focused on the medical professionals, the data are processed under Art. 9 (2) h) of the GDPR. It means that the processing is necessary for the purposes of medical diagnosis, the provision of health or social care or treatment on the basis of EU or member state law or pursuant to contract with a health professional and subject to the obligation of professional secrecy.

Some obligations of the controller are enumerated in Art. 5 of the GDPR. The controller has to process the personal data for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. The typical purposes of the health application are rendering a service to the consumer together with the marketing purposes. Another purpose of those application used by the consumers or doctors is a scientific research purpose. This purpose is not incompatible with the initial purposes provided that appropriate safeguards are taken to ensure the rights and freedoms of the data subject and the principle of data minimisation. The data must be accurate and must not be kept for a longer period of time than is necessary for the purposes again with the exception of the research purposes.

The controller has to ensure integrity and confidentiality of processing. Pursuant to Art. 32 of the GDPR the controller has to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk for rights and freedoms of the data subject. GDPR does not prescribe any obligatory measures to ensure the security of the processing. GDPR mentions some examples of possible security measures, besides other things pseudonymisation and encryption, the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services or the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident. The breach of confidentiality and integrity of the special categories of data relating to health can cause in particular a violation of the right to privacy and right not to be subject to discrimination on basis of the state of health. That is the reason why the provider of the application has to pay attention to the high level of risk and adjust the technical and organisational measures to the risk.

In the case of a personal data breach, the controller must according to Art. 33 of the GDPR without undue delay, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller must communicate the personal data breach also directly to the data subject. It is presumable that the breach of data relating to the health of numerous data subject will result in risk to aforementioned rights. For that reason, the provider of the health application should notify the breach to the supervisory authority as well as to the data subjects.[360]

Since the provider of the health application will process on a large scale of special categories of data and the processing of such data are the core activity, the provider is obliged to carry out a data protection impact assessment together with a designation of a data protection officer.

[359] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on consent under Regulation 2016/679*, p. 18.

[360] ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on Personal data breach notification under Regulation 2016/679. In: *European Data Protection Board* [online]. 2018 [2019-12-02]. Available at: <https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en>, p. 23.

In case that the provider of the application does not obey the GDPR the data subject may lodge a complaint with a supervisory authority (Art. 77 of the GDPR) and/or seek a judicial remedy against a controller or processor (Art. 79 of the GDPR). The data subjects have pursuant to Art. 82 of the GDPR the right to compensation for damage suffered arising in respect of both material and non-material damage. Data controllers are liable for damage caused by processing which infringes the GDPR. Data processors, are liable only where they have not complied with obligations specifically directed at them under the GDPR, or have acted outside of or contrary to lawful instructions from the data controller. A controller or processor can exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage. The liability for damage is a strict liability. The injured person does not need to prove the fault. On the other hand, he or she has to prove the damage caused by the violation of GDPR. The controller or processor releases from liability if only she proves an existence of an extraordinary reason that caused the damage.

The providers of the health applications assess the physical and health condition of the users. The providers face liability arising from erroneous assessment and from violation of data protection legislation. The assessment of the physical and health condition may be wrong due to incomplete data, wrong algorithm or incorrect evaluation of the self-learning algorithm. The user does not usually register a defect not until he or she suffers damage in particular damage to health. However, it is very complicated for the injured person to claim compensation for the defective product since it is up to him or her to prove the defect that is grounded in the inappropriate algorithm for the particular application or the wrong assessment of data.

The application provider processes the huge amount of biometric data. Those data are not the biometric data under GDPR, nevertheless, those data relate to health and fall under special categories of data. In case that the provider breaches the data protection legislation the provider faces not only administrative sanctions but also right of the data subject for compensation of material and immaterial damages.

3.4.3 Biometric Data and Neuromarketing[361]

The modern society is driven by profit and, therefore, develops new techniques in order to sell more goods as well as services. In order to achieve higher effectiveness in sales, companies employ specialized researchers examining an impact of various marketing strategies as well as particular advertisements on test subjects and later evaluate efficiency of their influence on a need of test subjects to choose a particular product over the others. Within the field of a marketing science, marketers started to utilize the knowledge produced based on monitoring of brain functioning. This trend is called “neuromarketing“.

Neuromarketing uses various monitoring techniques that either measure blood flow or electric activity in brain (for instance fMRI – functional magnetic resonance, QEEG – qualified electroencephalography, SST – steady-state topography) or techniques that indicate psychological or physiological arousal and changes in emotional responses of test subjects (for instance eye-tracking, galvanic skin response or facial coding).[362] With help of these techniques, test subjects are measured in order to establish what reaction a particular advertisement triggers. For instance, an emotional reaction or

[361] The following Section was published in KRAUSOVÁ, A. Neuromarketing from a Legal Perspective. *The Lawyer Quarterly.* 2017, Vol. 7, No. 1, pp. 40–49 [2019-12-10]. Available at: <https://tlq.ilaw.cas.cz/index.php/tlq/article/view/221>.

[362] VOORHEES, T. Jr. – SPIEGEL, D. L. – COOPER, D. Neuromarketing: Legal and Policy Issues. *A Covington White Paper* [online]. 2011 [2016-06-15]. Available at: <https://www.cov.com/files/upload/White_Paper_Neuromarketing_Legal_and_Policy_Issues.pdf >.

engagement have been proved as an efficient tool for either provoking irrational consumer behaviour or for creating a memory that can later help with unconscious selection of an advertised product.

From a social and legal point of view, such techniques of influencing people's brains are, however, quite controversial. Advocates of neuromarketing proclaim that the aim of neuromarketing is to understand clients and, therefore, serve them better.[363] Some authors also claim that knowledge published in books on neuromarketing actually helps customers to understand own decision-making patterns and subsequently allows them to understand whether they are being manipulated or simply influenced "for their own benefit".[364] Professional literature mentions that the current effectiveness of persuasion techniques based on neuroscientific knowledge cannot lead to manipulation of consumer behaviour.[365] At the same time, neuromarketing is envisioned as a great means for optimizing advertising messages in order for their content to influence a so called reptilian part of a human brain that "makes us extremely selfish and drives our strong preference for mental shortcuts over strong deliberations".[366] Opponents of neuromarketing understand using such techniques as an "effort to influence consumer decision-making at an unconscious level. In this regard, the techniques will inevitably be criticized as a tool for overriding or circumventing rational consumer choice by using powerful stimuli to provoke emotional responses to products."[367]

Both positive and negative criticism of neuromarketing draw attention to a very important social concept of personal autonomy. Personal autonomy refers to the capacity of an individual to decide about own actions and, among others, to make an autonomous choice. Compared to traditional methods of market research neuromarketing research methods have a greater potential to limit personal autonomy. Traditional methods of market research usually involve filling in a questionnaire by a test subject who is in fact limited only by their own sense of morality and free to decide whether to tell the truth or to deceive when being questioned. Moreover, a test subject can also decide unconsciously about not disclosing some information. Neuromarketing methods, on the other hand, circumvent the subject's decision process regarding the contents of information to be provided by monitoring real bodily reactions to certain stimuli and by interpreting these reactions independently with help of neuroscience. By doing so, these research methods can also potentially interfere with the right to privacy and with the existing data protection legislation.

Consequently, neuromarketing research methods need to be examined from two legal points of view: a) protection of personal autonomy, and b) protection of privacy. The following subchapters shall provide an overview of the relevant Czech legislation related to the problem of neuromarketing in the above mentioned contexts and shall also evaluate several strategies that natural persons could use for protection of their interests.

3.4.3.1 Personal Autonomy in the Context of the Czech Private Law

Personal autonomy is a broad and flexible concept whose meaning depends on a social context in which it is used. In general, two models of personal autonomy have been identified: a model of authenticity and a model of liberty. According to the model of authenticity "an autonomous person is a being who has his life in his own hands, acts rationally, consistently and independently and

[363] DOOLEY, R. *Brainfluence. 100 Ways to Persuade and Convince Consumers with Neuromarketing.* Hoboken: Wiley, 2012.
[364] RENVOISÉ, P. – MORIN, Ch. *Neuromarketing. Understanding the "Buy Buttons" in Your Customers Brain*. Nashville: Thomas Nelson, 2007, p. 10.
[365] MURPHY, E. – ILLES, J. – REINER, p. B. Neuroethics of Neuromarketing. *Journal of Consumer Behavior*. 2008, No. 7, pp. 293–302.
[366] MORIN, Ch. Neuromarketing: The New Science of Consumer Behavior. *Society*. 2011, Vol. 48, No. 2, pp. 131–135.
[367] VOORHEES, T. Jr. – SPIEGEL, D. L. – COOPER, D. *Neuromarketing: Legal and Policy Issues*.

is motivated by proper values and norms: he is able to control situations and to resist external power and hidden persuaders."[368] According to the model of liberty, on the other hand, "persons are supposed to be autonomous and this imposes a prima facie requirement that we should not control the choices and actions of others, except when they harm others."[369] As opposed to the model of liberty, the model of authenticity is more of a protective model that aims to provide safeguards to individuals whose autonomy in making decisions could be endangered for instance by their own irrational behaviour or a weak position in legal relationships. Traditionally, the model of authenticity is used by European countries with the tradition of civil law rather than by those with the tradition of common law.

Within the context of the Czech law, personal autonomy is defined in the Charter of Fundamental Rights and Freedoms[370] in Article 2 (3). According to this Article "[e]veryone may do that which is not prohibited by law; and nobody may be compelled to do that which is not imposed upon her by law". In the sphere of private law this principle has been defined in terms of autonomy of will and embodied into laws as a freedom of contract (or also as a freedom of legal transaction). The new Czech Civil Code of 2012[371] that has completely reformed the system of private law in the Czech Republic emphasizes the autonomy of will as its leading principle. Protecting the autonomy of will is considered as a necessary condition for ensuring the liberty to develop private life of an individual.[372] The autonomy of will is defined in § 1 (2) of the Civil Code as a right of persons to negotiate mutual rights and obligations notwithstanding the provisions of the Civil Code unless the Civil Code prohibits so specifically. The Civil Code prohibits contractual provisions that violate good manners, public order or rights related to personal status including rights to personal protection and privacy.

The interesting question that raises in this regard in the context of neuromarketing is to what extent the private law protects the autonomy of will of a potential buyer of products advertised with help of knowledge gained from neuromarketing research.

As already mentioned above, it is the aim of neuromarketing to create commercials that would appeal to basic human instincts and emotions as opposed to human intellect. However, the Civil Code protects one's own will especially with regard to their intellect. The Civil Code states that one could expect from any natural person who has a full capacity to make legal acts "to have intellect of an average person and an ability to use it with ordinary care and diligence."[373] From this perspective it may seem that despite promoting autonomy of will the law does not provide enough means to protect it against efficient techniques manipulating with basic instincts and emotions of a person.

On the other hand, one must take in account the full notion of personal autonomy which, apart from the right to act autonomously, also entails the obligation to act autonomously and be diligent. Although neuromarketing techniques may be considered as more efficient than other marketing techniques, it would be devastating for the whole society to see an average person as someone who is unable to manage their emotions and basic instincts when facing a possibly manipulative advertisement.

---

[368] RAES, K. Legal Moralism or Paternalism? Tolerance or Indifference? Egalitarian Justice and the Ethics of Equal Concern. In: ALLDRIDGE, P. – BRANTS, Ch. (eds). *Personal Autonomy, the Private Sphere and the Criminal Law. A Comparative Study.* Portland: Hart Publishing, 2001, p. 26.

[369] Ibid.

[370] Resolution of the Presidium of the Czech National Council of 16 December 1992 on the declaration of the CHARTER OF FUNDAMENTAL RIGHTS AND FREEDOMS as a part of the constitutional order of the Czech Republic. Available online in English at: <http://www.usoud.cz/fileadmin/user_upload/ustavni_soud_www/prilohy/Listina_English_version.pdf >.

[371] Act No. 89/2012 Coll., the Civil Code, as amended.

[372] Explanatory Memorandum to the Act No. 89/2012 of the Collection of Laws, Civil Code.

[373] See Article 4 (1) of the Civil Code.

Moreover, the purpose of private law is not to act in a patronizing manner but to allow persons to be active in making legal transactions and to take care of their own matters as they please compliant with an old principle of Roman law "vigilantibus iura scripta sunt". In this regard, the negligence to assess an advertisement in a rational manner represents a choice of an individual as well. Its consequences then need to be respected. However, in the context of marketing, the protection of autonomy of will is also regulated by specific provisions of public law that aim to protect consumers against unfair practices, such as misleading or aggressive commercial practices.

3.4.3.2 Protection of Autonomous Will in the Context of Neuromarketing Advertisement

In case a natural person would feel their will was manipulated by a neuromarketing advertisement, there are several strategies that such a person could use for their protection. The first strategy relates to challenging validity of a particular legal transaction with regard to the missing or mistaken will of a person. The second strategy utilizes provisions of public law related to unfair practice in advertising.

3.4.3.2.1 Challenging Validity of a Legal Transaction

In general, validity of a legal transaction depends on fulfilling certain requirements on a quality of a legal act. A legal act is defined in § 545 of the Civil Code and refers to an expression of will that aims to cause specific legal consequences. Will in this sense, is understood as "an inner psychological relationship of an acting person to the intended legal consequence".[374] According to § 551 of the Civil Code an act of a person cannot be considered as a legal act if will of a person to cause legal consequences is missing. The Czech doctrine specifies that will of an acting person is missing if the person formally performs an act without intending to do so, such as in the case of reflex movements, talking from sleep or when exposed to physical violence.[375] Law does not recognize legal consequences of such acts.

As opposed to missing will, the Czech legal doctrine also recognizes a situation in which will of a person has been deformed either by a mistake (§ 583 of the Civil Code) or by a threat of either physical or mental violence (§ 587 of the Civil Code). In these cases, an acting person whose will has been deformed can challenge validity of the respective legal transaction.

It is questionable whether either the objection of missing will or the objection of deformed will would be successful in challenging validity of a performed legal transaction. As an example, one can imagine a consumer who is exposed to an advertisement created based on neuroscientific knowledge which appeals to consumer's unconscious desires that she would never admit. The consumer buys the advertised product and later on she finds out that the advertisement was based on neuromarketing knowledge and might have influenced her decision process. Could she object that the transaction was made involuntarily?

From a legal perspective, the objection of missing will would be very hard to prove. The aim of neuromarketing is to persuade consumers in a more efficient way and, therefore, help them to make up their mind to buy products or services. If the will to buy is strong and long-lasting, the better for the producer as their return on investment in advertising becomes higher. Although neuromarketing techniques may compel a consumer to buy a product because specific emotions

[374] LAVICKÝ, P. et al. *Občanský zákoník I. Obecná část (§ 1−654). Komentář.* Prague: C. H. Beck, 2014, p. 1967.
[375] LAVICKÝ, P. et al. *Občanský zákoník I. Obecná část (§ 1−654). Komentář.*

are triggered, the will itself has been formed and exercised. Whether it has been deformed is another case.

Deforming somebody's will is a concept that requires a closer inspection. Deforming somebody's will must be strictly distinguished from persuading someone to do something. Persuasion, arguments and advertisements are a common part of social life. People share their opinions, try to promote them and find support of others. In this sense many persuasion techniques are being used, including rational arguments and manipulation with feelings. However, any average person exposed to persuasion usually has a chance to mentally process pros and cons of a possible decision and form her will accordingly to her values and goals. Persuasion is an inevitable part of life and in fact stimulates the decision process.

Deformation of will, on the other hand, happens in situations when someone manipulates a decision process of a person by providing false information, not providing certain information on purpose or by presenting very negative consequences for that person if she would not form her will in accordance with what has been suggested to her. These situations are characteristic with a high degree of vulnerability of a person who is forced to use limited resources when making a decision. Her ability to make a conscious decision is controlled. A similar situation happens if a person is exposed to an efficient technique that by using an appropriate symbol triggers an affective rather than cognitive response. In that case a person is often unable to use all mental resources to form their will freely. Professional literature states that "[e]ven if consumers are made aware of the affective response, it is very difficult for them to override the affective influence with cognitive reasoning. The authors speculate that cognitive processes may not be able to finalize a decision without a ''go/no go'' message from an affective function of the brain."[376]

Triggering a mental process that circumvents conscious mind and prevents a person to form their will with utilizing their intellectual capacity needs to be in this sense considered as deforming one's own will. However, since a person is neither mistaken (provided with false or misleading information) nor threatened with violence, she cannot invoke either of the two provisions of the Civil Code (§ 583 and § 587) and object invalidity of a transaction. The only objection such a person can make is to claim that the content of the respective legal transaction contravenes both the law as well as good manners and, therefore, the transaction must be considered invalid.

Limiting autonomy of will by its deforming definitely violates the fundamental principle of the Civil Code as well as the notion of good manners in the society. However, ultimately it will be the courts that will decide how the problem of neuromarketing should be approached in the future. The courts will most likely do so based on expert opinions on various techniques in individual cases.

3.4.3.2.2 Unfair Practice in Advertising

Neuromarketing and marketing in general are activities associated with advertising. Marketing, however, needs to be understood in a broader sense than simple advertising which, in fact, represents only the result of a marketing process. Marketing involves many activities such as market research, creating a product, testing its popularity, finding out preferences of clients, determining the right pricing scheme, defining strategies of promoting a product as well as creating an efficient advertisement.

[376] WILSON, R. M. – GAINES, J. – HILL, R. P. Neuromarketing and Consumer Free Will. *The Journal of Consumer Affairs*. 2008, Vol. 42, No. 3, pp. 389–410.

As opposed to marketing, advertising is strongly regulated by means of public law. In the Czech Republic, all advertisements need to comply with the Act of 9 February 1995 No. 40/1995 of the Collection of Laws, on Regulation of Advertising, as amended (herein after only Act on Regulation of Advertising).

According to § 1 (2) "advertising means announcement, demonstration or other presentation disseminated particularly with communication media that aims at promoting entrepreneurial activity, and in particular supports the consumption or sale of goods, construction, lease or sale of property, sale or use of rights or obligations, supports the provision of services or promotion of a trademark, unless stated otherwise".

Unfair commercial practice in advertising is prohibited in § 2 (1) b) of this Act. Ordering someone to create an unfair advertisement, delivering an unfair advertisement as well as its dissemination is punishable according to § 8a of the Act on Regulation of Advertising as an administrative offence with fine up to 5.000.000 CZK.

The definition of what is understood as unfair commercial practice can be found in the Act of 16 December 1992 No. 634/1992 of the Collection of Laws, on Consumer Protection, as amended (hereinafter Act on Consumer Protection).

According to § 4 (1) of the Act on Consumer Protection "a commercial practice is unfair if it is contrary to the requirements of professional diligence and substantially distorts or is able to substantially distort economic behaviour of consumers to whom it is addressed or who are exposed to influence of this practice, in relation to a product or a service." Professional diligence in this sense refers, among others, to fairness and general principles of good faith of consumers (§ 2 (1) letter p) of the same Act).

A key term with regard to advertisements based on neuromarketing is the "ability to distort economic behaviour of consumers". In case of a dispute over the ability of an advertisement to distort economic behaviour, the accused person needs to prove that the respective advertisement does not have such ability. At the same time, law requires from an average consumer to stay reasonably alert and cautious.[377]

The criterion for deciding about lawfulness or unlawfulness of an advertisement based on neuromarketing is its potential to distort behaviour, not the ability to influence a decision process of a consumer. Former version of the Act on Consumer Protection that was in force until 27 December 2015 stated in § 4 (1) that "a commercial practice is unfair if acting of an entrepreneur towards a consumer is contrary to the requirements of professional diligence and is able to substantially influence decision process of a consumer so the consumer can make a commercial decision that they would not otherwise make."

Since 28 December 2015 it has been more difficult to classify certain practices as unfair and, therefore, prohibited. Ability to substantially influence a decision process can be understood as an easier condition to fulfil as a decision process is internal, hidden and much more questionable compared to objectively perceivable behaviour of a person. Nevertheless, the border between these two concepts is not crystal clear and can be challenged.

Unlawfulness of a certain advertisement then depends on effects that neuromarketing techniques would have on consumer's behaviour. These effect can, however, vary greatly. Therefore, each case

[377] See Explanatory Memorandum to the Act of 9 December 2015 No. 378/2015 of the Collection of Laws on Amendment of the Act No. 634/1992 of the Collection of Laws on Consumer Protection, as amended.

will need to be assessed individually. Again, as in case of objecting validity of legal transaction made under influence of neuromarketing techniques, the courts will need to request expert opinions to evaluate possible effects. Right now, any specific results of such cases cannot be predicted. However, one can presume that given the rapid developments in this field and growing utilization of neuromarketing techniques a legislator will need to react soon and set up rules that would ensure efficient protection of consumers.

3.4.3.3 Neuromarketing and Privacy Protection

Neuromarketing practices are based on processing of data collected from research subjects based on monitoring their brain functioning. The data refers to specific neurological processes and is unique to individuals. As such it fulfils the definition of biometric data.

Biometric data is deemed to be special and different from other types of personal data due to its specific nature allowing unique identification of individuals.[378] This data has a character of an identifier which represents information itself as well as an identifying element linking the information with a particular individual. From the privacy point of view information value of biometric data implies higher vulnerability of subjects to whom the biometric data pertains.

In the context of neuromarketing, biometric data collected from research subjects are analysed in order to derive general principles of brain functioning that can be later used for designing an efficient advertisement. For instance, based on brain monitoring of test subjects, researchers were able to establish that if a brand refers to cultural meanings, memory of a person is activated and this person, therefore, tends to make a biased decision with regard to those relevant cultural meanings.[379]

Personal data protection legislation, however, protects only data that refer to a particular identified or identifiable person. Research test subjects usually need to provide explicit consent with monitoring their brain. On the other hand, privacy in the terms of processing biometric data of customers is not violated when people are exposed to techniques of influencing mental processes based on generalized principles. From this point of view there appears to be no problem. However, as the relevant legislation was not adopted taking in account advances in mental imaging, its application may result in negative consequences in the society.

The notion of privacy has been defined in many ways, while the most famous definition refers to privacy as to “the right to be alone”. Generally speaking, one can consider right to privacy as the right to be protected against unlawful intrusion in own personal space, be it person’s house, communication, body or mind. In terms of mind, privacy should be examined on two levels – privacy of contents (stored memories, formed attitudes and decisions) and privacy of processes (thinking, remembering, etc.).

Such as the society protects privacy of a household by prohibiting others to inspect what a person owns (privacy of contents) or what she does behind the walls of her house (privacy of process), this notion should be extended also to mind. However, more than anywhere else, in the mind, its contents depend strongly (if not completely) on mental processes. Therefore, if we accept a premise that human brains function the same way, the knowledge of mental processes and ways of their influencing and modification represents the key to the mechanism that, in fact, defines not only mental

[378] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Working document on biometrics*.
[379] MATTHEWS, S. Neuromarketing: What Is It and Is It a Threat to Privacy? In: CLAUSEN, J. – LEVY, N. (eds). *Handbook of Neuroethics.* Dordrecht: Springer, 2015.

privacy of a person, but other forms of privacy as well. As privacy is a concept that presupposes control of a person over what she wishes to keep secret and what to reveal in public, influencing mental processes of a person may also result in changing her understanding of what she needs to keep private.

Concerns about utilization of knowledge related to mental processes have been expressed already by many prominent scholars.[380] Unfortunately, absence of legislation providing clear guidelines for processing mental biometric data does not allow for efficient privacy protection. Unfortunately, the very nature of neuromarketing research currently renders privacy claims inapplicable.

Neuromarketing is one of the emerging fields that give rise to completely new problems in the society. These problems help us to explore and redefine existing concepts of social organization and recognized values. A possibility to efficiently influence people's behaviour through knowledge of their brain functioning opens the door to previously sacred space of mind. Neuromarketing techniques are designed to influence mental processes that, in fact, themselves define contents of mind as well as individual notions of privacy. However, although neuromarketing techniques in reality interfere with privacy of a person, the existing data protection legislation cannot be utilized for individual's protection against interference with privacy based on generalized principles. The only manner in which a person can claim her rights is by referring to the fundamental right of privacy that is formulated in a general manner and is subject to interpretation. Moreover, with respect to protection against neuromarketing techniques, one can also refer to provisions related to protection of autonomous will that are set out either in the Civil Code or in the Act on Regulation of Advertising. Predicting results of such claims at court is nearly impossible. However, courts should clearly express preference for protection of individual autonomy and privacy rather than economic interests of business companies.

The reason for preference of individual's protection of autonomous will and privacy over interests of business companies lies in the increasing body of knowledge related to brain functioning and a fast pace of developments of analytical methods. Business companies have strong economic interests and highly efficient tools on how to achieve their goals compared to individuals who have not yet had a chance to learn appropriate strategies on how to react to new challenges. The law needs to recognize this need as well as the asymmetry in the business to consumer relationship. For instance, subliminal advertising is one of methods that can efficiently influence person's decision process on a subconscious level without being perceived by this person. As such, this practice had been prohibited in the Czech law until 16 August 2015. Unfortunately, this specific provision was left out of the Act on Regulation of Advertising as the Czech legislators deemed that this provision does not comply with the European Directive 2005/29/EC; so called "Unfair Commercial Practices Directive".[381] In the future, the law should return to specification of methods that circumvent conscious mind and set up clear borders and guidelines on how to determine which practices are allowed and which are prohibited. This will certainly contribute to higher legal certainty and, therefore, not only to the protection of individuals but also to protection of business companies' interests in safe investments into marketing. The same specification should be done in the area of privacy protection as the relationship between generalized principles on brain functioning and individual brain functioning are strongly correlated.

[380] THE COMMITTEE ON SCIENCE AND LAW. Are Your Thoughts Your Own?: "Neuroprivacy" and the Legal Implications of Brain Imaging. In: *New York City Bar* [online]. 2005 [2019-12-15]. Available at: <https://www.nycbar.org/pdf/report/Neuroprivacy-revisions.pdf>.

[381] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (Text with EEA relevance).

3.4.4 Biometric Data and Profiling for the Purpose of Criminal Proceedings and Implications for Human Rights[382]

At present, analytical works of all kinds are carried out on computers which use sophisticated algorithms. As the result we have a situation where these algorithms either in part or in full perform a variety of tasks previously carried out by people.[383] Norbert Wiener, the founder of cybernetics, talks about this type of mechanisation as the type which has replaced human decision making. This notwithstanding, Wiener did not expected that complex decision making made by humans, involving many variables, could be replaced by mechanised decision making,[384] but the opposite has turned out to be the truth, as mechanised decision making is present in all kinds of areas of our everyday life.[385]

Algorithms are used, among other tasks, for categorisation of culprits concerning their potential recidivism. Culprits are categorised based on their actual or presumed psychological traits derived from their previous behaviour, and from other data available about them. According to WP29, profiles of culprits based on psychological traits are biometric personal data.[386] These are the so called second generation biometric data, where the goal of processing these data is not only to identify the person, but also to read this person's mind.[387] The culprit's profile which focuses on predicting his future criminogenic behaviour, is in this sense the so called behavioural biometric profile.[388] This behavioural biometric profile comprises both non-biometric data (address, age, education), and biometric data (the culprit's psychological features).[389]

Using algorithms in the decision making process in criminal proceedings is not a mere theory. This type of decision making is at present already used for determining the length of imprisonment, in deciding whether the defendant is to be given a suspended or unsuspended sentence of imprisonment, and in deciding whether the prisoner should be paroled.[390] The reason why algorithms are used in decision making in these cases may be the endeavour for precise and objective adjudication free of prejudices and biases, which are intrinsic to humans.[391] According to Kate Crawford, as algorithm is often meant a computing tool which autocratically decides on the basis of variables, and which creates a single output. As the result, these outputs are regarded as rational and free of any subjective notions and requirements.[392]

---

[382] This text was published in an extended version in FIALOVÁ, E. Využití algoritmů při profilování v trestním řízení a důsledky pro lidská práva. *Časopis pro právní vědu a praxi* [online]. 2018, no. 2, p. 229–258. [2019-12-16]. Available at: <https://journals.muni.cz/cpvp/article/view/8819>.

[383] STEINER, Ch. *Automate This. How Algorithms Came to Rule Our World*. London: Penguin Books, 2012., p. 11.

[384] WIENER, N. *The Human Use of Human Beings: cybernetics and society*. London: Free Association Books, 1989, p. 159.

[385] STEINER, Ch. *Automate This. How Algorithms Came to Rule Our World*, p. 41.

[386] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 3/2012 on developments in biometric technologies*, p. 4.

[387] DE HERT, P. Biometrics and the Challenge to Human Rights in Europe. In: CAMPISI, p. (ed). *Security and Privacy in Biometrics*, p. 406.

[388] YANNOPOULOS, A. – ANDRONIKOU, V. – VARVARIGOU, T. Behavioural Biometric Profiling and Ambient Intelligence. In: HILDEBRANDT, M. – SERGE, G. *Profiling the European Citizen. Cross-Disciplinary Perspectives*, p. 90.

[389] Administrative Office of the United States Courts Office of Probation and Pretrial Services. An Overview of the Federal Post Conviction Risk Assessment. In: *Uscourts* [online]. 2011. Available at: <www.uscourts.gov/file/2749/download>.

[390] See ROUVROY, A. L'algorithme n'est «pas un système de prédiction mais d'intervention». In: *Medipart* [online]. 2015 [2016-04-30]. Available at: <https://www.academia.edu/12603930/Lalgorithme_nest_pas_un_système_de_prédiction_mais_d_intervention_Entretien_réalisé_par_Jérôme_Hourdeaux_pour_Mediapart_25_mai_2015>, or CRAWFORD, K. Can an Algorithm be Agonistic? Ten Scenes from Life in Calculated Publics. *Science, Technology, & Human Values*. 2016, Vol. 41, No. 1, pp. 77–92. [2019-12-15]. Available at: <https://journals.sagepub.com/doi/abs/10.1177/0162243915589635 >.

[391] ROTH, A. Trial by Machine. Georgetown Law Journal. 2016, Vol. 104, No. 5, p. 6 [2016-04-30]. Available from: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2743800>.

[392] CRAWFORD, K. *Can an Algorithm be Agonistic? Ten Scenes from Life in Calculated Publics*.

3.4.4.1 Algorithmic decision making in criminal proceedings

3.4.4.1.1 Algorithmic decision making and application of law

According to Own Fiss, the corner stone of court power is a process for conducting of which are nominated judges who interpret the texts of legislative regulations. Fiss distinguishes between two aspects of a court process. The first of these is independence. He sees the other aspect in the judge's obligation to hear the proceedings participants. But according to Fiss, this aspect of the court system is in danger, because the court process has been bureaucratised.[393] "It is the judge's obligation to engage in a special dialogue, namely to hear all complaints, to hear all persons affected and to give the reasons for his ruling. By signing the verdict of the judge's opinion, the judge reassures the proceedings participants that he was fully engaged in the process and that he accepts an individual responsibility for his ruling. We accept the court authority under these conditions, and therefore its bureaucratisation evokes concerns that the judge's signature is a mere fraud, and that judges conduct their duties without being really engaged in the dialogue from which their authority arises."[394]

In court ruling made on the basis of an algorithm alone, there is no need to hear the proceedings participants or witnesses. The judge has no reason to show an interest in individual circumstances of the particular case, because the algorithm works exclusively with predefined values. For the judge all he has to do, and has no other alternative, is to enter certain values to the system which, albeit being characteristic for the given case, are limited to the predefined categories only. The case's individual aspects which cannot be assigned to any of the predefined categories, are in the decision making omitted.

The Czech criminal code contains many provisions which make it mandatory for the court to consider the circumstances of the particular case, to assess whether conditions exist for certain laws to be applied, and how the law is to be interpreted and applied. The impossibility for algorithmic adjudication to take into consideration individual circumstances might, as the result, lead to the violation of the fundamental principles of the Criminal Code. One of the most important principles of the Criminal Code is subsidiarity of criminal repression and the principle *ultima ratio* of the Criminal Code expressed in Article 12 paragraph 2 of Act no. 40/2009, the Criminal Code. According to this provision, the culprit may be held criminally liable and bear the legal consequences associated with this criminal liability only in cases which are harmful to the society, and where applying liability according to other laws will not suffice. When general courts fail to apply the principle of subsidiarity of criminal repression in line with the judicature of the Constitutional Court even though the factual circumstances show that the conditions for it have been met, in the opinion of this Court they violate the constitutional principle *nullum crimen, nulla poena sine lege*, which is embedded in clause 39 of the Charter of Fundamental Rights and Freedoms ("Charter").[395] Unless a particular offence has the symptoms of necessary harmfulness, criminal liability cannot be derived from committing this offence alone, even if it has all formal attributes of *Actus Reus* of a criminal act.[396] A prerequisite for societal harmfulness is the so called material corrective in relation to the formal attributes of *Actus Reus* of the criminal act committed. Another provision, in which the lawmaker has left a leeway for the law enforcement authorities to consider the circumstances of a particular case, is the provision in the Criminal Code concerning sentencing. Pursuant to Article 39 paragraph 1 of the Criminal Code, when

[393] FISS, O. M. *The Bureaucratization of the Judiciary.* Faculty Scholarship Series. Paper 1216. 1983, pp. 1442–1468 [2016-04-30]. Available at: <http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=2205&context=fss_papers>. See p. 1443.
[394] Ibid.
[395] Decision of the Constitutional Court of the Czech Republic, 29 April 2014, no. I. ÚS 3113/13.
[396] See Decision of the Municipal Court in Prague, 21 September 2011, no. 7 To 251/2011.

determining a sentence and its length, the court shall take into account the nature and seriousness of the committed criminal offence, the personal, family, financial and other the culprit's situation and his hitherto way of life, and the potential for his correction. The court shall regard as an aggravating circumstance especially the situation when the culprit has committed the criminal offence for greed, as a revenge, due to nationalist, race, ethnic, religious, class or other similar hatred, or due to some other contemptible motives (Article 42 letter b) of the Criminal Code), or if committed the criminal offence by a brutal or tormenting way (Article 42 letter c) of the Criminal Code).

Another institute through which courts can take into account concrete circumstances of the case is the decision not to impose any punishment pursuant to Article 46 of the Criminal Code. The court may decide not to punish a culprit who has committed a misdemeanour but regrets having committing it, and who has expressed the will for effective correction, and when judging from the culprit's hitherto life, it can be justifiable expected that mere dealing with the matter will be a sufficient deterrent and incentive for his correction, and hence protection of the society.

The case's specific circumstances play a role in the state prosecutor's decision to discontinue the culprit's criminal prosecution pursuant to Article 172 paragraph 2 of Act no. 141/1961, the Criminal Order. One of the facultative reasons named in this provision under letter c) is also discontinuing criminal prosecution if due to the importance and degree of the violation or the hazard posed to the public interests which have been affected, the way the offence has been committed and its consequences, or the circumstances under which the offence has been committed, and in view of the defendant's behaviour, especially his will to pay for he damages caused or to rectify other harmful consequences of his offence, it is apparent that the objective of the criminal prosecution has been achieved. In such case the discretionary authority of the state prosecutor is applied.

When using an algorithm, the judge does not rule on the basis of the case's concrete circumstances, but on the basis of profiling, which works with biometric data and other data and information applicable at the time the algorithm was developed. The algorithm works with a set of attributes characterising the culprit and his behaviour which have been acquired in the past, and arrives from them at a conclusion about the culprit's person at the time of the adjudication. Although at the time the software for assessing the defendant's degree of risk was developed the relationship between high and low degree of risk might have been valid, at the time of adjudication this relationship may in reality not exist.

When using algorithmic adjudication, judges become persons who merely sign the outcome generated by the algorithm, rather than persons who in the process of law enforcement interpret these laws based on the case's concrete circumstances. Although formally the authority to conduct the process and to make decisions should belong to judges, in reality "their" adjudication depends on the outcome produced by the algorithm. Should judges fail to respect this outcome, they would face responsibility for their decision, and this responsibility may evoke in the judges the so called *chilling effect* to the detriment of their own judgement.

The judge should also assess each defendant according to his individual characteristics, and in order to assess the degree of risk of recidivism, assign to each characteristic a different weight. For example, a similar social status can be in one case significant for assessing the defendant's degree of risk from the recidivism point of view, but in another case the defendant's social status may be for assessing the degree of his potential recidivism irrelevant. Algorithms which the software applications for assessing the degree of risk use, may not necessarily work with predefined values. These algorithms may have the form of algorithms with a teaching function, which select facts relevant for the outcome based on previous experience. When generating its outcome, the algorithm might start to accentuate some of the input values and disregard others, even though these values might in the

particular case be significant for the decision making. And alternatively, the algorithm may add input values if its previous experience shows a relationship between them and the defendant's degree of risk. However, this relationship does not have to be at the induction level but at the level of correlation, which does not imply causality. Thus the presence of certain characteristics of culprits with the past history of recidivism does not mean that all culprits with this characteristic will have an increased risk of recidivism.

The fact that the decisions are made based on an algorithm is usually not disclosed to the persons in respect of whom the decision is being made, and these persons do not know the values on the basis of which the algorithm has generated its outcome. In this kind of adjudication a big problem is transparency, i.e. the awareness of how the decision has been arrived at.[397] Even those who use the algorithm often do not know on the basis of what processes and values the algorithm decides. This applies especially to algorithms with a teaching function, which change in the course of time. The users are not only unaware how these automated processes function, but do not notice either that the automated process has defects and hence is incorrect. The failure to see that the algorithm is incorrect is also due to the fact that users trust the algorithmic adjudication. *"Their trust in the software is so strong that they do not take into consideration any other sources of information, including their own inner feeling."*[398] In court proceedings in which algorithmic adjudication is only recommended but is not mandatory, a situation may occur when, while the user has decided not to respect the outcome generated by the algorithm, he might be held accountable for potential consequences of not respecting the algorithmic outcome.

3.4.4.1.2 Actuarial justice

Court adjudication in criminal proceedings based on an actuarial model for determining probability is called actuarial justice. Algorithms[399] are used to determine probability. In criminal proceedings, actuarial justice is used in the United States to assess the risk associated with the defendant or convicted person and his potential recidivism to commit criminal acts. The Approbation and Pre-trial Service of the Administrative Section of the United States Courts compiled a *Federal Post Conviction Risk Assessment*.[400] The risk assessment includes data of the culprit's criminal past, his education and work experience, social status, housing and financial situation.[401] The part dealing with the actual assessment of the culprit as part of the *Federal Conviction Risk Assessment* is filed in the *Psychological Inventory of Criminal Thinking Styles*. After entering appropriate values into the system, the system's user is presented with an outcome generated by an algorithm which shows the assessed person's criminal thinking. After all values have been entered into the system, the output comprises results which define the person's risk category and his criminogenic needs, i.e. the risk factors and reaction factors. The overall risk is obtained by adding together all the points scored, and the assessed person is categorised as a culprit whose risk is either low, or low-to-medium, or medium or high.

The *Federal Conviction Risk Assessment* also deals with the issue when the system's users can, in their assessment of risks associated with a particular culprit, differ from the risk determined by the algorithm, and not have to respect it. The result generated by the algorithm can be disrespected

[397] HANNAH-MOFFAT, K. Actuarial Sentencing: An "Unsettled" Proposition. *Justice Quarterly*. 2013, Vol. 30, No. 2, pp. 270–296, p. 284, or BRUNTON, F. – NISSENBAUM, H. Vernacular resistance to data collection and analysis: A political theory of obfuscation. *First Monday*. 2011, Vol. 16, No. 5, pp. 1–10 [2019-12-15]. Available at: <http://firstmonday.org/article/view/3493/2955>.

[398] STEINER, Ch. *Automate This. How Algorithms Came to Rule Our World*, p. 41.

[399] Ibid.

[400] ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS OFFICE OF PROBATION AND PRETRIAL SERVICES. *An Overview of the Federal Post Conviction Risk Assessment*.

[401] Ibid., p. 10.

in exceptionally cases and in certain categories only, such as culprits who have committed sexual criminal offences, culprits who have repeatedly used violence, culprits with a serious mental disorder, juveniles and culprits with an extensive criminal history. It is permissible to deviate from the degree of risk generated by an algorithm also on other grounds. However, this deviation must be justified and requires the superior's approval.[402]

Actuarial models are also used by juvenile courts. When assessing the risk of the development of criminal behaviour of juveniles, used are for instance *Risk Assessment Instruments*[403] or an instrument developed by a company called Algorhythm, which is applied to assess the risks of recidivism in juvenile culprits in the State of Florida.[404]

Actuarial models for assessing the degree of risk of culprits are used in Europe, too, for example in Belgium, France and the Netherlands.[405] In the Netherlands, actuarial models are mandatory for assessing the risk of recidivism of juvenile culprits[406] and of culprits who have committed serious criminal offences and those who have committed a criminal offence when suffering a mental disorder (the so called *tbs-gestelde*).[407] In the Czech Republic, algorithmic adjudication in criminal proceedings is not used, and the survey conducted by the authoress has showed that Czech judges have no awareness of algorithmic adjudication.

3.4.4.1.3 Critique of the actuarial justice

Sonja Starr, an opponent of the actuarial method of assessing the degree of risk of culprits in respect of their potential recidivism, admits that judges have always been assessing the culprits' risk of potential future recidivism. But of course it has been done informally, without any concrete values which the judges had to take into consideration in their decision making. In this respect actuarial methods might be more accurate in their predictions. According to Starr, the problem is not assessing the risk of recidivism per se. The risk assessment is based on demographic and social and economic factors, i.e. on factors over which the culprit has no influence. Starr suggest that instead of these criteria for assessing the risk of recidivism, used are factors which the culprit can influence or might be able to influence in the future, among others also his past behaviour and his behaviour at the time of the court adjudication process.[408]

Towards the end of the twentieth century, Jonathan Simon and Malcolm Feeley pointed out at the changes taking place in the attitude towards sentencing and how the objective of punishment is perceived. According to Jonathan Simon and Malcolm Feeley, the pivotal element of the new discourse is substituting the process of assessing culprits based on their moral features individually established for each of them, with a mathematical language based on the computation of probability and on statistical elements and formulae derived from the behaviour of other culprits, not those

[402] Ibid., p. 13.
[403] BAIRD, Ch. et al. A Comparison of Risk Assessment Instruments in Juvenile Justice. In: *NCJRS* [online]. 2013 [2019-12-17]. Available at: <https://www.ncjrs.gov/pdffiles1/ojjdp/grants/244477.pdf>.
[404] KATHLEEN, H. Florida takes aim at juvenile recidivism with predictive analytics. In: *GCN* [online]. 31. 7. 2015 [2016-05-14]. Available at: <https://gcn.com/articles/2015/07/31/juvenile-predictive-analytics.aspx>.
[405] MARY, P. Pénalité et gestion des risques: versune justice « actuarielle » en Europe? *Déviance et Société*. 2001, Vol. 25, no. 1, pp. 33–51 [2019-12-15]. Available at: <https://www.cairn.info/revue-deviance-et-societe-2001-1-page-33.htm>. See p. 44
[406] PLAISIER, J. – VAN DITZHUIJZEN, J. Risico taxatie bij verlof van gedetineerden. Een (inter)nationale vergelijking van instrumenten en procedures. In: *Impact R&D* [online]. 2008 [2016-05-14]. Available at: <http://mpct.eu/wp-content/uploads/downloads/2013/03/Risicotaxatie-Verlof-Gedetineerden-1556_volledige_tekst_tcm44-167941-1.pdf>.
[407] Ibid., p. 56.
[408] STARR, S. Sentencing, by the Numbers. In: *The New York Times* [online]. 10. 8. 2014 [2016-05-31]. Available at: <http://repository.law.umich.edu/law_econ_current/90>.

against whom the prosecution has been instituted.[409] "New penology is not about punishment or re-socialisation of individuals. It is about identifying and controlling asocial groups. By its rationality it does not focus on the behaviour of individuals or even on community organising, but on managerial processes. Its objective is not to eradicate criminal activities, but rather to make them tolerated through a systemic coordination."[410] According to Bernard Harcourt, "actuarial methods in criminal law use statistical forecasts about the criminality of groups or about group characteristics, to determine the outcomes of criminal proceedings concerning concrete individuals belonging to these groups."[411] Using actuarial models in sentencing or in making a decision whether to grant a parole, focuses on predicting potential future criminal behaviour, on the basis of which the culprit can be sentenced to imprisonment of a certain length, or making a decision whether the prisoner is to be paroled or kept in prison to serve the rest of his sentence.[412] Harcourt subjects these actuarial models in the area of court adjudication to a critique. Harcourt claims that fair sentencing cannot be based on the risk that the culprit will again commit criminal offences sometime in the future.[413] The actuarial methods are based on group profiling. When judges use these methods, they get an impression that it is justifiable to punish the members of a particular group in a certain way, by sentencing them to an imprisonment of a certain length, because it is the members of this group who commit criminal offences more often than members of a different group. The legitimacy of the imposed punishment will not be based on the character of the criminal offence committed, but on the potential future criminal activity predicted by the algorithm based on the profile of a member of a particular group.[414]

According to Harcourt, actuarial methods create a social reality by accentuating the correlation between the characteristics of a certain group and criminality. The culprit which in the model shows a higher risk of recidivism is stigmatised by the profile which categorises him as a member of this group, and hence attributes future criminal behaviour to him. As the result this culprit faces, after being released to normal life, a more difficult situation, which in turn leads to a higher probability of recidivism.[415] This vicious circle is not the result of using actuarial methods in criminal proceedings. Actuarial methods used by the criminal law enforcement authorities have given their blessing to this approach, and made it an official part of the criminal law policy. What more, deviating from the outcome generated by the algorithm is conditioned by certain additional criteria being met.

These aspects of using actuarial methods in criminal court proceedings are in contradiction to the principle of the ban on discrimination and the right to a fair trial. The risk of discrimination is also linked to the processing of biometric personal data of second generation. Incorrect categorisation of an individual of a certain behavioural biometric profile, based on his real or psychological traits, may lead to his future discrimination.[416] In contradiction to the principle of the ban of discrimination is also the case when defendants or convicts in criminal proceedings are treated differently on the grounds of their race, membership to a particular ethnic group, gender or social status. Although the currently used systems for assessing the degree of risk of the culprit's recidivism do not contain biometric data about his race as one of the input values, entered into the system are values from which the race or ethnicity can be derived. One of such values is for example the culprit's address, as certain areas are usually inhabited by members of a low income social groups or members of a certain ethic or

[409] SIMON, J. – FEELEY, M. The New Penology: Notes on the Emerging Strategy of Corrections and Its Implications. *Criminology*. 1992, Vol. 30, no. 4. pp. 449–474 [2016-05-31]. Available at: <http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1717&context=facpubs>.

[410] Ibid., p. 455.

[411] HARCOURT, B. *Against Prediction. Profiling, Policing, and Punishing in an Actuarial Age*. Chicago: The University of Chicago Press, 2007, p. 17.

[412] Ibid., p. 25.

[413] Ibid., p. 32.

[414] Ibid., p. 33.

[415] Ibid., p. 36.

[416] GÜTTLER, V. – MATEJKA, J. *K otázkám některých základních lidských práv a svobod v souvislosti s právní ochranou biometrických údajů*, p. 1038.

national minority. Some systems even explicitly work with the culprit's gender as a value influencing the risk of recidivism.[417]

The United States Supreme Court has expressed its view concerning the right to a fair trial in its judgement in *Griffin v. Illinois*.[418] According to this Court, ensuring equality in the justice system for the poor and rich, or for the powerful and powerless with no influence, is a very old problem, nevertheless people still hope that there will be justice and that an endeavour exists to get closer to this goal. Ensuring equality before justice in criminal proceedings is guaranteed by the constitutional right to a fair trial and by a ban on discrimination. In the same verdict the Unites Stated Supreme Court also ruled that ensuring that the persons accused of having committed a criminal offence are before the court equal as stipulated by the legislation, is one of the cardinal principles of the court system as such.

In another verdict, *United States v. Virginia,* the United Stated Supreme Court refused a different treatment based on gender which is the result of a generalisation of characteristics popularly ascribed to one gender and to the other. The principal of equal treatment of men and women includes, inter alia, the guarantee of protection against excessive generalisation, because verdicts which would be based on such generalisation would maintain the historical patterns of gender-based discrimination.[419]

According to the United States Supreme Court, the reason for refusing to impose a suspended sentence cannot be the convicted person's poor financial situation either. The state cannot justify sentencing to a suspended sentence a convicted person who showed a good will and tried to repay his debt to the society. The state cannot label this individual as poor and classify him on the basis of his poverty as being dangerous. Such practice would ultimately mean that the person would be punished for his poverty, which according to the United States Supreme Court is inadmissible.[420]

The Unites States Supreme Court in its judgements also refutes different treatment based on statistics, and on the contrary accentuates uniqueness and individual approach.[421] Starr points out that no relevant research exists which would indicate that actuarial assessment of the risk of future recidivism brings better results in predicting the culprit's recidivism than when assessing each case individually.[422] Using an actuarial model for predicting future recidivism of culprits based on social, cultural, demographic and economic factors of a certain group to which the culprit belongs, is in contraction with the judgements of the Unites States Supreme Court, which accentuates the individuality of the culprit or of the person being tried in other than criminal proceedings, and abandoning unjustifiable generalisation based on society's prejudices towards the individual because of his belonging to a certain group, about which the society has its, often groundless, ideas.

A survey of judges who use in their adjudication systems for assessing the culprit's risk based on actuarial methods has shown that even professionals do not understand the principle of this method.[423] Hannah-Moffat in her research presents an evidence that certain characteristics which are presumed in a group of people are regarded by those who should be independent and impartial,

---

[417] CHRISTIN, A. – ROSENBLAT, A. – BOYD, D. Courts and Predictive Algorithms. In: *NYU Law* [online]. 2015 [2019-12-17]. Available at: <https://www.law.nyu.edu/sites/default/files/upload_documents/Angele%20Christin.pdf>.
[418] Judgement of the United States Supreme Court, 23 April 1956, Griffin v. Illinois, 351 U.S. 12 (1956).
[419] Judgement of the United States Supreme Court, 26 June 1996, United States v. Virginia, 518 U.S. 515 (1996).
[420] Judgement of the United States Supreme Court, 24 May 1983, Bearden v. Georgia, 461 U.S. 660 (1983).
[421] STARR, S. Evidence-Based Sentencing and the Scientific Rationalization of Discrimination. In: *Michigan Law* [online]. 2013 [2016-05-31]. Available at: <http://repository.law.umich.edu/law_econ_current/90>.
[422] Ibid., p. 36.
[423] HANNAH-MOFFAT, K. *Actuarial Sentencing: An "Unsettled" Proposition*, p. 278.

as characteristics of the individual belonging to this group, and hence ascribe to him the features of the group as a whole. Belonging to this group is the crucial factor in sentencing this individual.

The output of risk assessing actuarial models may not be the correct outcome of the culprit's degree of risk from the point of view of future recidivism. The errors made by these models are of two types. It could be a false positive result, when the presumed event will not happen. The culprit may be for instance classified as an individual with a very high risk of recidivism, but he does not commit any criminal offence in the future. The outcome can be also false negative. A false negative result is a situation when the model has erroneously presumed that a certain situation will not occur. The culprit is for example erroneously classified as a person whose risk of recidivism is low, but in spite of that, after certain time he does again commit a criminal offence.[424]

The culprit's degree of risk concerning potential recidivism should be the subject of an individual assessment. In the Czech legislation as well as in the legislations of the countries of continental Europe, a principle of free assessment of evidence applies, in conjunction with the requirement on the judge's inner conviction.[425] This principle is expressed in Article 2 paragraph 6 of CO. According to this provision, criminal law enforcement authorities must, when making an assessment, use their inner conviction based on careful consideration of all circumstances of the case, both individually and in their summary. The principle of free assessment of evidence means that the criminal law enforcement authorities not only can, but must, take into consideration all circumstances of the particular case, its peculiarities and characteristic features. The aim of the free assessment of evidence is to prevent adopting a mechanical procedure when assessing evidence.[426] The judge assesses the presented evidence based on his inner conviction in each individual case. If the judge were to be bound by the result generated by an algorithm, the above described principles would be violated. The judge's inner conviction would be, even if the result generated by algorithm were to be only a recommendation, with a high degree of probability influenced, in spite of the claimed presumed objectivity of the algorithmic decision making. Introducing algorithmic decision making in criminal proceedings would violate the above-defined principles and constitute a deviation from the modern principles of adjudication used in continental criminal proceedings.

3.4.4.2 Problem of algorithmic decision making in criminal proceedings and fundamental human right in the light of European judicature

3.4.4.2.1 Ban on discrimination

Even though the decision making based on algorithm is claimed to be objective, i.e. not only independent and impartial, but also free of any illegitimate differentiation of people and discrimination, there is a concern when using a decision making algorithm that people will be treated differently depending on their real or presumed attributes. Such attributes could be nationality, ethnicity, belonging to a certain social group, gender, age or other indicator. According to Christopher Slobogin, attributes such as gender or age are part of the methodology for predicting criminal activity.[427] As we have already mentioned earlier, included among the values which the algorithm works with could be also other attributes such as race, ethnicity or belonging to a certain social group.

---

[424] BARNES, G. C. – HYATT. M, J. Classifying Adult Probationers by Forecasting Future Offending. In: *NCJRS* [online]. 2012 [2016-05-14]. Available at: <https://www.ncjrs.gov/pdffiles1/nij/grants/238082.pdf>.

[425] See Art. 427 of the French Code de procédure pénal, or § 261 of the German Strafprozeßordnung.

[426] ŠÁMAL, P. a kol. *Trestní řád. Komentář.* 7th ed. Praha: C. H. Beck, 2013.

[427] SLOBOGIN, Ch. *Proving the Unprovable. The Role of Law, Science, and Speculation in Adjudicating Culpability and Dangerousness*. Oxford: Oxford University Press, 2007, p. 112.

Rouvroy explains the contradiction between the objectivity of algorithmic decision making and the concerns about unequal treatment and discrimination by the algorithm's property of learning from previous operations. According to Rouvroy, the algorithm adopts the view of the world of its users, who by accepting the results the algorithm has generated, are even more convinced of the results' correctness. Discrimination is very difficult to prove, because of the argument of objectivity of algorithm-based decision making.[428]

Decision making based on values such as race, ethnicity, age, gender or belonging to a certain social group can be implemented in the system directly. In such case the algorithm works with these values right from the beginning. The algorithm can start generating outputs based on these values in the course of the system's functioning, as the result of learning from previous operations, if the users observe the outputs generated based on these values.

There are two types of discrimination – direct discrimination and indirect discrimination. By direct discrimination is meant a conduct when we treat one person less favourably than another person in a comparable situation, based on unacceptable criteria.[429] Indirect discrimination is evoked by different treatment at the application level, caused by discriminatory interpretation of the law or by its defective construction.[430]

The European Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter "ECHRF") it its clause 14 prohibits discrimination in exercising the rights and freedoms guaranteed by this Convention. Exercising the rights and freedoms must be ensured without discrimination based on any grounds whatsoever, being it gender, race, skin colour, language, religion, political or other conviction, nationality or social origin, belonging to a national minority, assets, linage or other position. This provision does not stipulate that the state could restrict this right not to be discriminated on legitimate grounds, as is the case for instance with the right to the protection of private and family life, or the right of free expression.

Pursuant to clause 1 paragraph 1 of Protocol no. 12 to ECHRF, exercising all rights granted by legislation must be guaranteed without any discrimination on the grounds of race, skin colour, language and religion, political or other conviction, nationality or social origin, belonging to a national minority, assets, linage or other position. The second paragraph of this provision stipulates that nobody may be discriminated against by any state administration authority on any grounds whatsoever, especially on the grounds named in the first paragraph.

According to the judicature of the ECHR, literature distinguishes between *a priori* suspicious criteria, and criteria which are not *a priori* suspicious.[431] Differentiation between the two criteria is within the degree of consideration discretion of ECHR. While in respect of criteria which are not *a priori* suspicious the state may exercise a broader degree of leeway, in respect of criteria which are *a priori* suspicious the state must justify different treatment by giving objective and legitimate reasons, while preserving proportionality between the means used and the ground for the different treatment.[432] *A priori* suspicious criteria are gender, sexual orientation, nationality, race or ethnicity, a child being born in wedlock or out of wedlock, the state of health or disability.[433]

[428] ROUVROY, A. "Of Data and Men".Fundamental Rights and Freedoms in a World of Big Data. In: *Bepress* [online]. 2011 [2016-05-04]. Available at: <http://works.bepress.com/antoinette_rouvroy/64>.
[429] BOBEK, M. – BOUČKOVÁ, P. – KÜHN, Z. (eds). Rovnost a diskriminace. Praha: C. H. Beck, 2007, p. 43.
[430] Ibid., p. 53.
[431] See. KABELOVÁ DOLEJŠOVÁ, K. *Zákaz diskriminace jako právní problém v judikatuře Evropského soudu pro lidská práva*. Praha: Univerzita Karlova v Praze, Právnická fakulta, 2012, p. 114.
[432] Decision of the European Court of Human Rights, 24 July 2003, no. 40016/98 (Karner against Austria).
[433] See WÁGNEROVÁ, E. a kol. *Listina základních práv a svobod. Komentář*. Praha: Wolters Kluwer ČR, 2012, p. 104.

Pursuant to ECHR, unequal treatment in court proceedings is discrimination. Discrimination leads to the violation of the right to a fair trial. In case *Paraskeva Todorova vs. Bulgaria*[434] the complainant of a Romany origin was given a three-year unsuspended sentence. The court's justification mentioned her Romany origin, and neither the court of first instance nor the appellate court gave a reason why a suspended sentence was not possible. In addition, the court of first instance in its judgement stated that members of minorities did not regard a suspended sentence of imprisonment as a real sentence. ECHR ruled that if the argument in the court's verdict mentions a different treatment which this court deployed, and this argument is based exclusively on the criteria named in clause 14 of ECHRF, the state must justify the different treatment in its verdict, something which in this case had not been done, when the only argument used was the complainant's ethnicity. ECHR arrived at the conclusion that in this case an unjustifiable difference in treatment existed in the criminal proceedings to the complainant's detriment, which meant that the provisions of clause 14 of ECHRF were violated.

In the verdict in *Fredin vs. Sweden*[435], ECHR dealt with the burden of proof on the complainant's side. In order for the complaint concerning a violation of clause 14 to be upheld, it had to be based, inter alia, on the argument that the situation of the alleged victim of discrimination could be regarded as similar to the situation of the persons who have received a more favourable treatment.

Discrimination does not have to be only an unequal treatment. According to ECHR, discrimination can be also equal treatment meted to an individual who is factually in a different position than that of others. A violation of clause 14 of ECHRF can be caused by equal treatment of persons who are in fact not equal. In this case the equal treatment deepens the factual inequality instead of correcting it. According to this Court, unequal treatment is discriminatory if it lacks an objective and reasonable justification, i.e. if it does not pursue a legitimate goal, or if there is no proportionality between the means deployed and the goal that is to be achieved. *(Stec and others against the United Kingdom)*.[436] ECHR also ruled in favour of unequal treatment in cases of factual inequality, in its verdict in case *Thlimmenos against Greece*.[437]

Similarly, as in ECHRF, the ban on discrimination is also embedded in the Charter of Fundamental Rights of the European Union (hereinafter "EU Charter"). Discrimination in exercising human rights and freedoms is also banned by the EU Charter. Pursuant to clause 3 paragraph 1, fundamental rights and freedoms are guaranteed to all irrespective of gender, race, skin colour, language, faith and religion, political or other conviction, national or social origin, belonging to a national or ethnic minority, wealth, linage or other position. Pursuant to the Constitutional Court's ruling, encroachment upon the rights protected by clause 10 of the EU Charter[438] could be caused by a conduct with intended or unintended consequences, as well as by a conduct targeted against a generally defined group of people an individual feels belonging to.[439] The Constitutional Court criticised the argumentation of general courts, according to which it is not possible for an individual not to feel offended by a discriminatory conduct targeted at group defined in general terms.

It is our opinion that algorithmic assessment of the degree of risk of recidivism, predicting whether a culprit who has committed a criminal offence will commit a criminal offence again in the future,

[434] Decision of the European Court of Human Rights, 25 May 2010, no. 37193/07 (Paraskeva Todorova against Bulgaria).
[435] Decision of the European Court of Human Rights, 18 February 1991, no. 12033/86 (Fredin against Sweden).
[436] Decision of the European Court of Human Rights, 12 April 2006, no 65731/01 and no. 65900/01 (Stec and others against the United Kingdom).
[437] Decision of the European Court of Human Rights, 6 April 2000, no. 34369/97 (Thlimmenos against Greece).
[438] Art. 10 Charter of Fundamental Rights and Freedoms of the Czech Republic: (1) Everyone has the right to demand that her human dignity, personal honour, and good reputation be respected, and that her name be protected. (2) Everyone has the right to be protected from any unauthorized intrusion into her private and family life. (3) Everyone has the right to be protected from the unauthorized gathering, public revelation, or other misuse of her personal data.
[439] Judgment of the Constitutional Court of the Czech Republic, 13 January 2010, no. II. ÚS 1174/09.

is direct discrimination, because the culprit who is of a certain race, ethnicity, age, gender or who belongs to a certain social or cultural group, is treated less favourably than culprits who do not have these attributes. By less favourable treatment is meant assessing the culprit as being riskier compared to other culprits merely on the above defined grounds. If this type of an algorithmic decision making is used, such culprit will be assessed more harshly and will be for example sentenced to imprisonment, while other culprits may receive an alternative punishment not restricting their freedom, or receive an unsuspended sentence instead or suspended one, or his application for parole will be turned down instead of approved, unlike in the case of another culprit in a comparable situation.

When using actuarial assessment of the degree of risk of culprits, direct discrimination is one of the characteristics of this system. The systems of actuarial assessment work with categories such as race, ethnicity, age and economic group. The presence of these categories increases the culprit's determined degree of risk. The culprit himself does not necessarily have to be the source of the reason for increasing the risk by his individual features, character or other characteristic which he cannot influence. Discrimination will take place the right exercising level, and of course will not be an outcome of interpreting law, but will be a reflection of the results of the decision made by the automated algorithm, which constitutes learning of recapitulated outcomes of a discriminatory character.[440]

Although ECHRF does not allow member states to restrict the ban on discrimination on legitimate grounds, the Court does give member states the discretion of a broader consideration in respect of some grounds. Therefore, it is up to the state's consideration to decide whether to apply a different treatment or not. However, it has to justify using a different treatment. When assessing the culprit's degree of risk, the decision is usually made on the basis of values in respect of which ECHR applies more stringent criteria concerning the degree of the state consideration, i.e. gender, race, nationality and ethnicity. In our opinion, ECHR would regard different treatment of an accused by a member state as a violation of clause 14 of ECHRF, if this accused were to be sentenced to imprisonment of a greater length or receive an unsuspended sentence, or his application for parole would be turned down exclusively on the grounds of some of the accused's attributes over which he has no influence. Unless the state would use different argumentation for the different treatment justified by a wider consideration, and for the grounds such as gender, race, nationality or ethnicity by stating objective and legitimate reasons for the different treatment, and ECHR would find these grounds as legitimate and adequate for the purpose.

The right which would in this case be violated would be the right to a fair trial pursuant to clause 6 of ECHRF. ECHR has ruled a case when a state not only failed to investigate a complaint of different treatment meted by persons in charge (see *B.H. against Spain*[441]), but in which these persons even actively participated in the discrimination (see *Paraskeva Todorova against Bulgaria*), to be a violation of clause 14 of ECHRF . Therefore, we could assume, especially in view of the judgement in *Paraskeva Todorova against Bulgaria,* that ECHR would find using actuarial models for assessing culprits based on the criteria such as race, ethnicity, gender, age, etc., to be a violation of clause 14 of ECHRF.

ECHR might also find a violation of clause 14 of ECHRF a procedure deployed by the state when imposing a fine or setting a bail in lieu of detention using an actuarial model, if this model would assess the accused as a person for whom this type of punishment or bail is appropriate on account of his degree of risk, but would fail to take into consideration the accused's financial situation and impose an identical or similar fine or bail for all accused. Here as discriminatory would be regarded an equal

[440] ROUVROY, A. *"Of Data and Men".Fundamental Rights and Freedoms in a World of Big Data*, p. 33.
[441] Decision of the European Court of Human Rights, 24 July 2012, no. 47159/08 (B.H. against Spain).

treatment of persons whose financial situation was significantly different. Setting an identical bail which less well-off accused could not afford, or imposing an identical fine which less well-off accused would be unable to pay and had to serve a sentence of imprisonment instead, would exclude those less well off from benefiting from the alternative punishments to imprisonment. ECHR would regard such adjudication based on an actuarial model as discriminatory (see *Thlimmenos against Greece*), unless the state could objectively and reasonably justify it.

3.4.4.2.2 Right to a fair trial

The right to a fair trial is part of many legal documents concerning human rights. It also pervades as a red thread sub-constitutional legal process regulations the provisions of which concretise and specify this right in a certain process stage. Pursuant to clause 6 paragraph 1 of ECHRF, everybody has the right to have his case tried fairly, publicly and within a reasonable time, by an independent and impartial court established by legislation, which will rule on the person's citizen's rights or obligations, or on the legitimacy or any criminal charges laid against him. The second paragraph of this provision guarantees the presumption of innocence. Anyone who has been accused of having committed a criminal offence shall be deemed innocent until found guilty in a legal process. The third paragraph of clause 6 deals with the accused's right to defence. Part of the right to a fair trial is also the right of appeal. This right is part of Protocol 7 to ECHRF.[442] The right to a fair trial is also stipulated in the EU Charter. Clause 47 of the EU Charter has embedded in it the principle of presumption of innocence as well as the right to defence. In respect of algorithmic adjudication, mentioned must be also the provision of clause 49 paragraph 3 of the EU Charter, according to which the punishment meted must not be out of proportion with the criminal offence committed.

The right to a fair trial is similarly embedded in the Czech legislation. Pursuant to clause 36 of the Charter, anyone can exercise his rights in a specified procedure before an independent and impartial court, and in defined cases also before other bodies. Clause 38 of the Charter guarantees that nobody can be taken away from his legitimate judge, and guarantees also that the court hearings are public. Pursuant to clause 40 of the Charter, only a court of law can rule on the guilt and punishment for criminal offences. Anyone against whom criminal prosecution has been instituted shall be deemed innocent unless found guilty by a court in legal adjudication. The Charter also guarantees to the accused basic minimal rights to defence, in a similar way as in ECHRF.

One of the main premises of the right to a fair trial is an independent court and an impartial and independent judge. An independent court is an institutional aspect of the right to a fair trial. Neither the executive nor the legislature may interfere with the adjudication power of courts. The content of the adjudication authority of courts is judging in cases specified by the Constitution and by legislation. Courts as the only authority have the right to rule on the guilt and punishment for criminal offences. The principle of an independent and impartial judge does not mean only an absence of influencing judges' verdicts by other persons, but also a presence of own free opinion about the facts which turn up during the proceedings, and about their legal assessment.[443] The impartiality of judges is perceived similarly also by Recommendation CM/Rec(2010)12 adopted by the Committee of Ministers of the Council of Europe to the Member States, titled: Independence, Efficiency and Responsibility of 17 November 2010 (hereinafter "Recommendation").[444] Pursuant to clause 1 paragraph 5 of the Recommendation, judges should have an unlimited freedom to rule on matters impartially and in accordance with the legislation and their interpretation of the facts.

[442] The right of appeal in Art. 2 of the Protocol 7 relates solely to criminal matters.
[443] Decision of the Constitutional Court of the Czech Republic, 28 April 2005, no. Pl.ÚS 60/04.
[444] Judges: independence, efficiency, and responsibilities. Recommendation CM/Rec(2010)12 and explanatory memorandum. In: *Council of Europe* [online]. 2003 [2019-10-23]. Available at: <https://rm.coe.int/16807096c1>.

Pavel Molek sees the judge's impartiality from two aspects. These aspects are the absence of the judge's bias and prejudice[445] and the knowledge of the proceedings participant which judge will be adjudicating in his case, i.e. preventing a "*faceless judge*" from adjudicating in the case. In *Remli against France*, ECHR dealt with the complaint filed by a French citizen of Algerian descent, who claimed than the national court disregarded a remark made by one of the assessors about his racist thinking. The national court did not concern itself with the complainant's claim of bias. ECHR ruled that clause 6 of ECHRF had been violated, because the court which tries a case must be impartial. And ECHR ruled similarly in case *Sander against the United Kingdom*,[446] in which according to the complainant part of the decision making was a juror with racist attitudes.

Violation of clause 6 of ECHRF need not to be only an absence of measures adopted by the court against the doubts of a racist attitude of jurors. An absence of measures against doubts about jurors' impartiality may concern also the juror's prejudices towards those proceedings participant who belongs to a certain subcultural group. In case *Ekeberg and others against Norway*, such group was the Hells Angels Motorcycle Club.[447]

Another aspect of impartiality and independence of judges, and hence also guarantee of the right to a fair trial, is the absence of anonymity of judges. When the proceedings participant does not know the judge's identity, as was the case in *Polay Campos against Peru*[448] in the matter concerning a complaint by the Human Rights Council against the practice in which judges tried with their faces covered, the principle of impartiality and independence has been violated. In algorithmic adjudication, although the judge is present in the courtroom and he himself formally announces a verdict or other decision, he is in his ruling not guided by his own view of the facts and their evaluation which he subsequently assesses within the intentions of legislative regulations, but by the outcome generated by an algorithm which works with predefined categories entered into the system by the judge. The proceeding's participants even do not have to be aware that the outcome of the proceedings has been guided by an output generated by an algorithm, as no legislative regulation exists which would order the judge to tell this fact to the proceedings participant. Thus the proceedings participant does not know that this is how the decision has been made, and hence it will be difficult for him to argue against the lack of the judge's own free opinion and from it arising violation of his right to a fair trial. If the proceedings participant's right to a free trial is violated by the bias and prejudice of judges, jurors or other persons participating in the proceedings, we can derive that the right to a fair trial has been violated also by using actuarial models predicting the degree of risk of culprits. Although defence of the proceedings participants is possible, if the appellate or recourse court works with the same actuarial model or with a different model which, however, is based on the same values, the defence will be merely formal, because the outcome generated by the algorithm will be identical or differ only marginally. There are two reasons why we have mentioned the problem of faceless judges. The first reason is that the judge who controls the court proceedings only formally and signs the verdict or other type of judgement, in fact does not decide about the proceeding's participants. The decision is made for him by an algorithm. The persons who developed the actuarial model thus participate in a decision which should be made by the trial judge alone. Therefore, to the accused, these persons are "faceless judges".

Another aspect of the right to a fair trial which the algorithmic decision making violates, is the right to defence. According to ECHR, defence in criminal proceedings must be given a space to adequately

[445] MOLEK, P. *Právo na spravedlivý proces*. Praha: Wolters Kluwer ČR, 2012, p. 169.
[446] Decision of the European Court of Human Rights, 9 May 2000, no. 34129/96 (Sander against the United Kingdom).
[447] Decision of the European Court of Human Rights, 31 July 2007, no. 11106/04, no. 11108/04, no. 11116/04, no. 11311/04 and no. č.13276/04 (Ekeberg and others against Norway).
[448] Decision of Human Rights Committee, 6 November 1997, no. 577/1994 (Polay Campos against Peru). In: *Office of the United Nations High Commissioner for Human Rights* [online]. [2016-05-15]. Available from: <https://www.ohchr.org/Documents/Publications/SDecisionsVol6en.pdf>.

present its arguments. According to ECHR, the defence's function is to be a guardian ensuring that criminal proceedings take place in a legal way (*Ensslin, Baader, Raspe against Germany*[449]). According to ECHR, in order to ensure that the rights guaranteed by ECHRF are not encroached upon, they must be exercised practically and effectively, not merely formally and seemingly (e.g. *Airey against Ireland*[450]). If algorithmic adjudication is an adjudication made on the basis of certain values the algorithm works with and which are independent from the accused's will, his defence is merely formal and seeming.

Algorithmic adjudication penetrates the adjudication of judges. The reason might be speed and efficiency of the decision making process, as well as the trust in its objectivity, because of a general assumption that algorithmic decision making is, unlike human decision making, free of prejudices and biases. When used to assess the degree of risk of a particular accused, the algorithm uses profiles constructed from the culprit's personal data. Some of these data have the character of biometric data based on the individual's psychological traits. Thus if the accused belongs to a certain group or has certain psychological traits, he is by the system automatically assessed as either riskier or less risky, although the thus assessed degree of risk of this accused does not have to correspond with reality. Algorithmic adjudication might violate two fundamental rights of the accused, the right not to be discriminated against, and the right to a fair trial. It is discriminatory also towards the accused if he is treated less favourably, especially on the grounds of his race, ethnicity or national minority, age, gender or belonging to a certain social group. Although these criteria do not necessarily have to be entered into the system directly, they can be derived from the values which provide information about these facts indirectly.

It is a violation of the principle of equality before law which encroaches upon the right to a fair trial. Although the conditions for courts to make a decision are stipulated by legislation, in reality different people are treated differently, based on the general characteristics of their profile to which they have been assigned by the system. A violation of the right to a fair trial can be seen also in the fact that the accused does not have to be at all aware that the decision about him has not made on the basis of his individual characteristics, but on the basis of a model which works with values applicable to a group.

A judge should decide not only independently and impartially, but also after having considered all facts and circumstances of the case, because the algorithm on the basis of which the decision is made, works with predefined values.

In view of these arguments, we can state that algorithmic court decision making can constitute an encroachment upon the fundamental human rights and freedoms. Compared to encroachments upon these rights by a decision which has not been made based on an algorithm, the scope for remedying the encroachment in the case of an accused whose rights have been violated by the algorithmic decision making, is more difficult. The reason for this is the presumed impartiality of the actuarial model and the absence of transparency of the decision making process based on an algorithm. Formally though, all accused's rights might have been preserved.

[449] Decision of the European Court of Human Rights, 8 July 1978, no. 7572/76 (Ensslin, Baader, Raspe against Germany).
[450] Decision of the European Court of Human Rights, 9 October 1979, no. 6289/73 (Airey against Ireland).

4. Data Subjects and Their Options with Regard to Protecting Own Biometric Data

4.1 Concerns of Data Subjects

Users' preferences, awareness and knowledge about risks of biometric technologies significantly determine what applications are they going to use, whether they are going to provide an explicit consent with biometric data processing

This chapter will briefly focus on three surveys that were conducted in 2018 and that examine approach of people to biometrics. Each survey was conducted on a geographically different demographic segment. The first survey focused solely on U. S. population. The second survey focused on respondents from the U. S., EU and from Australia, India and Singapore. The third survey focused on respondents from the Czech Republic.

An American survey "Consumer Attitudes About Biometric Authentication" conducted in May 2018 by the University of Texas focused on the level of use of biometrics, individual understanding of biometrics, or preferences of certain types of biometrics.[451] This survey mainly found out that "more than 42% of participants use biometrics for unlocking their personal devices, usually fingerprint recognition. The most popular account use for biometrics is financial services, with 17% using them to access personal banking, and 5% to manage investments online ... A significant proportion of those using biometrics appear to not have recognized them as such at the beginning of the questionnaire. Alternately, they might not consider 'giving' the information to their phone the same thing as giving it to the organization ... Of all biometric types included in the survey, participants were most comfortable giving their fingerprint in biometric form, with 58% saying they were very comfortable, and 28% saying they were somewhat comfortable ... 42% of participants say they are very concerned about the misuse of their personal information, and 44% are somewhat concerned."[452]

An IBM survey "Consumer perspectives on authentication: Moving beyond the password"[453] focused mainly on issues related to biometrics and security. According to this study age significantly influences approach of people to security while younger generations expect stronger security. Respondents expressed their preferences for security over convenience. 67 % of respondents said they were

[451] Results of the survey were summarized in GERMAN, R. L. – BARBER, K. S. Consumer Attitudes About Biometric Authentication. In: *The University of Texas at Austin, Center for Identity* [online]. 2018 [2019-01-30]. Available at: <https://identity.utexas.edu/assets/uploads/publications/Consumer-Attitudes-About-Biometrics.pdf>.

[452] Ibid.

[453] IBM SECURITY. IBM Security: Future of Identity Study, Consumer perspectives on authentication: Moving beyond the password. In: *ORBIS* [online]. 2018 [2019-12-08]. Available at: <https://espas.secure.europarl.europa.eu/orbis/sites/default/files/generated/document/en/security-ibm-security-solutions-wg-research-report-22012422usen-20180124.pdf>.

comfortable using biometrics. Despite that around 50 % of respondents were concerned about privacy and security. Interestingly, the strongest password practices were found in Europe.

In September 2018, the Czech Academy of Sciences conducted a survey called "Biometrics and its use from the perspective of the Czech public".[454] The aim of this survey was to find out how well the Czech citizens are informed about what is biometrics and its risks and well as whether they prefer user friendliness or privacy protection when it comes to biometrics.

Results of the survey showed that 71 % of the respondents have heard of biometrics and 47 % of the respondents know approximately what biometrics is. Only 13 % of the respondents expressed that they know very well what biometrics is. Greater awareness about biometrics was indicated mainly by male respondents, respondents in the age group 30–44 years, respondents with university education, respondents living in big cities, respondents with professional jobs, and respondents with higher living standards. Out of all respondents, 30 % are not aware of a potential risk of collecting, processing and exploitation of personal data by various modern technologies without their consent or awareness. This lack of awareness was indicated mainly by respondents in the age group 60 years and older, respondents with basic education, unemployed respondents and respondents with low living standards and those who do not use the Internet. However, 95 % of the respondents who indicated that they know very well what biometrics is also indicated their awareness of the above mentioned risk.

Interesting results and correlations were identified in preferences of user friendliness and comfort over privacy protection. In the Czech Republic 63 % of the respondents prefer privacy protection over maximal user comfort offered by new technologies with help of personal data processing. On the other hand, 21 % of respondents prefer maximal user comfort at the price of providing personal data. 16 % of the respondents could not decide on their preferences. There were, however, strong correlations of preferences with age and education as well as with religious belief and political preferences.

4.2 Scope of Data Subjects' Autonomy

4.2.1 General Remarks on the Principle of Personal Autonomy

The protection of privacy and personal data belongs among the fundamental human rights and freedoms.[455] The importance of these rights is becoming more and more evident in the digital age. This is mainly due to the ever-increasing amount of processed personal data and constantly evolving methods of data analysis. Not only do individuals knowingly disclose a lot of information about themselves but they also leave various digital footprints when using information and communication devices. In exchange for services, they increasingly share personal data with their providers, including data the processing of which could seriously undermine the rights and freedoms of these people in the future (e.g. health or biometric data). Natural persons often find themselves losing track of their

[454] The survey was initiated by the authors of this article and conducted by the Public Opinion Research Centre in September 2018. In total 1037 respondents older than 15 years were questioned during a personal interview. Complete results were summarized in ČERVENKA, J. *Biometrika a její využívání z pohledu české veřejnosti*. For more details see also Chapter 3.5.1.

[455] Protection of privacy is guaranteed in Article 7 (1) and Article 10 (2) and (3) of the Czech National Council's Resolution no. 2/1993 Coll., On the Declaration of the Charter of Fundamental Rights and Freedoms as a part of the constitutional order of the Czech Republic.

dependence on the intensive use of information and communication equipment, and thus, control of their personal data. They are also deprived of the opportunity to effectively influence their lives.

The European Union responded to these trends by adopting the GDPR. The GDPR highlights, inter alia, the need to ensure that individuals can control their personal data.[456] According to this regulation, deprivation of such control represents a risk to the rights and freedoms of an individual.[457] The GDPR stipulates that "a personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned".[458] In order to enhance control over personal data, the GDPR introduces rights of data subjects[459] in its Chapter III. Compared to the DPD this chapter includes new rights, such as an explicitly formulated "right to be forgotten" (Art. 17 of the GDPR,) or the right to data portability (Art. 20 of the GDPR).

The GDPR specifically mentions as reasons for its adoption in particular the need to establish trust in society through consistent law enforcement and by strengthening the legal and practical certainty of all stakeholders. However, these objectives shall also contribute to strengthening data subjects' autonomy. From the perspective of philosophy of law, the concept of personal autonomy can be perceived as "the ability to create one's life and determine its course".[460] This concept is closely linked to the concepts of human dignity and personal freedom[461] and overlaps with more fundamental rights and freedoms. In Czech law, the concept of personal autonomy vastly corresponds to the legal principle of freedom of contract, whose essence is mainly the freedom of entities to form private contracts.

However, the GDPR will also affect these private relations. With regard to Art. 10 of the Constitution of the Czech Republic[462] and Art. 2 (1) as well as Art. 288 of the Treaty on the Functioning of the European Union (TFEU),[463] the GDPR shall prevail over Czech laws. At the same time, however, private law relationships will be regulated by existing national laws in the areas not regulated by the GDPR. For example, national law provisions on legal acts or provisions regulating the processing of personal data or protecting personal rights and privacy will apply in cases where the GDPR either refers to a special national regulation or excludes itself from the application. At the same time, the general legal principles laid down in the Civil Code will remain applicable.[464] Moreover, in certain cases it will be possible to apply national rules if adopted by Member States.[465] These national rules can be introduced (or maintained) for "special category of personal data" that are defined and primarily regulated by Art. 9 of the GDPR. Processing of the data in this category leads to increased vulnerability of the persons to whom they relate. Biometric data processed for purposes of unique identification represent one type of data belonging to this category. Given the fact that biometric data

[456] See Recitals 7 and 68 of the GDPR.
[457] See Recital 75 of the GDPR.
[458] See Recital 85 of the GDPR.
[459] A data subject is defined in Art. 4 (1) of the GDPR as "an identified or identifiable natural person". The term identification, however, is not defined. The same provision further states that "identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".
[460] RAZ, J. *The Morality of Freedom*. Oxford: Clarendon Press, 1988, p. 154.
[461] KOFFEMAN, N. R. (The right to) personal autonomy in the case law of the European Court of Human Rights. In: *Leiden University Repository* [online]. 2010 [2019-12-08]. Available at: <https://openaccess.leidenuniv.nl/handle/1887/15890>.
[462] Constitutional Act no. 1/1993 Coll., Constitution of the Czech Republic.
[463] Consolidated version of the Treaty on European Union and the Treaty on the Functioning of the European Union.
[464] The Civil Code provides a list of general principles in the Sec. 3.
[465] See Recital 10 or Art. 9 (4) of the GDPR.

cannot be easily altered (if in some cases at all), its potential misuse poses a much greater threat to individuals. At the same time, the use of biometric technologies in everyday life is increasing.[466] The question then arises as to the extent of their actual control over these data.

In the light of the above, this chapter aims to clarify to what extent the GDPR leaves natural persons free to decide on the processing of their biometric data in the light of Czech law and to what extent it limits them. In fact, this concurrence of several legal regulations raises the question about the real scope of personal autonomy in this area. In theory, the scope of personal autonomy should be strengthened by the GDPR.

In Czech law, the principle of personal autonomy is primarily enshrined on the Constitutional level in the Charter of Fundamental Rights and Freedoms[467] within the rule according to which "everyone can do what is not prohibited by law and no one must be forced to do what the law does not impose".[468] This provision reflects the general premise of protection of human freedom enshrined in Art. 1 of the Czech Charter of Fundamental Rights and Freedoms. This rule guarantees the right of free choice.[469] This right stands at the same level as other fundamental rights and freedoms, and, given the nature of the protected values, overlaps and complements them. On the other hand, it may also conflict with other fundamental rights or constitutional principles. In such a case, a potential conflict is resolved with help of a proportionality test.

Protection of privacy as well as protection of family life is guaranteed in the Czech Charter of Fundamental Rights and Freedoms by Art. 10 as a personality right. This personality right set out in Art. 10 at the same time protects human dignity, personal honour, reputation, name and also enshrines protection against unauthorized collection, disclosure or other misuse of personal data.

Personal autonomy, the right to privacy, and protection against unauthorized processing of personal data are, therefore, protected at the constitutional level as absolute rights. Specific conditions for the exercise of these rights are defined in different laws, in particular in the Civil Code and in the Personal Data Processing Act, that implements some parts of the directly applicable GDPR. The GDPR takes precedence over the Czech law.[470]

Personality rights and the right to the protection of personal data overlap to some extent and protect a person simultaneously. Personality rights can be divided into two groups: absolute rights and relative rights.[471] Absolute personality rights take effect *erga omnes* , i.e. everyone needs to respect these rights of an individual. On the other hand, relative personality rights arise on the basis of established legal facts and an individual has these rights only in relation to a person who is a party to the respective legal relationship (effect *inter partes*). One could say that special laws on protection of personal data fall within the definition of relative personality rights. In the event of violation of personality rights, a natural person may choose which instrument will she use to protect her rights and interests. However, given the application priority of the GDPR, the courts shall apply the GDPR as a matter of priority in all areas regulated by it.

---

[466] For example, in 2018, over one billion smart phones equipped with a biometric sensor were expected to be delivered to the global market. See SHARMA, P. *More Than One Billion Smartphones With Fingerprint Sensors Will Be Shipped In 2018*.

[467] LAVICKÝ, P. et al. *Občanský zákoník I. Obecná část (§ 1−654). Komentář*, p. 56.

[468] Art. 2 (3) of the Czech National Council's Resolution no. 2/1993 Coll., On the Declaration of the Charter of Fundamental Rights and Freedoms as part of the constitutional order of the Czech Republic.

[469] LAVICKÝ, P. et al. *Občanský zákoník I. Obecná část (§ 1−654). Komentář*, p. 395.

[470] As already mentioned, the GDPR takes precedence over the Czech law with regard to Art. 10 of the Czech Constitution. However, at the same time the GDPR does not take precedence over constitutional acts. Therefore, the GDPR does not take precedence over the Czech Charter of Fundamental Rights and Freedoms.

[471] LAVICKÝ, P. et al. *Občanský zákoník I. Obecná část (§ 1−654). Komentář*, p. 396.

In this context, it should be noted that, although the GDPR takes precedence over Czech laws, its purpose is not to reduce the protection of individuals guaranteed by national law. A natural person may continue to avail provisions of the Czech law on personality protection if the strict application of the GDPR in a particular case threatens her rights and interests protected by law. At the same time, a natural person cannot completely rule out effects of the GDPR. Therefore, if there is a dispute between the natural person who is the data subject and the data subject's personal data controller, in which the claimant data subject refers only to the protection of personality enshrined in the Civil Code, the claimant should in particular prove why in this case the effects of GDPR are unfair and how they interfere with her absolute personality right. A court should then take into account whether, in the case of the applicability of the GDPR, the defendant has fulfilled its obligations under the GDPR, in particular whether the interests and fundamental rights and freedoms of data subjects have been sufficiently taken into account. It should also consider whether sufficient protection can be provided by the GDPR and only if it finds that this is not possible, the claimant can benefit from the provisions of the Civil Code. A court could also refer to the clause in the GDPR, which allows Member States to maintain existing conditions or restrictions on processing or to introduce new measures.[472] This option is relevant for biometric data, since Member States can maintain conditions, including restrictions on their processing. The question is, therefore, whether processing of biometric data is protected by absolute personality rights. The very nature of biometric data is an argument for affirmative answer. Biometric data define the physical component of a person (her body) or manifestations of a personal nature (her form and appearance, voice, behaviour, signature, etc.). Therefore, unless the Civil Code explicitly excludes the applicability of personality rights to biometric data, a court should also take into account personality protection enshrined in the CC. The GDPR does not provide that the existing conditions must apply exclusively to biometric data and not to be of a general nature.

In connection with the adoption of the new Civil Code and its relation to the existing public protection of personal data, some authors claimed that certain personality rights enshrined in the CC will not be applicable in practice.[473] However, except in the case of the biometric data mentioned above,[474] other exceptions would apply in areas not regulated by the GDPR in accordance with its Art. 2 (2). In private law this will be the case when a natural person will process the personal data of another person in the course of exclusively personal or domestic activities. Here, for example, in case of taking a portrait, an individual would need a permission of the photographed person with reference to the relevant provisions of the CC. With regard to biometric data, a house owner would for instance need permission of her family members to use their fingerprints instead of classic keys when entering their home.

4.2.2 Instruments of Data Subjects for Exercising Their Right to Autonomy

As mentioned above, in the area of privacy protection in private relations, there are two parallel protection regulations – the GDPR, which relates solely to personal data processing issues, and the personality protection enshrined in the Civil Code. The protection in the CC not only provides protection to individuals in cases of processing their biometric data and in cases not covered GDPR, but it also sets the general conditions of legitimacy, to which the GDPR refers.[475] Both branches

[472] Such authorization is provided for in Art. 6 (2) and 9 (4) of the GDPR. However, Art. 6 (2) does not apply to biometric data which have specific regulation in Art. 9. At the same time, Art. 6 (2) allows only maintaining or introducing more specific, more precise provisions. In contrast, Article 9 (4) speaks of maintaining or introducing any further conditions.

[473] NONNEMAN, F. Právní úprava ochrany osobnosti v novém občanském zákoníku a její vztah k ochraně osobních údajů. *Právní rozhledy*. 2012, Vol. 13–14, pp. 505 et seq.

[474] General conditions may be maintained also for genetic data and health data

[475] See Article 5 (1) b) and Recital 40 of the GDPR.

of regulations must be interpreted in accordance with the constitutional framework of the Czech Republic. The following subchapters will clarify which specific instruments for exercising the right to personal autonomy are provided by both regulations to individuals in connection with processing of biometric data.

4.2.2.1 General Data Protection Regulation

The principle of lawfulness, fairness and transparency of personal data processing set out in the GDPR contributes to the protection of personal autonomy of data subjects.[476] The principle of transparency in the GDPR has been even described in detail in a separate document of the WP29.[477] Although the principle of transparency is primarily linked to the principle of fairness, it has a significant impact on personal autonomy of data subjects. Generally, it is the duty of the controller to inform data subjects, to communicate with them in a certain way and to enable them to exercise their rights.[478] Strict requirements on the form of communication are particularly important. Controllers must help data subjects to truly understand the meaning, scope and implications of the processing of their personal data and not to keep this information too technical or technical. Only a genuine understanding of the whole process can lead to free formation of the data subject's will. Moreover, transparency "empowers data subjects to hold data controllers and processors accountable and to exercise control over their personal data by, for example, providing or withdrawing informed consent and actioning their data subject rights".[479] It is the consent and rights of data subjects that are the main instruments for exercising personal autonomy within the GDPR.

The consent of a data subject is a concept taken over from the Data Protection Directive. To a certain extent it corresponds to the protection of personality rights in the current Civil Code, which uses the term "permission" with regard to allowing interference with personality rights, and the term "consent" with regard to specific cases of interference with the integrity of an individual. Art. 4 (11) of the GDPR defines the term consent. Conditions for granting consent are governed in particular by Art. 7 and the related recitals.[480] According to the GDPR, consent means "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". By granting a consent, the data subject can define the scope of the controller's authority to process personal data. The scope of the consent must be clearly stated in the consent itself, i.e. in particular for what purpose the consent is granted.

At the end of 2017, WP29 published detailed guidelines on consent.[481] These guidelines expand former WP29's opinion on the definition of consent.[482] These new guidelines set high standards for the validity of the granted consent. The guidelines focus mainly on the issue of freedom of consent and on situations in the data subject grants her consent while being in an unequal position. Consent shall not be deemed to be free if its granting is considered a condition for provision of certain services, or if the data subject is not demonstrably offered alternatives and guarantees that she will not be adversely affected by whichever her decision. The consent must also be specific and relate to the specific purpose of the processing. If there are more purposes for processing, the controller must

[476] See Article 5 (1) a) of the GDPR.
[477] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on transparency under Regulation 2016/679*.
[478] Ibid., p. 5.
[479] Ibid., p. 6.
[480] See for namely Recitals 32, 33, 42, 43, or 51.
[481] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on consent under Regulation 2016/679*.
[482] ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 15/2011 on the definition of consent. In: *European Commission* [online]. 13. 7. 2011 [2019-12-08]. Available at: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf>.

demonstrate that the data subject has given his consent for all of these purposes. The validity of the consent also depends on the correct information provided to the data subject. As stated above, provision of sufficient information is a condition of free will. The data subject shall be also required to give consent in an active manner. Consent cannot be presumed and the data subject must not be forced to actively express disagreement.

In the field of biometric data processed for the purpose of the unique identification of an individual, so-called "explicit consent" is required. This consent must not only meet all of the above conditions, but must also be made explicitly. The WP29 guidelines acknowledge that the new consent requirements are stricter than the former ones. The guidelines suggest the best practice in obtaining this type of consent. It can be for instance an explicit written consent signed by the data subject, or a 2-step verification process of granting a consent during which the data subject gives his or her consent by email and then confirms it by clicking the link in the verification message.[483]

The rights of data subjects are additional tools by which natural persons can exercise their decisions regarding the processing of their own personal data and thus realize their fundamental right to personal autonomy. These rights are specified in Chapter III. (Art. 12-23) of the GDPR. These rights include the right to receive transparent information about personal data, the right of access to personal data, the right to rectification, the right to erasure (the right to be forgotten), the right to restriction of processing, the right to notification, the right to data portability, and the right to object to the processing of personal data in certain cases and "the right not to be subject to any decision based solely on automated processing, including profiling, which has legal effects or similar effects for him".[484]

In the field of biometric data, the right to rectification under Art. 16 of the GDPR should be highlighted. In particular, although biometric data based on biological (anatomical) characteristics are generally stable, accidents that for instance alter biological characteristics (e.g. burns, scars, etc.) may occur. In such cases, the data subject shall have the right to re-enrol in the biometric system and to create a new template based on her new biological characteristics. Furthermore, the data subject shall have the right to be deleted from the database if she withdraws her consent to the processing of her biometric data. Incidentally, the exercise of this right provides a strong argument in situations where providers of biometric authentication or identification systems claim that they cannot in fact identify individual persons in the system from the data they process and, therefore, they claim not to process personal data and not to be subject to the GDPR. If an administrator is able to selectively delete a person from the database of people who are allowed to access certain premises on the basis of biometrics, then they are demonstrably processing personal data. Where the data subject has given the controller consent to the processing of biometric data, she shall also have the right to obtain it "in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided".[485] Theoretically, the data subject has the right to obtain her biometric template, which she could then provide to another controller. In practical terms, however, this right is unlikely to be exercised. With a view to ensuring security and credibility, administrators will always require an original entry into their biometric system, under their control, so as to avoid any confusion of identity or system disruption by providing a biometric template to a person other than the one to be granted access. Cases of refusal of access to restricted areas on the basis of determining biometric identity can be considered as decisions based solely on automated processing. In the event that such a refusal of access would have legal effects or similarly affect that person, then, subject to Art.

[483] See Chapter 4 of ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on consent under Regulation 2016/679*.
[484] See Art. 22 of the GDPR.
[485] See Art. 20 of the GDPR.

22 and the right not to be the subject of a decision based solely on automated processing, the data subject should also have the right to review such automatic refusal and the right to obtain human intervention. Here, however, the question is what can be considered as legal or similar effects. WP29 mentions as examples of such legal effects situations of refusal of entry at the border or being subjected to increased security measures or monitoring by competent authorities.[486] Regarding the definition of similar effects, the guidelines state that it is difficult to determine precisely the threshold of materiality beyond which a particular decision can already be regarded as having legal effects. These are decisions that "must have the potential to significantly influence the circumstances, behaviour or choices of the individuals concerned; have a prolonged or permanent impact on the data subject; or at its most extreme, lead to the exclusion or discrimination of individuals".[487] Additional guidelines of WP29 analyse in detail the concept of "substantially influence" and mention, for example, damage or inconvenience, embarrassment, or other adverse consequences.[488] Anyway, substantial influence should be examined case by case. The same should apply to the concept of similar effects.

4.2.2.2 Personal Rights in the Civil Code

The personality rights enshrined in the Civil Code, despite the preferential regulation in the GDPR, have an impact on the extent of personal autonomy that natural persons can exercise. The principle of personal autonomy is expressed in private law in Art. 3 (1) of the Civil Code.[489] In general, personal autonomy comprises the freedom of a private person to decide on the addressee, content and a form of a legally relevant conduct and whether or not to do so.[490] This is also reflected in the field of personal data processing where a natural person can choose which controller to authorize to process her personal data, to what extent (i.e. for which specific purposes of processing) and whether she will do so orally or in writing.

In the area of personality rights, the exercise of personal autonomy is specified in particular in Art. 81-60 of the Civil Code. The "free choice of an individual to live as he pleases" is primarily protected.[491] Just as in the GDPR, the consent (which may be revoked) represents the main instrument for implementing personal autonomy of the person concerned. This consent never establishes a contractual relationship between the authorizing and the authorized party. Personality rights cannot be the subject to obligations, i.e. relative property rights. However, their scope also has limitations.[492] At the same time, however, such restrictions must not be disproportionately applied in such a way that they would conflict with the legitimate interests of the natural person concerned.[493]

4.2.3 Limitations of Personal Autonomy

The GDPR and the Civil Code provide extensive protection of the personal autonomy of data subjects. On the other hand, they also grant rights to controllers and individuals who have made and use records relating to a natural person in the context of personality protection, while protecting

[486] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.*
[487] Ibid., p 21.
[488] ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines for Identifying a Controller or Processor's Lead Supervisory Authority. In: *European Commission* [online]. 5. 4. 2017 [2019-12-08]. Available at: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235>.
[489] LAVICKÝ, P. et al. *Občanský zákoník I. Obecná část (§ 1−654). Komentář*, p. 5.
[490] Ibid., p. 56.
[491] See Art. 81 (1) of the CC.
[492] For more details see below.
[493] See Art. 90 of the CC.

absolute personality rights so that even the data subject's consent or consent cannot reverse that protection. The following subchapters will explain how natural persons are limited in their personal autonomy in relation to the processing of their biometric data.

4.2.3.1 General Data Protection Regulation

The main instrument of will autonomy in GDPR is the data subject's consent to the processing of personal data. In this context, however, it should be noted that here too the data subject's autonomy is limited. The processing is always subject to the processing principles of Article 5 of the GDPR, so that, for example, although the data subject could give the controller consent to the processing of data that is redundant and not related to the declared purpose of processing, such consent would not have legal effects.[494]

Personal autonomy is also somewhat modified in granting consent to the processing of biometric data for scientific research purposes. Here, according to Recital 33 of the GDPR, it is often not possible to "fully identify the purpose of personal data processing for scientific research purposes at the time of data collection". In the field of biometric data, behavioural biometric data processing is particularly critical. It gives the opportunity to examine patterns of behaviour of individuals that lead to their unique identification. The effects of such research are not yet known. However, it is confirmed that additional information regarding, for example, their age, sex or a particular disease can be derived from the behaviour of individuals. Scientific research can be carried out not only by academic institutions but also by businesses.[495] Scientific research must meet the criteria set out in Art. 89 of the GDPR at all times.

The GDPR protects natural persons from processing of their biometric data by the general rule of prohibiting such processing. However, Art. 9 (2) of the GDPR mentions nine exceptions under which controllers may process biometric data for unique identification without the consent of the data subject. These exemptions therefore limit the data subject's control over her own biometric data. However, processing under these exceptions is, of course, subject to the principles of the processing of personal data and the data subject may exercise his rights.

The first exception where a natural person must suffer is the processing of biometric data "for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject".[496] Under the Czech law, there is currently only one area, which explicitly lays down a biometric identification obligation for employees. Biometric identification is obligatory for the entry into nuclear facilities. The conditions of entry into the facility are regulated by a special decree.[497] Employees working in this facility are obliged to comply with the rules laid down in this Decree, based on Art. 106 c) of the Labour Code.[498] However, for example, employees whose labour obligations are regulated by a collective agreement will also have to bear biometric identification,[499] which allows such practice. In the absence of a collective agreement, an employer would not be able to process

[494] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on consent under Regulation 2016/679*.
[495] Recital 159 of the GDPR states that "the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research".
[496] See Art. 9 (2) b) of the GDPR.
[497] Decree no. 361/2016 Coll., on Security of Nuclear Installation and Nuclear Material.
[498] Act no. 262/2006 Coll., Labour Code, as amended.
[499] Collective agreements are regulated in Art. 23 et seq. Of the Labout Code.

the employees' biometric data without their explicit consent. If biometric identification was introduced when entering employer's premises, an employee would have to provide an alternative. The suggestion of an alternative is also a condition in labour-law relations for a possible consent to be regarded as granted freely. At the same time, an employee is always entitled to withdraw his consent. Employers should therefore take this into account and prepare for this possibility. Failure to give an explicit consent to the processing of biometric data shall not constitute grounds for terminating employment with an employee. At the same time, employers must ensure that appropriate safeguards are in place to safeguard the fundamental rights and interests of their employees.

The second exception is processing "necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent".[500] This is a logical exception in which vital interests outweigh the fundamental right to the protection of personal data.

The third exception is relatively problematic with regard to the processing of biometric data. It is obviously related more to the other specific categories referred to in Article 9 (1) of the GDPR, namely political opinions, philosophical beliefs or religion. Indeed, a special category may be processed "by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects".[501] At the same time, such processing should take place within the authorized activities of these bodies. The question is whether these entities can also process the biometric data of their members and ask them for example biometric identification when entering the building. A positive argument could be that in order to ensure the security of the members of these associations, given the sensitivity of the opinions and issues discussed here, it should be possible to require the highest possible degree of protection on entry. Religious communities in particular are often the target of various attacks. On the other hand, biometric identification is not content related to the activities of these subjects. Given the general principle of data minimization, the relevance of the processing is crucial here, and therefore the argument in favour of the possibility of applying the exemption to biometric data is unlikely to succeed.

The fourth exception allows the processing of "personal data which are manifestly made public by the data subject".[502] Characteristic features of biometric data are their visibility and accessibility. For instance, information on the characteristic appearance of the face, voice, walking or smell can be observed in a face-to-face meeting with a natural person. The fact that a natural person has appeared somewhere cannot be interpreted as the publication of biometric data and hence the reason for the use of the fourth exception. In this context, it should be noted that biometric data are understood to be data that have been produced by the specific technical processing of images or other records of the biological, physiological or psychological characteristics of a natural person. The fourth exception could only be applied if a natural person would disclose his biometric token, i.e. a digital representation of his unique features.

The fifth exception concerns processing "necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity".[503] Under this exception, it is envisaged, for example, to grant access to a biometric identification system and biometric data to

[500] See Art. 9 (2) c) of the GDPR.
[501] See Art. 9 (2) d) of the GDPR.
[502] See Art. 9 (2) e) of the GDPR.
[503] See Art. 9 (2) f) of the GDPR.

an expert witness who assesses in a possible litigation whether the controller has complied with all its obligations.

The sixth exception is processing "necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".[504] Public interest is a term that is relatively ambiguous. In general, it protects interests of a state or public corporations.[505] It remains a question as to which types of processing may be included under this exemption in the future. From the wording of the exception, it can be inferred that it is sufficient to refer to the public interest, which is formulated either in EU law or in the law of a Member State. However, this law does not need to explicitly require biometric identification. The purpose of this exemption is to provide a sufficient scope for the protection of the public interest without specific delegation. These may be formulated with reference to Article 9 (4) of the GDPR.

The seventh exception is "processing necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to [further]conditions and safeguards".[506] This exemption is obviously more likely to relate to personal data primarily indicative of health status or genetic data. It is difficult to imagine a situation in which it would be necessary to process biometric data providing a unique identification in this area. The identification of a natural person can be reliably achieved in other areas and therefore, in view of the principle of minimization, this exemption is unlikely to apply to biometric data. However, occurrence of a special case justifying the use of biometrics cannot be completely excluded.

The eighth exception is processing "necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy".[507] This exception can be used in the field of processing of biometric data, for example, to uniquely identify foreigners using a passport with biometric data in cases where it is assumed that these people can be infected with serious diseases, so as to avoid, for example, the confusion patients they are physically similar.[508]

And the last ninth exception is processing "necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes" that is based on either EU law or the law of a Member State.[509] Unless the law provides for such an objective, biometric data may only be processed with the explicit consent of the data subject.

These exemptions represent limits to the personal autonomy of the data subjects. In the past, biometric data could also be processed under the Personal Data Protection Directive for the sake of contract performance because biometric data were not considered sensitive personal data. It could

[504] See Art. 9 (2) g) of the GDPR.
[505] GERLOCH, A. Veřejný zájem. In: HENDRYCH, D. et al. *Právnický slovník*. Prague: C. H. Beck, 2009.
[506] See Art. 9 (2) h) of the GDPR.
[507] See Art. 9 (2) i) of the GDPR.
[508] In this context, however, it should be noted that even biometric identification is not absolutely reliable. The errors in the identification of unfortunately occurs for example in recognition of monozygotic twins. Mistakes have also been reported in fathers and sons.
[509] See Art. 9 (2) j) of the GDPR.

only be a contract in which biometric services were provided.[510] However, this possibility was in the Czech Republic excluded in 2004 by an amendment that introduced the concept of biometric data as a type of sensitive personal data.[511]

4.2.3.2 Personal Rights in the Civil Code

The exercise of personal autonomy in the area of personality rights is limited in the Civil Code in two ways. First, the Civil Code makes a number of exceptions where there is no need for permission to make and use a natural person's portrait, sound or image. In the field of biometrics, for example, face recognition, voice recognition or fingerprint technologies correspond to this.

Permission is not required in the case of Art. 88 (1) of the Civil Code, when these records are "made or used to exercise or protect other rights or legally protected interests of others". Here we can imagine a situation where a homeowner will require family members to enter a biometric system that protects access to her home. In so doing, she will not be considered to be a controller within the meaning of the GDPR, since she will carry out such processing by way of derogation under Article 2 (2) (c) of the GDPR as a purely household activity. This situation is quite controversial and affects in particular personality rights of family members living in this house. They come into conflict with the property rights of the homeowner. A proportionality test will be required to address such a situation. Authorization to make and use records is not necessary even if, pursuant to Art. 88 (2) of the Civil Code, this is "by means of a statute for official purposes, or where someone performs a public act in matters of public interest". The same applies under Art. 89 of the Civil Code to the making and appropriate use of records "for scientific or artistic purposes and for print, radio, television or similar coverage."

Secondly, as with the GDPR, a natural person cannot legitimize the acquisition and use of records of his or her person which are prohibited. The Civil Code now in Art. 1 (2) prohibits such agreements that violate "good morals, public order or the law concerning the status of persons, including the right to protection of personality rights". Only specific cases from practice show how these concepts are interpreted in relation to the processing of biometric data.

4.3 Right to Hide

Data subjects (users of technology) should be able to exercise their right to personal autonomy also with regard to their biometric data. However, this may not always be possible as users may not even know that their biometric data is processed. For instance, analysis of online behaviour can also fulfil definition of biometric data although not many people would consider it so.[512] Moreover, processing of biometric data for additional purposes such as voice analysis for mood indication can be performed unobtrusively and unrecognized by a user. At this situation a user faces a great disadvantage compared to the person who is "listening".

The question is whether a person is entitled to circumvent biometric systems and conceal her identity by different means. In other words, do data subjects have a right to hide? There is a number of ways how biometric systems can be easily circumvented. For instance, fingerprint scanners can

[510] Article 29 Data Protection Working Party. *Opinion 3/2012 on developments in biometric technologies.*
[511] Act no. 493/2004 Coll., Amending Act no. 101/2000 Coll., On the protection of personal data and on amending certain acts, as amended.
[512] KRAUSOVÁ, A. *Online Behavior Recognition: Can We Consider It Biometric Data Under GDPR?*

be circumvented with the help of 3D prints of fingers based on high-resolution photographs, 2D photographs of fingerprints on a conductive paper or even by providing false fingerprints in the enrolment phase. Facial recognition can be circumvented for instance with special dental implants or even make-up. Systems recognizing gait can be fooled by placing an object into a shoe or by placing a bandage around a knee. However, what are the legal limitations on the right to hide?

In the Czech law, there are three acts within public law that explicitly authorize people to conceal their identity, including biometrics. All of these acts relate to use of under-cover agents. In the sphere of private law, a number of aspects must be taken into account in assessing whether in a specific situation a person can conceal her identity. Hiding own identity can be considered as an expression of the right to self-determination (through change of one's own appearance). Limitations of the right to hide are given by the following provisions:

a) Czech Charter of Fundamental Human Rights and Freedoms: Everyone can do what is not forbidden by law, and no one must be forced to do what the law does not impose;

b) Civil Code:

    a. Right to privacy protection;

    b. Principle of honesty: in this case the content of the principle of honesty depends on the circumstances of the particular case – the principle of the autonomy of the will is limited by the principle of legal certainty and trust in acts of other persons;

    c. Preventive duty: if circumstances of the case or custom of private life so require, everyone is obliged to act in such a way that there is no undue detriment to the freedom, life, health or property of another;

    d. Self-help: everyone can reasonably help his own right if this right is compromised and if it is obvious that the intervention of public power would come too late.

c) GDPR: There is no explicit obligation for the data subject to provide correct information.

Moreover, the right to hide is limited by specific acts of public law, such as laws on travel documents, ID cards, criminal laws, et.

Given the above mentioned, one must conclude that the right to hide cannot be formulated absolutely. Hiding of biometric data is acceptable for instance in cases when a person acts without the intention to commit fraud or harm to another person (e.g. logging of false biometric data into own device, make-up and masking own identity in publicly monitored premises, etc.). On the other hand, examples of unacceptable hiding of biometric data are for instance change of voice in communication with a bank, use of fake biometric data for travel documents, or acting with intention to cause harm.

5. Recommendations for Data Controllers

As it has been illustrated in the previous chapters, processing of biometric data is rather specific compared to other types of personal data. The GDPR lays down principles and obligations that are common for more categories. However, particular questions may arise when biometrics is used in various contexts. This chapter provides an overview of these problems and attempts to provide answers as well.

5.1 Adhering to Principles of Personal Data Processing

Principles relating to processing of personal data are defined in Art. 5 of the GDPR and are common for any processing of personal data. There are in total seven principles: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability.

5.1.1 Lawfulness, Fairness and Transparency

The notion of lawfulness refers to processing biometric on the legitimate basis of one of the grounds defined in Art. 9 (2) of the GDPR (see Section 5.2). The notion of fairness excludes processing of biometric data in a covert manner, i. e. without the knowledge of the data subject.[513] This principle is especially important for situations in which online activities of a user are monitored for her unique identification as well as for her profiling. As it has been already illustrated in Section 2.2.1.3, in the online world profiling and biometrics are closely intertwined. In accordance with the requirement on transparency, the controller must disclose her identity in a prescribed manner and to make an effort to inform data subjects about the fact that processing is taking place. The GDPR expressly specifies that "[n]atural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing".[514] Particular requirements on provision of information is specified in Art. 12 – 14 of the GDPR.

With regard to biometric data, controllers should provide data subjects with specific information as to the risks, rules and safeguards of the processing. Each biometric system is individual and processes information in accordance with a specific algorithm and based on data of varying quality depending on the type and quality of a sensor used for acquiring biometric data. Therefore, each system guarantees a different level of privacy.[515]

---

[513] RÜCKER, D. – KUGLER, T. (eds). *New European Data Protection Regulation. A Practitioner's Guide Ensuring Compliant Corporate Practice*. Baden-Baden: Nomos, 2018, p. 52.

[514] See Recital 39 of the GDPR.

[515] There are more notions of the concept of privacy. Private matters are for instance those matters that are not public. In this book we understand privacy in terms of relating to what is "individual, personal, or one's own". See GONZÁLES FUSTER, G. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Springer, 2014, p. 22.

There have been attempts to define privacy levels with regard to potential correlation of databases.[516] However, levels of privacy protection can be defined with regard to what data are acquired, stored and later processed within a biometric system. Depending on these variables, five levels of privacy protection can be identified, while the first level provides the highest protection to data subjects (lowest degree of vulnerability) and the fifth level provides the lowest protection (highest degree of vulnerability.

The following table illustrates processing of raw and biometric data and their influence on the level of privacy protection:

Level of privacy protection	Processing and storage of raw and biometric data
1 (highest)	Raw data acquired, processed, raw data discarded, only processed data kept (a biometric template)
2	Raw data acquired, processed, raw data kept, processed data kept (together with the raw data/separately from the raw data – safer practice)
3	Raw data acquired, processed, raw data kept, processed data kept, raw data processed with a new algorithm, old processed data discarded
4	Raw data acquired, processed, raw data kept, processed data kept, raw data processed with a new algorithm, old processed data kept
5 (lowest)	Raw data acquired, processed, raw data kept, processed data kept, raw data processed with a new algorithm, old processed data kept, comparison of raw data and analysis of developments (possibilities to derive new information)

Table 1.: Levels of Privacy Protection

Data subjects should be informed about the level of privacy provided by the system. Information about risks related to processing biometric data also depends on the level of privacy protection. The amount of data stored determines higher risk of reverse engineering, alteration of data, or deriving sensitive information from the data. The more data are stored, the more serious impact on rights and freedoms of an individual a potential attack would have.

The requirement of securing transparency is most often fulfilled by a document commonly titled Privacy Policy.

5.1.2 Purpose Limitation

The principle of purpose limitation with regard to biometric data especially calls for specification whether biometric data is going to be used only for verification/identification purposes or whether the data will be used also for acquiring additional information about an individual including profiling. A purpose must be specified, explicit and legitimate. The requirement on legitimacy of a purpose is rather complicated. When assessing compliance of a purpose, the law must be taken in account in its broadest sense.[517] This refers to "all forms of written and common law, primary and secondary

[516] SADHYA, D. – SINGH, S. K. *Privacy risks ensuing from cross-matching among databases: A case study for soft biometrics.*

[517] RÜCKER, D. – KUGLER, T. (eds). *New European Data Protection Regulation. A Practitioner's Guide Ensuring Compliant Corporate Practice*, p. 57.

legislation, municipal decrees, judicial precedents, constitutional principles, fundamental rights and other legal principles, as well as jurisprudence. Furthermore, when determining whether a particular purpose is legitimate, it may also be necessary to consider customs, codes of conduct, codes of ethics, contractual arrangements, and the general context and facts of the case, including the nature of the relationship between the controller and the data subjects".[518] Under the Czech law, controllers will have to take in account especially the requirements of compliance with good morals, public order and provisions on personality protection. This must be especially taken in account when considering processing of biometric data in a manner that is incompatible with initially specified purposes. Processing biometric data for scientific purposes is a provision that can be exploited for circumventing strict rules and principles on processing biometric data. However, such processing shall be examined especially with regard to the principles of good morals. So called compatibility test must be performed as well.[519]

5.1.3 Data Minimisation

The principle of data minimisation refers to the requirement that the controller should collect and process only the data that is "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".[520] With regard to the levels of privacy protection specified above, the controller must provide specific reasons for processing data at the levels 2 – 5. This requires knowledge of the controller as to the functioning of the respective biometric system.

5.1.4 Accuracy

The principle of accuracy requires that the controller keeps biometric data up to date. This in fact implies that the controller needs to update a biometric template of the data subject in case when the physical appearance of a person changes. This can be a case when a person loses fingers in an accident or when she undergoes plastic surgery. Especially in cases of plastic surgery the controller needs to be extra careful. Plastic surgery can be done not only to correct a medical condition or to improve physical appearances. It can be also used for circumventing biometric systems and possibly also for identity theft.[521] Moreover, when requesting and acquiring new biometric template, the controller needs to have respect to personality rights, namely to the human dignity. Rectification must be done without delay.

5.1.5 Storage Limitation

The principle of storage limitation works with the notion of necessity. Time limits for storing biometric data should be determined by internal policies. Again, this principle provides an exception for processing data for "archiving purposes in the public interest, scientific or historical research purposes or statistical purposes".[522] The same concerns as with the exception to purpose limitation pertain.

---

[518] Ibid.
[519] Ibid., p. 60 et seq.
[520] See Art. 5 (1) c) of the GDPR.
[521] BHATT, H. S. – BHARADWAJ, S. – SINGH, R. – VATSA, M. Face Recognition and Plastic Surgery: Social, Ethical and Engineering Challenges. In: KUMAR, A. – ZHANG, D. (eds). *Ethics and Policy of Biometrics. Third International Conference on Ethics and Policy of Biometrics and International Data Sharing, ICEB 2010Hong Kong, January 4-5, 2010. Revised Selected Papers*. Springer, 2010.
[522] See Art. 5 (1) e) of the GDPR.

5.1.6 Integrity and Confidentiality

This principle requires from the controller to secure an appropriate level of security of biometric data. The level of security measures must correspond to potential risks. The GDPR provides more specific guidelines as to various measures that could be implemented in order to protect personal data in Art. 32. When assessing the risks, controllers should also consider the level of protection guaranteed in their system.

5.1.7 Accountability

According to this principle, the controller is responsible for and must "be able to demonstrate compliance with" all the above mentioned principles.[523] This principle is tightly connected to determining liability of the controller for damage that occurs in relationship with processing of personal data. This principle in fact requires the controller to be able to prove at any moment of processing that she has complied with all legal requirements. The GDPR states that "[a]ny controller involved in processing shall be liable for the damage caused by processing which infringes"[524] the GDPR. At the same time the controller can be exempt from this liability "if it proves that it is not in any way responsible for the event giving rise to the damage."[525]

5.2 Respecting Legal Grounds for Processing Biometric Data

As it has been stated several times in the previous chapters, processing of biometric data is in general prohibited. However, controllers can process biometric data in specific cases. These are specified in Art. 9 (2) of the GDPR. Choosing an appropriate title for processing biometric data corresponds to the principle of fairness. In this regard it is very important for a controller to be able to justify selection of the appropriate title for processing. The most critical title for processing is processing for scientific purposes.[526] Controllers must be able to properly justify the purpose, design and social benefit of such research. At the same time controllers need to comply with requirements set out in Art. 89 of the GDPR that requires putting in place technical and organisational measures that would guarantee adhering to the principle of data minimisation.

5.3 Fulfilling Rights of Data Subjects

The GDPR formulates three rights of data subjects that are especially interesting when applied in the context of biometrics.

[523] See Art. 5 (2) of the GDPR.
[524] See Art. 82 (2) of the GDPR.
[525] See Art. 82 (3) of the GDPR.
[526] In personal data processing, research is considered to have „ a relatively strong position in comparison with other sectors of society". See CORRALES, M. – FENWICK, M. – FORGÓ, N. (eds). *New Technology, Big Data and the Law*. Singapore: Springer Nature, 2017, p. 61.

5.3.1 Right to Be Forgotten

The right to be forgotten, or the right to erasure is set out in Art. 17 of the GDPR. According to this provision, "[t]he data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay" if one of specified ground applies. Although the aim of this right is to provide higher protection of individuals in the online world, it is sometimes being criticized as a potential tool for limiting the freedom of expression.[527]

Application of this right may prove difficult in situations in which biometric data is used for profiling and for creating various models with help of machine learning techniques. These techniques may be used to analyse behaviour of people for determining their future actions. Information derived from patterns of their behaviour may not be easily erased from such model. It is, therefore, necessary that data used for training intelligent models are not personal data as this is the surest way how to avoid complications with operation of those intelligent models.

5.3.2 Right to Data Portability

This right is set out in Art. 20 of the GDPR. According to Art. 20 (1) "[t]he data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided" on the condition that processing of personal data is based either on consent or on a contract and at the same time "the processing is carried out by automated means". The aim of this provision is to "strengthen the competition among service providers for customers and, in doing so, foster the development of privacy-friendly technologies and interoperable data formats".[528]

According to this provision, the data subject has the right to be provided with a biometric template stored in the controller's database. However, practical issues rise as to the transferability of this biometric template. Biometric systems differ based on (usually proprietary) algorithms that may not be compatible with each other. There are various technical standards for exchanging biometric information (such as ISO Common Biometric Exchange Formats Framework, or ANSI/NIST-ITL standard). Technical feasibility is the criterion for exercising the right to transferring biometric data from one controller to another. At the same time, it is, however, questionable whether the controller needs to accept a transferred biometric template from another controller with regard to her obligation to maintaining certain level of security measures in own system. Controllers should have a policy in place for such cases and for instance verify the provided biometric template with regard to the principle of accuracy.

[527] GAUDAMUZ, A. Developing a Right to be Forgotten. In: SYNODINOU, T.-E. – JOUGLEUX, P. – MARKOU, Ch. – PRASTITOU, T. (eds). *EU Internet Law. Regulation and Enforcement*. Cham: Springer, 2017.

[528] VOIGT, P. – VON DEM BUSSCHE, A. *The EU General Data Protection Regulation (GDPR). A Practical Guide*. Cham: Springer, 2017, p. 169.

5.3.3 Right not to Be Subject to Automated Decision-Making and Profiling

According to Art. 22 (1) of the GDPR "[t]he data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." 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".[529]

This right is very relevant for systems using biometric data as the inherent characteristics of these systems is automated decision making with regard to identification or verification of identity of a person. A typical result of automated decision-making in this area is a decision whether to allow a person to enter certain premises or even whether to cross a border. With regard to profiling, results can vary. The GDPR itself warns against discriminatory effects that such practice could have on involved data subjects. Moreover, the GDPR requires use of "mathematical or statistical procedures for the profiling" and implementation of "technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimise".[530]

5.4 Specific Obligations

Apart from the above mentioned principles of data processing and rights of data subjects, the GDPR sets out specific obligations for controllers that relate to putting in place certain organizational and technical measures. These consist in securing appropriate protection of the data while having in mind concepts of Privacy by Design and Privacy by Default. Particular conditions are set out in Art. 32 of the GDPR.

Moreover, controllers are obliged to keep records of their processing activities under Art. 30 of the GDPR or to perform Data Protection Impact Assessment in accordance with Art. 35 of the GDPR. Performing DPIA is especially relevant for cases of processing biometric data. The assessment aims to mitigate risks related to processing certain categories of personal data (including biometric data and profiling) and processing data on a large scale. The GDPR sets out minimum requirements of the DPIA: "a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; an assessment of the necessity and proportionality of the processing operations in relation to the purposes; an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned."[531]

[529] See Art. 4 (4) of the GDPR.
[530] See Recital 71 of the GDPR.
[531] See Art. 35 (7) of the GDPR.

5.5 Data Vulnerability and Privacy Policy

When fulfilling their obligations, data controllers always need to take in account the specific nature of biometric data and its potential to increase vulnerability of data subjects. As it has been illustrated in subchapter 1.3.1.4, biometric data can be further analysed for additional information such as soft biometric characteristics or biomarkers. This intrinsically embedded information augments indicative value of biometric data beyond mere identification of a human being.

Each type of biometric data contains some additional information. When deciding about which type of biometric data to use, controllers should choose the appropriate type of data also with regard to its potential to harm a data subject by revealing data that in case of being misused would have a significant negative impact on rights and freedoms of the respective individual.

In order to assess the potential to increase vulnerability of a data subject, in 2017 we performed a literature review aimed to identify what additional information could be under certain circumstances derived from raw data based on which biometric templates are created. Results of the review can be found in Annex I. Five most common types of biometric data were chosen: fingerprint, face, iris, voice, and keystroke dynamics. For each type of the data we attempted to identify research that proves possibility to reveal additional information about identity of a person (gender, age, ethnic origin, etc.), her mental state (level of stress, type of currently experienced emotion, etc.), other information (such as bodily functions, performance in tasks, attractiveness, etc.), and about diseases that a person is suffering together with potential complications related to this disease (potential complications can be used for instance for marketing purposes in order to sell certain products to a person more efficiently or can result in discrimination of a person by excluding her from certain activities or terminating her employment contract based on her potential health complications).

The following table illustrates findings from the research report published in Annex I. A possibility to derive additional information from a respective type of biometric data in a certain category is marked by X and followed by indication in brackets of how many types of information in that category can be derived. The category of complications does not contain the number as the complications from various diseases often overlap or may not be exhaustive.

Type of biometric data	Identity	Mental state	Other	Disease	Complications
Fingerprint	X (2)	X (2)	X (4)	X (11)	X
Face	X (3)	X (1)	X (1)	X (37)	X
Iris				X (9)	X
Voice	X (2)	X (2)	X (3)	X (7)	X
Keystroke dynamics	X (2)	X (1)		X (2)	X

Table 2.: Assessment of Data Vulnerability based on Annex I.

Based on these findings, it is obvious that face provides the greatest amount of information regarding the identity and diseases of a person including related complications. On the other hand, iris provides only information about diseases and related complications. Probably the most used type of biometric data, a fingerprint, can be analysed for a quite broad range of additional information.

In case we would take into account only the number of results of the research report, the types of biometric data that provide lowest to greatest number of information would be sorted as follows: keystroke dynamics, iris, voice, fingerprint, and face. However, such classification can fail in the real world scenarios and may be used only as a supporting information for controllers who are about to design their biometric systems and need to perform Data Protection Impact Assessment.

There are several reasons why the results cannot be generalized. First of all, extracting or deriving information from a person depends on sensors that capture information about a human body or behaviour. These sensors can vary in quality of captured raw data and for instance resolution of an image can play a significant role regarding the amount of captured data. Next, algorithms used for analysis and processing of the raw data vary in their capabilities. Moreover, a provided level of privacy protection (see subchapter 5.1.1) plays a great role as to the amount of data available for a potential analysis of additional information as well as to the overall level of vulnerability of a respective person. One also needs to take in account that sensors and algorithms may produce incorrect information which – depending on circumstances – may lower or rise vulnerability of a person.

Vulnerability should be understood as a context-dependant concept. It is due to the fact that in various settings various information may prove to be discriminatory. In some cases, health information may be discriminatory, in others not depending on the purpose for which the information was identified at the first place. Therefore, especially in context of biometric data processing, a thorough DPIA is necessary. A controller needs to identify risks for a data subject and with respect to own obligations including principles of personal data processing set up an appropriate technical, organizational and legal framework in order to protect data subjects.

What concerns the legal framework, a controller is responsible for drafting a document generally titled as Privacy Policy. The aim of this document is usually to inform data subjects about the controller, the purposes of processing personal data, rights of data subjects etc. With regard to the varying degrees of vulnerability as well as provided levels of protection of biometric data, a privacy policy should provide clear and concise information to data subjects.

The main instrument of a data subject for exercising control over own personal data and personal autonomy is her consent. According to Rec. 32 of the GDPR, “[c]onsent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them.” A controller then needs to acquire consent of a data subject for each purpose individually and properly distinguish purposes of processing. This should be reflected in a privacy policy. With regard to the levels of privacy protection, a privacy policy should also clarify why additional data is processed (levels 2 – 5). Where technically possible, a data subject should be given a choice as to the level of privacy protection.

Conclusion

"*They who can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety*."

Benjamin Franklin

In many ways, biometric data represent the core of our identity. They refer not only to our physical appearance but in a broader sense also to the state of our mind and overall well-being and health. Despite we do not usually hide these characteristics from other people and tend to share this information with others, we should be much more careful when communicating this information via electronic means. Automated recognition of patterns in our physical appearance, in physical functioning of our body or in our behaviour can not only distinguish who we are but also how are we. In a face to face communication and interaction with another person this would not be a problem. In such a situation we are also able to assess what is going to happen with our data as we are also observing the other person and deriving at least intuitively certain information how the other person is and what her intentions might be. However, in the digital environment we face a significant information asymmetry as the communication of personal information is usually one way – from users of a certain service to its provider. In this situation we have to rely on the information from the provider's side about what shall happen with our personal data. Sometimes we might not receive this information at all. Moreover, given the nature of biometric data, we may not even know that our personal data is being gathered and further processed.

This book has illustrated that biometric data are very rich as to their indicative value. Despite being used primarily for identification or verification purposes and defined so by the GDPR, biometric data in general have much broader meaning and, thus, can be used for many more purposes than just for identification. Information available from raw biometric data can be used for extracting additional indication about a person – information such as racial or ethnic origin, gender, age, or health can be easily derived for instance from photographs used for creating biometric template for facial recognition. Monitoring of person's behaviour (such as monitoring online activity or patterns of interaction with electronic devices) intended originally for identifying a person in the digital environment can even provide information about capabilities or intentions of a person.

Specificities of biometric data, such as their linkability to a particular individual or a permanent impact on an individual when the data is compromised, increase vulnerability of a person whom the data refers to. Moreover, there is a number of specific risks related to the use of biometric data, such as risks related to the very design of biometric systems (opacity of biometric systems, biometric surveillance, possibility of cross-matching the data, augmented indicative value, discriminative decision-making, or inefficient cybersecurity), risks related to attacks on biometric systems, and even risks related to legislation regulating use of biometric systems (namely exceptions for using biometrics for security purposes that might not provide sufficient safeguards and open space to further processing of additional information acquired from biometric data).

The significance of biometric data has been recognized at the level of the international law and later on at the level of EU law. Biometric data have been mentioned in international conventions and in

the EU their specificities have been recognized primarily in the opinions and documents of WP29. The GDPR fully recognized the special status of biometric data and provided stricter rules for their processing. Moreover, the GDPR adopted specific rules that significantly influence processing of biometric data. These are namely exceptions from the general prohibition of processing specific categories of personal data as well as rules related to profiling and the right not to be subject to automated decision making. At the same time the GDPR provides space for national derogations and enables EU Member States to maintain or introduce new provisions on processing biometric data at the national level. Some states, such as Germany, have introduced quite detailed rules for processing biometric data in various situations, while others, such as the Czech Republic, rely on the general provisions of the GDPR. Moreover, the processing of biometrics will be affected by future regulation of artificial intelligence which is a technology that is used in processing biometric data (pattern identification, forecasting models, etc.).

As it has been mentioned, the Czech Republic relies mainly on the provisions of the GDPR with regard to the rules for processing biometric data. The Czech Personal Data Processing Act that was adopted in reaction to the GDPR does not contain any specificities regarding biometrics. However, there is a number of other laws that regulate it. In general, Czech constitutional laws have precedence over the EU law including the GDPR. Moreover, there are public laws regulating use of biometric data for identification purposes (e.g. identification documents, powers of authorities on acquiring biometric data, or obligatory use of biometrics for entry into nuclear facilities). The GDPR and the Czech Personal Data Processing Act also overlap with personality protection defined in the Czech Civil Code. Specificities of processing biometric data appear in various application domains, such as dynamic biometric signature, processing biometric data for health purposes of for purposes of criminal proceedings, or even for the purposes of so called neuromarketing.

Personal autonomy of data subjects regarding decision-making about processing of their biometric data by other subjects is limited. The main instruments for exercising the right to personal autonomy with regard to biometrics is the consent of a person without which processing of biometric data would be unlawful. However, the GDPR provides a list of exceptions under which biometric data can be processed without such explicit consent of a data subject. Out of all those exceptions the most dangerous exception is processing for the purposes of scientific research. Scientific research is a broad term that can cover a number of activities. Moreover, this term may cover also activities of private companies that might misuse its original meaning for circumventing the general prohibition of processing biometric data without a consent. Another instrument for exercising the right to personal autonomy can be defined as the “right to hide” and refers to the legally approved (or at least not prohibited) possibility of a person to fool a system processing biometric data. In general, concealing one’s own identity is approved only for undercover agents. However, each person has the right to personal self-determination. This means that a person has an innate freedom to change her body, behaviour, and clothing in the way she pleases. Such changes can then help her to “hide” from the system by not being identifiable any more. However, this right is limited by certain legal provisions, for instance prohibition of fraudulent behaviour.

In practice personal autonomy can by limited also by inability of a person to efficiently enforce her rights. This can relate mainly to her unawareness about processing of her biometric data. It is impossible to fight against unlawful practice if we do not know that such practice is taking place. Therefore, it is of the utmost importance that controllers who process biometric data act as responsible as possible. They need to be aware of the risks that the technology poses to data subjects. Ideally, controllers should not only provide data subjects with various safeguards but also with flexibility regarding decision-making about the level of privacy that data subjects require. This can be done in the form of different consents for different purposes of processing.

In the future, processing of biometric data and profiling shall overlap to a much greater extent. In privately operated systems, it will be done so for the purposes of cybersecurity, optimization of services to users as well as for the purpose of more efficient marketing or influencing users in other ways. Expanding in processing biometric data is, however, presumed also in systems operated by public authorities – typically operation of cameras in public spaces equipped with technology of facial recognition and an alert system in case a wanted person is identified. Unfortunately, this type of efficient processing can be used for malicious purposes as well. In this regard, debates about protection of democracy start to appear more and more often. The Chinese system of biometric surveillance combined with profiling and creation of social credit scoring system is an example of technologically enabled highly efficient state control that may lead to significant violation of fundamental human rights. Unfortunately, such a system can be also easily implemented in the digital environment within an online platform operated by a private subject.

Given these examples, it is everyone's responsibility to take a proper care of own biometric data and to disclose them with care. Although for instance using a face for unlocking a smartphone may be comfortable, consequences of providing raw biometric data can be much more serious that we can currently imagine.

List of References

Books:

[1.] AZUAJE, F. *Bioinformatics and Biomarker Discovery. "Omic" Data Analysis for Personalized Medicine*. Chichester: John Wiley & Sons, Ltd., 2010. ISBN 978-0-470-74460-4.

[2.] BAUMAN, Z. *Liquid Modernity*. Cambridge: Polity Press, 2002. ISBN 0-7456-2410-3.

[3.] BĚLINA, M. – DRÁPAL, L. a kol. *Zákoník práce: komentář*. Praha: C. H. Beck, 2012. ISBN 978-80-7179-251-2.

[4.] BOBEK, M. – BOUČKOVÁ, P. – KÜHN, Z. (eds). *Rovnost a diskriminace*. Praha: C. H. Beck, 2007. ISBN 978-80-7179-584-1.

[5.] CAMENISCH, J. – LEENES, R. – SOMMER, D. (eds). *Digital Privacy. PRIME – Privacy and Identity Management for Europe*. Heidelberg: Springer, 2011. ISBN 978-3-642-19049-0.

[6.] CAMPISI, P. (ed). *Security and Privacy in Biometrics*. 2nd Vol. London: Springer-Verlag, 2013. ISBN 978-1-4471-5230-9.

[7.] CORRALES, M. – FENWICK, M. – FORGÓ, N. (eds). *New Technology, Big Data and the Law*. Singapore: Springer Nature, 2017. ISBN 978-981-10-5037-4.

[8.] DUNSTONE, T. – YAGER, N. *Biometric System and Data Analysis. Design, Evaluation, and Data Mining*. New York: Springer, 2009. ISBN 978-0387776255.

[9.] DOOLEY, R. *Brainfluence. 100 Ways to Persuade and Convince Consumers with Neuromarketing*. Hoboken: Wiley, 2012. ISBN 978-1-118-17594-1.

[10.] GONZÁLES FUSTER, G. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Springer, 2014. ISBN 978-3-319-05022-5.

[11.] HARCOURT, B. *Against Prediction. Profiling, Policing, and Punishing in an Actuarial Age*. Chicago: The University of Chicago Press, 2007. ISBN 978-0226316147.

[12.] HILDEBRANDT, M. – GUTWIRTH, S. (eds). *Profiling the European Citizen. Cross-Disciplinary Perspectives*. Dordrecht: Springer, 2008. ISBN 978-1-4020-6914-7.

[13.] HILDEBRANDT, M. *Smart Technologies and the End(s) of Law*. Cheltenham: Edward Elgar Publishing, 2015. ISBN 978-1-84980-876-7.

[14.] JOHAR, S. *Emotion, Affect and Personality in Speech. The Bias of Language and Paralanguage*. Springer, 2016. ISBN 978-3319280455.

[15.] KABELOVÁ DOLEJŠOVÁ, K. *Zákaz diskriminace jako právní problém v judikatuře Evropského soudu pro lidská práva*. Praha: Univerzita Karlova v Praze, Právnická fakulta, 2012. ISBN 978-80-87146-60-6.

[16.] KINDT, E. J. *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis*. Dordrecht: Springer, 2013. ISBN 978-94-007-7521-3.

[17.] KMEC, J. – KOSAŘ, D. – KRATOCHVÍL, J. – BOBEK, M. *Evropská úmluva o lidských právech. Komentář*. Praha: C. H. Beck, 2012. ISBN 978-80-7400-365-3.

[18.] KNAPP, V. *O možnosti použití kybernetických metod v právu*. Praha: Nakladatelství Československé akademie věd.

[19.] KNAPP, V. *Právo a informace*. Praha: Academia, 1988.

[20.] KUČEROVÁ, A. – NOVÁKOVÁ, L. – FOLDOVÁ, V. – NONNEMANN, F. – POSPÍŠIL, D. *Zákon o ochraně osobních údajů. Komentář.* Praha: C. H. Beck, 2012. ISBN 978-80-7179-226-0.

[21.] Lavický, p. et al. *Občanský zákoník I. Obecná část (§ 1−654). Komentář*. Prague: C. H. Beck, 2014. ISBN 978-80-7400-529-9.

[22.] LESSIG, L. *Code V.2*. New York: Basic Books, 2006. ISBN 978-1441437648.

[23.] LYON, D. *The Electronic Eye: The Rise of the Surveillance Society*. Minneapolis: University of Minnesota Press, 1994. ISBN 0-8166-2515-8.

[24.] MARX, G. T. *Undercover: Police Surveillance in America*. Berkeley: University of California Press, 1988. ISBN 0-520-06969-2.

[25.] MASON, S. *Electronic Signatures in Law*. Cambridge: Cambridge University Press, 2012. ISBN 978-1-911507-01-7.

[26.] MATEJKA, J. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí.* Praha: CZ.NIC, 2013. ISBN 978-80-904248-7-6, 256 s. Available at: <https://knihy.nic.cz/files/nic/edice/jan_matejka_ijop.pdf>.

[27.] MATOUŠOVÁ, M. – HEJLÍK, L. *Osobní údaje a jejich ochrana*. 2nd edition. Praha: ASPI, Wolters Kluwer, 2008. ISBN 80-7357-322-9.

[28.] MAYER-SCHÖNBERGER, V. – CUKIER, K. *Big Data: a revolution that will transform how we live, work and think*. London: John Murray, 2013. ISBN 978-1-84854-790-2.

[29.] MELZER, F. – TÉGL, P. a kol. *Občanský zákoník. Velký komentář. III. Svazek*. Praha: Leges, 2014. ISBN 978-80-87576-73-1.

[30.] MICHAEL, MG – MICHAEL, K. A Note on "Überveillance". In: MICHAEL, MG. *The Second Workshop on the Social Implications of National Security. From Dataveillance to* Überveillance and the Realpolitik of the Transparent Society [online]. 2007 [2014-08-14]. Available at: <http://works.bepress.com/cgi/viewcontent.cgi?article=1050&context=kmichael>.

[31.] MILLET, L. I. – PATO, J N. (eds). *Biometric Recognition: Challenges and Opportunities*. National Academies Press, 2010. EISBN 9780309142083.

[32.] MINELLI, M. – CHAMBERS, M. – DHIRAJ, A. B*ig Data, Big Analytics: Emerging Business Intelligence and Analytic Trends for Today's Businesses*. Hoboken: John Wiley & Sons, Inc., 2012. ISBN 978-1118147603.

[33.] MOLEK, P. *Právo na spravedlivý proces*. Praha: Wolters Kluwer ČR, 2012. ISBN 978-80-7357-879-4.

[34.] MORDINI, E. – TZOVARAS, D. (eds). *Second Generation Biometrics: The Ethical, Legal and Social Context*. Dordrecht: Springer, 2012. ISBN 978-94-007-3891-1.

[35.] NAFUS, D. (ed). *Quantified. Biosensing Technologies in Everyday Life*. Cambridge, MA: The MIT Press, 2016. ISBN 9780262528757.

[36.] NIEUWENHUIS, A. J. *Tussen privacy en persoonlijkheidsrecht*. Nijmegen: Ars Aequi Libri, 2001. ISBN 9789069164281.

[37.] NORRIS, C. From personal to digital CCTV, the panopticon, and the technological mediation of suspicion and social control. In: LYON, D. (eds). *Surveillance as social sorting: Privacy, risk and automated discrimination*. London: Routledge, 2003. ISBN 0-203-99488-4.

[38.] PETROV, J. – VÝTISK, M. – BERAN, V. a kol. *Občanský zákoník. Komentář.* C. H. Beck, 2017. ISBN: 978-80-7400-653-1.

[39.] POLČÁK, R. *Internet a proměny práva*. Praha: Auditorium, 2012. ISBN 978-80-87284-22-3.

[40.] POLČÁK, R. a kol. *Právo informačních technologií*. Praha: Wolters Kluwer ČR, 2018. ISBN 978-80-7598-045-8.

[41.] RAINEY, B. – WICKS, E. – OVEY, C. *The European Convention on Human Rights*. 6th edition. Oxford: Oxford University Press. ISBN 978-0-19-965508-3.

[42.] RAK, R. – MATYÁŠ, V. – ŘÍHA, Z. *Biometrie a identita člověka: ve forenzních a komerčních aplikacích*. Praha: Grada, 2008.

[43.] RAZ, J. *The Morality of Freedom*. Oxford: Clarendon Press, 1988. ISBN 9780198248071.

[44.] RENVOISÉ, P. – MORIN, Ch. *Neuromarketing. Understanding the "Buy Buttons" in Your Customers Brain*. Nashville: Thomas Nelson, 2007. ISBN 978-0-7852-2680-2.

[45.] REVETT, K. *Behavioral Biometrics. A Remote Access Aproach*. Hoboken: Wiley, 2008. ISBN 978-0470518830.

[46.] RÜCKER, D. – KUGLER, T. (eds). *New European Data Protection Regulation. A Practitioner's Guide Ensuring Compliant Corporate Practice*. Baden-Baden: Nomos, 2018. ISBN 978-3-8487-3262-3.

[47.] SLOBOGIN, Ch. *Proving the Unprovable. The Role of Law, Science, and Speculation in Adjudicating Culpability and Dangerousness*. Oxford: Oxford University Press, 2007. ISBN 9780195189957.

[48.] STEINER, Ch. *Automate This. How Algorithms Came to Rule Our World*. London: Penguin Books, 2012. ISBN 978-1-101-57215-3.

[49.] SVOBODA, P. et al. *Právní a daňové aspekty e-obchodu*. Praha: Linde Praha, 2001. ISBN 80-7201-311-4.

[50.] SYNODINOU, T.-E. – JOUGLEUX, P. – MARKOU, Ch. – PRASTITOU, T. (eds). *EU Internet Law. Regulation and Enforcement*. Cham: Springer, 2017. ISBN 978-3-319-64954-2.

[51.] ŠÁMAL, P. a kol. *Trestní řád. Komentář*. 7th ed. Praha: C. H. Beck, 2013. ISBN 978-80-7400-465-0.

[52.] ŠVESTKA, J. a kol. *Občanský zákoník. Komentář. Svazek I*. Wolters Kluwer, 2014. ISBN 978-80-7478-370-8.

[53.] VACCA, J. R. *Biometric Technologies and Verification Systems*. Oxford: Elsevier, 2007. ISBN 978-0-7506-7967-1.

[54.] VOIGT, P. – VON DEM BUSSCHE, A. *The EU General Data Protection Regulation (GDPR). A Practical Guide*. Cham: Springer, 2017. ISBN 978-3-319-57958-0.

[55.] WÁGNEROVÁ, E. a kol. *Listina základních práv a svobod. Komentář*. Praha: Wolters Kluwer ČR, 2012. ISBN 9788073801403.

[56.] *Webster's Encyclopedic Unabridged Dictionary of the English Language*. New York: Random House, 1996. ISBN 978-0517150269.

[57.] WIENER, N. *The Human Use of Human Beings: cybernetics and society*. London: Free Association Books, 1989. ISBN 978-1-118-97793-4.

[58.] WRIGHT, D. – DE HERT, P. (eds). *Enforcing Privacy. Regulatory, Legal and Technological Approaches*. Springer, 2016. ISBN 978-3-319-25045-8.

Book chapters:

[59.] ANDRONIKOU, V. – YANNOPOULOS, A. – VARVARIGOU, T. Biometric Profiling: Opportunities and Risks. In: HILDEBRANDT, M. – SERGE, G. *Profiling the European Citizen. Cross-Disciplinary Perspectives*. Dordrecht: Springer, 2008. ISBN 978-1-4020-6914-7.

[60.] BANSE, C. – HERRMAN, D. – FEDERRATH, H. Tracking Users on the Internet with Behavioral Patterns: Evaluation of its Practical Feasibility. In: GRITZALIS, D. – FURNELL, S. – THEOHARIDOU, M. (eds). *27th IFIP TC 11 Information Security and Privacy Conference, SEC 2012* Heraklion, Crete, 4–6 June 2012, Berlin: Springer. ISBN 978-3-642-30436-1.

[61.] BHATTASALI, T. et al. A Survey of Security and Privacy Issues for Biometrics Based Remote Authentication in Cloud. In: *13th IFIP International Conference on Computer Information Systems and Industrial Management (CISIM)*. 2014 [2019-12-08]. Available at: <https://hal.inria.fr/hal-01405569/document>.

[62.] BOULAY, B. – BRÉMOND, F. Activity Recognition. In: DUFOUR, J.-Y. *Intelligent Video Surveillance Systems*. London: ISTE, 2013. ISBN: 978-1-848-21433-0.

[63.] DE HERT, P. Biometrics and the Challenge to Human Rights in Europe. In: CAMPISI, P. *Security and Privacy in Biometrics*. Dordrecht: Springer, 2013. ISBN ISBN 978-1-4471-5230-9.

[64.] FAIRHURST, M. – LI, C. – ERBILEK, M. Exploiting biometric measurements for prediction of emotional state: A preliminary study for healthcare applications using keystroke analysis. In: *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/>.

[65.] GERLOCH, A. Veřejný zájem. In: HENDRYCH, D. et al. *Právnický slovník*. Prague: C. H. Beck, 2009. ISBN 978-80-7400-059-1.

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

[67.] HULMÁK, M. Commentary on Section 40. In: ŠVESTKA, J. – SPÁČIL, J. – ŠKÁROVÁ, M. – HULMÁK, M. et al. *Občanský zákoník. Komentář.* 2nd edition. Praha: C. H. Beck, 2009.

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

[69.] LU, X. – JAIN, A. K. Ethnicity identification from face images. In: *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>.

[70.] LYON, D. Surveillance as social sorting. Computer codes and mobile bodies. In: LYON, D. (eds). *Surveillance as social sorting: Privacy, risk and automated discrimination*. London: Routledge, 2003. ISBN 0-203-99488-4.

[71.] MAGGIO, S. – HAUGEARD, J.-E. – MEDEN, B. – LUVISON, B. – AUDIGIER, R. – BURGER, B. – PHAM, Q. C. Tracking of Objects of Interest in a Sequence of Images. In: DUFOUR, J.-Y. *Intelligent Video Surveillance Systems*. London: ISTE, 2013. ISBN 978-1-848-21433-0.

[72.] MATEJKA, J. Zaměstnanec jako objekt profilování a automatizovaného rozhodování dle obecného nařízení o ochraně osobních údajů, In: HROMADA, M. *Pocta Jarmile Pavlátové k 85. narozeninám*. Plzeň: Západočeská univerzita v Plzni, 2018. ISBN 978-80-261-0809-2.

[73.] MATTHEWS, S. Neuromarketing: What Is It and Is It a Threat to Privacy? In: CLAUSEN, J. – LEVY, N. (eds). *Handbook of Neuroethics*. Dordrecht: Springer, 2015. ISBN 978-94-007-4707-4.

[74.] MILLER, M. I. – VAILLANT, M. – HOFFMAN, W. – SCHUEPP, P. 2D-to-3D Systems Face Recognition. In: VOELLER, J. G. *Detection and Intelligent Systems for Homeland Security (1)*. Somerset, US: Wiley, 2014. ISBN 9781118787366.

[75.] MORDINI, E. – ASHTONS, H. The Transparent Body: Medical Information, Physical Privacy and Respect for Body Integrity. In: MORANDI, E. – TZOVARAS, D. *Second Generation Biometrics: The ethical, Legal and Social Context*. Dordrecht: Springer, 2011. ISBN 978-94-007-3892-8.

[76.] PARZIALE, G. Biometric Sensor and Device, Overview. In: LI, S. Z. – JAIN, A. K. (eds). *Encyclopedia of Biometrics*. Springer, 2009. ISBN 978-1-4899-7488-4.

[77.] RAES, K. Legal Moralism or Paternalism? Tolerance or Indifference? Egalitarian Justice and the Ethics of Equal Concern. In: ALLDRIDGE, P. – BRANTS, Ch. (eds). *Personal Autonomy, the Private Sphere and the Criminal Law. A Comparative Study.* Portland: Hart Publishing, 2001. ISBN 1-901362-82-5.

[78.] SUTROP, M. Ethical Issues in Governing Biometric Technologies. In: KUMAR, A. – ZHANG, D. (eds). *Ethics and Policy of Biometrics. ICEB 2010*. Berlin – Heidelberg: Springer, 2010. Available at: <https://link-springer-com.ezproxy.techlib.cz/chapter/10.1007%2F978-3-642-12595-9_14>.

[79.] 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. In: *2015 IEEE 2nd International Conference on Cybernetics (CYBCONF)*. 2015 [2017-12-17]. Available at: <http://ieeexplore.ieee.org/document/7175984/>.

[80.] VOLAREVIC, M. – STRASBERGER, V. – PACELAT, E. A philosophy of the electronic document management. In: *Proceedings of the 22nd International Conference on Information Technology Interfaces*. 2000 [2019-12-15]. Available at: <https://ieeexplore.ieee.org/document/915870>.

[81.] YAMPOLSKIY, R. V. – GOVINDARAJU, V. Taxonomy of Behavioural Biometrics. In: WANG, L. – GENG, X. (eds). *Behavioral Biometrics for Human Identification: Intelligent Applications*. IGI Global, 2010 [2019-12-08]. Available at: <https://www.igi-global.com/book/behavioral-biometrics-human-identification/99#table-of-contents>. ISBN 9781605667256.

[82.] YANNOPOULOS, A. – ANDRONIKOU, V. – VARVARIGOU, T. Behavioural Biometric Profiling and Ambient Intelligence. In: HILDEBRANDT, M. – SERGE, G. *Profiling the European Citizen. Cross-Disciplinary Perspectives*. Dordrecht: Springer, 2008. ISBN 978-1-4020-6914-7.

[83.] ZEDNER, L. Seeking Security by Eroding Rights: The Side-stepping of Due Process. In: GOOLD, B. J. – LAZARUS, L. *Security and Human Rights*. Portland: Hart Publishing, 2007. ISBN 978-1-84113-608-0.

Articles:

[84.] BRUNTON, F. – NISSENBAUM, H. Vernacular resistance to data collection and analysis: A political theory of obfuscation. *First Monday*. 2011, Vol. 16, no. 5, pp. 1–10 [2019-12-15]. Available at: <http://firstmonday.org/article/view/3493/2955>.

[85.] BLOSFIELD, E. Data Privacy Risks as Digital Identity Moves to Biometrics, Blockchain. *Insurance Journal*. 21. 5. 2018 [2019-12-08]. Available at: <https://search-proquest-com.ezproxy.techlib.cz/docview/2041724444/fulltext/A7B188C363E7486APQ/1?accountid=119841>. ISSN 0020-4714.

[86.] CHINGOVSKA, I. – RABELLO DOS ANJOS, A. – MARCEL, S. Biometrics Evaluation Under Spoofing Attacks. *IEEE Transactions on Information Forensics and Security.* 2014, Vol. 9, no. 12, pp. 2264–2276 [2019-12-08]. Available at: <https://ieeexplore-ieee-org.ezproxy.techlib.cz/document/6879440>. DOI: 10.1109/TIFS.2014.2349158.

[87.] CLARKE, R. *Profiling: A Hidden Challenge to the Regulation of Data Surveillance* [online]. 1993 [2012-03-15]. Available at: <http://www.rogerclarke.com/DV/PaperProfiling.html>.

[88.] CRAWFORD, K. – SCHULTZ, J. Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *Boston College Review*. 2014, Vol. 55, no. 1, pp. 93–128 [2016-04-30]. Available at: <http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=3351&context=bclr>.

[89.] CRAWFORD, K. Can an Algorithm be Agonistic? Ten Scenes from Life in Calculated Publics. *Science, Technology, & Human Values*. 2016, Vol. 41, no. 1, pp. 77–92. [2019-12-15]. Available at: <https://journals.sagepub.com/doi/abs/10.1177/0162243915589635 >.

[90.] CURMI, F. – FERRARIO, M. A. – WHITTLE, J. Biometric data sharing in the wild: Investigating the effects on online sports spectators. *International Journal of Human-Computer Studies.* 2017, Vol. 105, pp. 56–67 [2019-12-08]. Available at: <https://doi.org/10.1016/j.ijhcs.2017.03.008>.

[91.] ČERMÁK, K. jr. Elektronický podpis: pohled soukromoprávní. *Bulletin advokacie*. 2002, no. 11, pp. 64–77. ISSN 1210-6348.

[92.] DANTCHEVA, A. – ELIA, P. – ROSS, A. What Else Does Your Biometric Data Reveal? A Survey on Soft Biometrics. *IEEE Transactions on Information Forensics and Security.* 2015, Vol. 11, no. 3 [2019-12-08]. Available at: <https://ieeexplore-ieee-org.ezproxy.techlib.cz/document/7273870>. DOI: 10.1109/TIFS.2015.2480381

[93.] EMERY, Ch. M. Relational Privacy – A Right To Grieve In The Information Age: Halting The Digital Dissemination Of Death-Scene Images. *Rutgers Law Journal*. 2011, Vol. 42, no. 3, pp. 765–818 [2014-03-05]. Available at: <http://lawjournal.rutgers.edu/sites/lawjournal.rutgers.edu/files/issues/07EmeryVol.42.3.pdf>.

[94.] FIALOVÁ, E. Využití algoritmů při profilování v trestním řízení a důsledky pro lidská práva. Časopis pro právní vědu a praxi [online]. 2018, no. 2, p. 229-258. [2019-12-16]. Available at: <https://journals.muni.cz/cpvp/article/view/8819>. ISSN 1805-2789.

[95.] FISS, O. M. The Bureaucratization of the Judiciary. *Faculty Scholarship Series. Paper 1216*. 1983, pp. 1442–1468 [2016-04-30]. Available at: <http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=2205&context=fss_papers>.

[96.] 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>.

[97.] GABRIELSON, B. Who Really Did It? Controlling Malicious Insiders by Merging Biometric Behavior with Detection and Automated Responses. In: *45th Hawaii International Conference on System Sciences*. IEEE, 2012. Available at: <https://ieeexplore-ieee-org.ezproxy.techlib.cz/document/6149310>. DOI: 10.1109/HICSS.2012.643.

[98.] GALBALLY, J. – MARCEL, S. – FIERREZ, J. Biometric Antispoofing Methods: A Survey in Face Recognition. *IEEE Access*. 2014, Vol. 2 [2019-12-08]. Available at: <https://ieeexplore-ieee-org.ezproxy.techlib.cz/document/6990726>. E-ISSN 2169-3536. DOI: 10.1109/ACCESS.2014.2381273.

[99.] GHOUZALI, S. et al. Trace Attack against Biometric Mobile Applications. *Mobile Information Systems.* 2016 [2019-12-08]. Available at: <https://www.hindawi.com/journals/misy/2016/2065948/>.

[100.] 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>.

[101.] GILLESPIE, T. *The relevance of algorithms*. 2012. Available at: <http://www.tarletongillespie.org/essays/Gillespie – The Relevance of Algorithms.pdf>.

[102.] GOLDSTEIN, D. M. – ALONSO-BEJARANO, C. E-Terrify: Securitized Immigration and Biometric Surveillance in the Workplace. *Human Organization*. 2017, Vol. 76, no. 1, pp. 1–14 [2019-12-08]. Available at: <https://search-proquest-com.ezproxy.techlib.cz/docview/1879074866>.

[103.] GÜTTLER, V. – MATEJKA, J. K otázkám některých základních lidských práv a svobod v souvislosti s právní ochranou biometrických údajů. *Právník*. 2016, no. 12, pp. 1033–1056.

[104.] HABIBU, T. – SAM, A. E. Assessment of vulnerabilities of the biometric template protection mechanism. *International Journal of Advanced Technology and Engineering Exploration*. 2018, Vol. 5, no. 45, pp. 243–254 [2019-12-08]. Available at: <https://search-proquest-com.ezproxy.techlib.cz/docview/2126783210?pq-origsite=summon>. DOI:10.19101/IJATEE.2018.544003.

[105.] HANNAH-MOFFAT, K. Actuarial Sentencing: An “Unsettled” Proposition. *Justice Quarterly*. 2013, Vol. 30, no. 2, pp. 270–296.

[106.] 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/>.

[107.] HLAVNIČKA, J. – ČMEJLA, R. – TYKALOVÁ, T. – ŠONKA, K. – RŮŽIČKA, E. – RUSZ, J. Automated analysis of connected speech reveals early biomarkers of Parkinson’s disease in patients with rapid eye movement sleep behaviour disorder. *Scientific Reports*. 2017, Vol. 7, no. 12 [2019-12-08]. Available at: <https://www.nature.com/articles/s41598-017-00047-5>. doi:10.1038/s41598-017-00047-5. ISSN 2045-2322.

[108.] HODSON, H. Google knows your ills. *New Scientist*. 2016, Vol. 230, no. 307, pp. 22–23.

[109.] HOLLIEN, H. – GEISON, L. – 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>.

[110.] IOVANE, G. – BISOGNI, C. – DE MAIO, L. – NAPPI, M. An encryption approach using Information Fusion techniques involving prime numbers and Face Biometrics. *IEEE Transactions on Sustainable Computing*. 2018 [2018-01-15]. Available at: <http://ieeexplore.ieee.org/document/8259031/>. ISSN 2377-3782.

[111.] JACKSON, J. R. Algorithmic Bias. *Journal of Leadership, Accountability and Ethics*. 2018, Vol. 15, no. 4, pp. 55–65 [2019-12-15]. Available at: <https://search-proquest-com.ezproxy.techlib.cz/docview/2170233068?pq-origsite=summon>. ISSN 1913-8059.

[112.] JOHNSON, M. L. Biometrics and the threat to civil liberties. *Computer*. 2004, Vol. 37, no. 4, pp. 90–92 [2019-12-08]. Available at: <https://ieeexplore-ieee-org.ezproxy.techlib.cz/document/1297317>. DOI: 10.1109/MC.2004.1297317.

[113.] 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>.

[114.] KAUSHAL, N. – KAUSHAL, P. Human Identification and Fingerprints: A Review. *Journal of Biometrics & Biostatatistics*. 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>.

[115.] KIRKPATRICK, K. Battling algorithmic bias: How do we ensure algorithms treat us fairly? *Communications of the ACM*. 2016, Vol. 59, no. 10, pp. 16–17 [2019-12-15]. Available at: <http://delivery.acm.org.ezproxy.techlib.cz/10.1145/2990000/2983270/p16-kirkpatrick.pdf?ip=195.113.241.166&id=2983270&acc=ACTIVE%20SERVICE&key=D6C3EEB3AD96C931%2E507606E42780605B%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&__acm__=1576440854_59828787bbd98db1cee32497e251627a>. ISSN 0001-0782.

[116.] KISTLERA, A. – MARIAUZOULSB, C. – VON BERLEPSCHA, K. Fingertip temperature as an indicator for sympathetic responses. *International Journal of Psychophysiology*. 1998, Vol. 29, no. 1 [2017-12-17]. Available at: <http://www.sciencedirect.com/science/article/pii/S0167876097000871>.

[117.] KMENT, V. Nahradí elektronický podpis prostý ten tradiční vlastnoruční? *Bulletin advokacie*. 2016, no. 12. ISSN 1210-6348.

[118.] KOOPS, B.-J. Technology and the Crime Society: Rethinking Legal Protection. *Selected Works* [online]. 2009 [2014-05-14]. Available at: <http://works.bepress.com/bert_jaap_koops>.

[119.] KORBEL, F. – MELZER, F. Písemnost, elektronický a biometrický podpis v elektronickém právním jednání. *Bulletin advokacie*. 2014, no. 12, pp. 31–36. ISSN 1210-6348.

[120.] 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>.

[121.] KRAUSOVÁ, A. Neuromarketing from a Legal Perspective. *The Lawyer Quarterly.* 2017, Vol. 7, no. 1, pp. 40–49 [2019-12-10]. Available at: <https://tlq.ilaw.cas.cz/index.php/tlq/article/view/221>. ISSN 1805-840X.

[122.] KRAUSOVÁ, A. Online Behavior Recognition: Can We Consider It Biometric Data Under GDPR? *Masaryk University Journal of Law and Technology*. 2018, Vol. 12, no. 2 [2019-12-08]. Available at: <https://journals.muni.cz/mujlt/article/view/8803>.

[123.] KRAUSOVÁ, A. Zásada autonomie v ochraně soukromí: Možnosti a limity v rozhodování o vlastních biometrických údajích. *Právní rozhledy*. 2018, Vol. 26, no. 6, pp. 191-197. ISSN 1210-6410.

[124.] KRAUSOVÁ, A. – HAZAN, H. – MATEJKA, J. Biometric Data Vulnerabilities: Privacy Implications. *The Lawyer Quarterly.* 2018, Vol. 8, no. 3, pp. 295–306 [2019-12-10]. Available at: <https://tlq.ilaw.cas.cz/index.php/tlq/article/view/291>. ISSN 1805-840X.

[125.] KUNER, Ch. *The 'Internal Morality' of European Data Protection Law.* November 24, 2008 [online]. [2019-12-08]. Available at: <http://ssrn.com/abstract=1443797>.

[126.] 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>.

[127.] LI, C. C. Biometrics. *AccessScience*. 2014 [2017-10-16]. Available at: <https://doi.org/10.1036/1097-8542.083700>.

[128.] MANSFIELD-DEVINE, S. Social identity: is biometric technology on social networks a benefit or a threat? *Biometric Technology Today*. 2012, Vol. 2012, no. 10, pp. 5–9 [2019-12-08]. Available at: <https://doi.org/10.1016/S0969-4765(12)70203-5>.

[129.] MARRAUD, D. – CÉPAS, B. – SULZER, J.-F. – MULAT, Ch. – SÈDESA, F. Posteriori Analysis for Investigative Purposes. In: DUFOUR, J.-Y. *Intelligent Video Surveillance Systems*. London: ISTE, 2013. ISBN 978-1-848-21433-0.

[130.] MATEJKA, J. Úprava elektronického podpisu v právním řádu ČR. *Právník*. 2001, Vol. 140, no. 6, pp. 582–611.

[131.] MATEJKA, J. – KRAUSOVÁ, A. – GÜTTLER, V. Biometrické údaje a jejich právní režim. *Revue pro právo a technologie*. 2018, Vol. 9, no. 17, pp. 91–129 [2019-12-02]. Available at: <https://journals.muni.cz/revue/article/view/8801/pdf>. ISSN 1805-2797.

[132.] MARY, P. Pénalité et gestion des risques: versune justice « actuarielle » en Europe? *Déviance et Société*. 2001, Vol. 25, no. 1, pp. 33–51 [2019-12-15]. Available at: <https://www.cairn.info/revue-deviance-et-societe-2001-1-page-33.htm>.

[133.] MAYER-SCHÖNBERGER, V. – INGELSSON, E. Big Data and medicine: a big deal? *Journal of Internal Medicine*. 2018, Vol. 283, no. 5, p. 418–429.

[134.] MAYSON, S. G. Bias In, Bias Out. *Yale Law Journal*. 2019, Vol. 128, no. 8, pp. 2218–2300 [2019-12-15]. Available at: <http://web.a.ebscohost.com.ezproxy.techlib.cz/ehost/detail/detail?vid=0&sid=e39e5a41-db7c-4c08-874e-31f478e4eff8%40sdc-v-sessmgr03&bdata=Jmxhbmc9Y3Mmc2l0ZT1laG9zdC1saXZl#AN=137113291&db=a9h>.

[135.] MOHAPATRA, S. et al. Real time biometric surveillance with gait recognition. *AIP Concerence Proceedings*. 2018, Vol. 1952, no. 1 [2019-12-08]. Available at: <https://aip-scitation-org.ezproxy.techlib.cz/doi/abs/10.1063/1.5031969>.

[136.] MORIN, Ch. Neuromarketing: The New Science of Consumer Behavior. *Society*. 2011, Vol. 48, no. 2, pp. 131–135.

[137.] MURPHY, E. – ILLES, J. – REINER, p. B. Neuroethics of Neuromarketing. *Journal of Consumer Behavior*. 2008, no. 7, pp. 293–302.

[138.] Nonneman, F. Právní úprava ochrany osobnosti v novém občanském zákoníku a její vztah k ochraně osobních údajů. *Právní rozhledy.* 2012, Vol. 13–14, pp. 505 et seq. ISSN 1210-6410.

[139.] 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>.

[140.] PODSZUN, R. Kartellrecht in der Internet-Wirtschaft: Zeit für den more technological approach. *Wirtschaft und Wettbewerb.* 2014, Nr. 3. ISSN 0043-6151.

[141.] POLČÁK, R. Elektronické právní jednání: změny, problémy a nové možnosti v zákoně č. 89/2012 Sb. *Bulletin advokacie*. 2013, no. 10, pp. 34–40. Available at: <http://www.bulletin-advokacie.cz/elektronicke-pravni-jednani-zmeny-problemy-a-nove-moznosti-v-zakone-c.-892012-sb>. ISSN 1210-6348.

[142.] POLČÁK, R. Praxe elektronických dokumentů. *Bulletin advokacie*. 2011, no. 7–8. ISSN 1210-6348.

[143.] POPE, C. Biometric data collection in an unprotected world: Exploring the need for federal legislation protecting biometric data. *Journal of Law & Policy.* 2018, Vol. 26, no. 2, pp. 769–803 [2019-12-08]. Available at: <http://web.a.ebscohost.com.ezproxy.techlib.cz/ehost/pdfviewer/pdfviewer?vid=3&sid=6ea67a93-83d9-47b0-bb10-0562f5f125f0%40sdc-v-sessmgr01>.

[144.] RATHGEB, Ch. – UHL, A. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security.* 2011, Vol. 2011, no. 3, pp. 1–25 [2019-12-08]. Available at: <https://search-proquest-com.ezproxy.techlib.cz/docview/1323854588/fulltextPDF/91CADB9B1F374FD2PQ/3?accountid=119841>. DOI:10.1186/1687-417X-2011-3.

[145.] ROTH, A. Trial by Machine. *Georgetown Law Journal*. 2016, Vol. 104, no. 5, pp. 1–48. Available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2743800>.

[146.] ROUVROY, A. Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence Privacy. *Studies in Ethics, Law, and Technology*. 2008, Vol. 2, no. 1 [2014-05-14]. Available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1013984>.

[147.] RUBINSTEIN, I. S. Big Data: The End of Privacy or a New Beginning? *International Data Privacy Law*. 2013, Vol. 3, no. 2, pp. 1–14 [2014-05-10]. Available at: <http://idpl.oxfordjournals.org/content/early/2013/01/24/idpl.ips036.full>.

[148.] SADHYA, D. – SINGH, S. K. Privacy risks ensuing from cross-matching among databases: A case study for soft biometrics. *Information Processing Letters*. 2017, Vol. 128, pp. 38–45 [2019-12-08]. Available at: <https://doi.org/10.1016/j.ipl.2017.08.001>.

[149.] 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>.

[150.] SIMON, J. – FEELEY, M. The New Penology: Notes on the Emerging Strategy of Corrections and Its Implications. *Criminology.* 1992, Vol. 30, no. 4. pp. 449–474 [2016-05-31]. Available at: <http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1717&context=facpubs>.

[151.] SOH, Ch. et al. Employee profiling via aspect-based sentiment and network for insider threats detection. *Expert Systems with Applications*. 2019, Vol. 135, pp. 351–361 [2019-12-08]. Available at: <https://doi.org/10.1016/j.eswa.2019.05.043>.

[152.] 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>.

[153.] SUN, Y. – ZHANG, M. – SUN, Z. – TAN, T. Demographic Analysis from Biometric Data: Achievements, Challenges, and New Frontiers. *IEEE Transactions on Pattern Analysis and Machine Intelligence.* 2017, Vol. 40, no. 2 [2019-12-08]. Available at: <https://ieeexplore-ieee-org.ezproxy.techlib.cz/document/7855777>. DOI: 10.1109/TPAMI.2017.2669035.

[154.] SUTROP, M. – LAAS-MIKKO, K. From Identity Verification to Behavior Prediction: Ethical Implications of Second Generation Biometrics. *Review of Policy Research.* 2012, Vol. 29, no. 1, pp. 21–36 [2019-12-08]. Available at: <https://onlinelibrary-wiley-com.ezproxy.techlib.cz/doi/abs/10.1111/j.1541-1338.2011.00536.x>.

[155.] TOOR, A. S. – WECHSLER, H. – NAPPI, M. Biometric surveillance using visual question answering. *Pattern Recognition Letters*. 2019, Vol. 126, pp. 111–118 [2019-12-08]. Available at: <https://doi.org/10.1016/j.patrec.2018.02.013>.

[156.] TOPAK, Ö. E. – BRACKEN-ROCHE, C. – SAULNIER, A. – LYON, D. From Smart Borders to Perimeter Security: The Expansion of Digital Surveillance at the Canadian Borders. *Geopolitics*. 2015, Vol. 20, no. 4, pp. 880–899. ISSN 1465-0045.

[157.] TOPCU, B. et al. Practical security and privacy attacks against biometric hashing using sparse recovery. *EURASIP Journal on Advances in Signal Processing*. 2016, Vol. 2016, pp. 1–20 [2019-12-08]. Available at: <https://search-proquest-com.ezproxy.techlib.cz/docview/1819663613?pq-origsite=summon>. DOI: 10.1186/s13634-016-0396-1.

[158.] 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/>.

[159.] 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>.

[160.] VALER, T. Biometrie obličeje pro autentizaci osob. *Data Security Management*. 2014, Vol. XVIII, no. 2. ISSN 1211-8737.

[161.] VELASTIN, S. A. – BOGHOSSIAN, B. A. – PING LAI LO, B. – SUN, J. – VICENCIO-SILVA, M. A. PRISMATICA: Toward Ambient Intelligence in Public Transport Environments. *IEEE Transactions On Systems, Man, and Cybernetics—Part A: Systems and Humans* . 2005, Vol. 35, no. 1, s. 164–182 [2016-06-01]. Available at: <http://ids.snu.ac.kr/w/images/9/9e/AmI04.pdf>.

[162.] 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>.

[163.] UNDERWOOD, B. Law and the Crystal Ball: Predicting Behavior with Statistical Inference and Individualized Judgment. *Yale Law Journal*. 1979, Vol. 88, pp. 1408–1449. Available at: <http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=4140&context=fss_papers>.

[164.] 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>.

[165.] WACHTER, S. – MITTELSTADT, B. – FLORIDI, L. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*. 2017, Vol. 7, no. 2, s. 76–99. ISSN 2044-3994.

[166.] WARREN, S. – BRANDEIS, L. The Right to Privacy. *Harward Law Review.* 1890, Vol. 6, no. 4 [2012-03-15]. Available at: <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>.

[167.] WILSON, R. M. – GAINES, J. – HILL, R. P. Neuromarketing and Consumer Free Will. *The Journal of Consumer Affairs*. 2008, Vol. 42, no. 3. pp. 389–410.

[168.] ZARSKY, T. Governmental Data Mining and its Alternatives. *Penn State Law Review.* 2011, Vol. 116, no. 2, s. 285–330 [2016-05-04]. Available at: <http://www.pennstatelawreview.org/116/2/116 Penn St. L. Rev. 285.pdf>.

[169.] ZARSKY, T. Understanding Discrimination in the Scored Society. *Washington Law Review*. 2014, Vol. 89, no. 4, pp. 1375–1412 [2019-12-15]. Available at: <https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=4822&context=wlr>.

Other:

[170.] ‘1m fingerprint’ data leak raises doubts over biometric security. *Biometric Technology Today*. 2019, Vol. 209, no. 8, pp. 1–2 [2019-12-08]. Available at: <https://doi.org/10.1016/S0969-4765(19)30104-3>.

[171.] Administrative Office of the United States Courts Office of Probation and Pretrial Services. An Overview of the Federal Post Conviction Risk Assessment. In: *Uscourts* [online]. 2011. Available at: <www.uscourts.gov/file/2749/download>.

[172.] Algorithmic bias. In: *Wikipedia* [online]. 12. 12. 2019 [2019-12-15]. Available at: <https://en.wikipedia.org/wiki/Algorithmic_bias>.

[173.] ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines for Identifying a Controller or Processor’s Lead Supervisory Authority. In: *European Commission* [online]. 5. 4. 2017 [2019-12-08]. Available at: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235>.

[174.] ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on consent under Regulation 2016/679. In: *European Data Protection Board* [online]. 10. 4. 2018 [2019-09-30]. Available from: <https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en>.

[175.] ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. In: *European Data Protection Board* [online]. 6. 2. 2018 [2019-09-30]. Available from: <https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en>.

[176.] ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. In: *European Data Protection Board* [online]. 2018 [2019-12-02]. Available at: <https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en>.

[177.] ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on transparency under Regulation 2016/679. In: *European Commission* [online]. 2017 [2019-12-02]. Available at: <http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850>.

[178.] ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on Personal data breach notification under Regulation 2016/679. In: *European Data Protection Board* [online]. 2018 [2019-12-02]. Available at: <https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en>.

[179.] ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 15/2011 on the definition of consent. In: *European Commission* [online]. 13. 7. 2011 [2019-12-08]. Available at: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf>.

[180.] ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 3/2012 on developments in biometric technologies. In: *European Commission* [online]. 27. 4. 2012 [2019-12-08]. Available at: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf>.

[181.] ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 4/2007 on the concept of personal data. In: *European Commission* [online]. 20. 6. 2007 [2019-12-08]. Available at: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>.

[182.] ARTICLE 29 DATA PROTECTION WORKING PARTY. Working document on biometrics. In: *European Commission* [online]. 1. 8. 2003 [2019-12-08]. Available at: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf>.

[183.] Automatic Detection of Abnormal Behaviour and Threats in crowded Spaces. In: *CORDIS* [online]. [2019-12-08]. Available at: <https://cordis.europa.eu/project/id/218197>.

[184.] 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>.

[185.] BAIRD, Ch. et al. A Comparison of Risk Assessment Instruments in Juvenile Justice. In: *NCJRS* [online]. 2013 [2019-12-17]. Available at: <https://www.ncjrs.gov/pdffiles1/ojjdp/grants/244477.pdf>.

[186.] BARNES, G. C. – HYATT. M, J. Classifying Adult Probationers by Forecasting Future Offending. In: *NCJRS* [online]. 2012 [2016-05-14]. Available at: <https://www.ncjrs.gov/pdffiles1/nij/grants/238082.pdf>.

[187.] CHRISTIN, A. – ROSENBLAT, A. – BOYD, D. Courts and Predictive Algorithms. In: *NYU Law* [online]. 2015 [2019-12-17]. Available at: <https://www.law.nyu.edu/sites/default/files/upload_documents/Angele%20Christin.pdf >.

[188.] CLARKE, R. Introduction to Dataveillance and Information Privacy, and Definitions of Terms. In: *Roger Clarke's Web-Site* [online]. 1997 [2014-06-15]. Available at: <http://www.rogerclarke.com/DV/Intro.html>.

[189.] ČERVENKA, J. *Biometrika a její využívání z pohledu české veřejnosti*. Research report. Centrum pro výzkum veřejného mínění, Sociologický ústav AV ČR, v. v. i., 2018.

[190.] DE HERT, P. – CHRISTIANEN, K. Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data. In: *Council of Europe* [online]. 2013 [2019-09-15]. Available at: <https://rm.coe.int/progress-report-on-the-application-of-the-principles-of-convention-108/1680744d81>.

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

[192.] Explanatory report to Act no. 110/2019 Coll., on Personal Data Processing. In: *Beck-online* [online]. 2019 [2019-04-30]. Available at: <https://www.beck-online.cz/bo/chapterview-document.seam?documentId=oz5f6mrqge4v6mjrgbpwi6q&rowIndex=0>.

[193.] 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>.

[194.] ERDOS, D. et al. Biometric Identification and Privacy. In: *Oxford Human Rights Hub* [online]. 2013 [2019-07-15]. Available at: <http://ohrh.law.ox.ac.uk/wordpress/wp-content/uploads/2018/02/4.-Indian-Biometric-Identification-and-Privacy.pdf>.

[195.] EUROPEAN COMMISSION. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Building Trust in Human-Centric Artificial Intelligence. In: *European Commission* [online]. 8.4.2019 [2019-10-19]. Available at: <https://ec.europa.eu/digital-single-market/en/news/communication-building-trust-human-centric-artificial-intelligence>.

[196.] EUROPEAN COMMISSION. Communication from The Commission to the European Parliament, The European Council, The Council, The European Economic and Social Committee and the Committee of the Regions. Artificial Intelligence for Europe. In: *European Commission* [online]. 25.4.2018 [2019-10-19]. Available at: <https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe>.

[197.] EUROPEAN COMMISSION. Cookies. In: *European Commission* [online]. 2016 [2017-12-22]. Available at: <http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm>.

[198.] EUROPEAN PARLIAMENT. Civil Law Rules on Robotics. In: *European Parliament* [online]. 16. 2. 2017 [2019-10-20]. Available at: <http://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.pdf>.

[199.] EUROSTAT. Internet usage. Eurostat (isoc_ci_ifp_iu) and (isoc_ci_ifp_fu). In: *European Commission*. [online]. 2018 [2019-09-30]. Available at: <https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals#Internet_usage>.

[200.] 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/>.

[201.] FitBit Privacy Policy. In: *Fitbit* [online]. Available at: <https://www.fitbit.com/eu/legal/privacy-policy#info-we-collect>.

[202.] FitBit Terms of Service. In: *Fitbit* [online]. Available at: <https://www.fitbit.com/eu/legal/terms-of-service>.

[203.] GERMAN, R. L. – BARBER, K. S. Consumer Attitudes About Biometric Authentication. In: *The University of Texas at Austin, Center for Identity* [online]. 2018 [2019-01-30]. Available at: <https://identity.utexas.edu/assets/uploads/publications/Consumer-Attitudes-About-Biometrics.pdf>.

[204.] GILLESPIE, T. *The relevance of algorithms*. 2012. Available at: <http://www.tarletongillespie.org/essays/Gillespie – The Relevance of Algorithms.pdf>.

[205.] 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>.

[206.] High-Level Expert Group on Artificial Intelligence. Ethics Guidelines for Trustworthy AI. In: *European Commission* [online]. 8. 4. 2019 [2019-10-19]. Available at: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>.

[207.] IBM SECURITY. IBM Security: Future of Identity Study, Consumer perspectives on authentication: Moving beyond the password. In: *ORBIS* [online]. 2018 [2019-12-08]. Available at: <https://espas.secure.europarl.europa.eu/orbis/sites/default/files/generated/document/en/security-ibm-security-solutions-wg-research-report-22012422usen-20180124.pdf>.

[208.] Information asymmetry. In: *Wikipedia* [online]. 10. 10. 2019 [2019-12-10]. Available at: <https://en.wikipedia.org/wiki/Information_asymmetry>.

[209.] 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>.

[210.] JENKINS, J. – SWEET, C. – SWEET, J. – MOEL, S. – SZU, H. Authentication, privacy, security can exploit brainwave by biomarker. In: *SPIE.digital library* [online]. 19. 6. 2014 [2019-12-08]. Available at: <https://www.spiedigitallibrary.org/conference-proceedings-of-spie/9118/1/Authentication-privacy-security-can-exploit-brainwave-by-biomarker/10.1117/12.2051323.short?SSO=1>. DOI: 10.1117/12.2051323.

[211.] Judges: independence, efficiency, and responsibilities. Recommendation CM/Rec(2010)12 and explanatory memorandum. In: *Council of Europe* [online]. 2003 [2019-10-23]. Available at: <https://rm.coe.int/16807096c1>.

[212.] KATHLEEN, H. Florida takes aim at juvenile recidivism with predictive analytics. In: *GCN* [online]. 31. 7. 2015 [2016-05-14]. Available at: <https://gcn.com/articles/2015/07/31/juvenile-predictive-analytics.aspx>.

[213.] 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>.

[214.] KITE-POWELL, J. Making Facial Recognition Smarter With Artificial Intelligence. In: *Forbes* [online]. 30. 9. 2018 [2019-10-19]. Available at: <https://www.forbes.com/sites/jenniferhicks/2018/09/30/making-facial-recognition-smarter-with-artificial-intelligence/#66442807c8f1>.

[215.] KOFFEMAN, N. R. (The right to) personal autonomy in the case law of the European Court of Human Rights. In: *Leiden University Repository* [online]. 2010 [2019-12-08]. Available at: <https://openaccess.leidenuniv.nl/handle/1887/15890>.

[216.] Laura and John Arnold Fundation. Public Safety Assessment. *Laura and John Arnold Fundation. Pretrial Criminal Justice Research* [online]. Available at: <http://www.arnoldfoundation.org/initiative/criminal-justice/crime-prevention/public-safety-assessment>.

[217.] LAURI, J. P. *The Data Protection Directive on Police Matters 2016/680 protects privacy – The evolution of EU's data protection law and its compatibility with the right to privacy*. Master's thesis. University of Helsinki, 2017.

[218.] Law no. 190/2018 on measures for the application of Regulation (EU) 2016/679 of the European Parliament and 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). (Unofficial translation from Romanian language prepared by PrivacyOne). In: *IAPP* [online]. [2019-01-30]. Available at: <https://iapp.org/media/pdf/resource_center/Romanian_Data_Protection_Law_English_Translation.pdf>.

[219.] 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>.

[220.] MINISTRY OF DEFENCE. Joint Doctrine Note 2/13. Information Superiority. In: *GOV.UK* [online]. 2013 [2019-12-10]. Available at: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819814/archive_doctrine_uk_info_superiority_jdn_2_13.pdf>.

[221.] MINISTRY OF DEFENCE. Joint Concept Note 2/18. Information Advantage. In: *GOV.UK* [online]. 2018 [2019-12-10]. Available at: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/764075/20181126-JCN_2_18_Information_Advantage_web.pdf>.

[222.] MIT claims breakthrough in ending biometric bias. *Biometric Technology Today*. 2019, Vol. 2019, no. 2, p. 12 [2019-12-15]. Available at: <https://doi.org/10.1016/S0969-4765(19)30028-1>. ISSN 0969-4765.

[223.] Next Generation Identification (NGI). In: *FBI* [online]. [2019-12-08]. Available at: <https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi>.

[224.] OECD. Working Party on Information Security and Privacy. Biometric-based Technologies. In: *OECD* [online]. 2004 [2019-12-04]. Available at: <https://www.oecd-ilibrary.org/docserver/232075642747.pdf?expires=1575372645&id=id&accname=guest&checksum=FF00B8A8B118873A62B7857A864A3A71>.

[225.] Opinion no. 2/2014 of the Office for Personal Data Protection – Dynamic Biometric Signature pursuant to Personal Data Protection Act. In: *The Office for Personal Data Protection* [online]. 18. 7. 2014 [2017]. Available at: <https://www.uoou.cz/stanovisko-c-2-2014-dynamicky-biometricky-podpis-z-pohledu-zakona-o-ochrane-osobnich-udaju/d-11298>.

[226.] Opinion no. 1/2017 of the Office for Personal Data Protection – Biometric Identification or Authentication of Employees. In: *The Office for Personal Data Protection* [online]. 8. 6. 2017 [2017]. Available at: <https://www.uoou.cz/stanovisko-c-1-2017-biometricka-identifikace-nebo-autentizace-zamestnancu/d-23849>.

[227.] Opinion of the Supreme Court's plenum of 5 January 2017 on the filings made electronically and the delivery of documents electronically issued by the court through public data network (Opinion no. Plsn 1/2015). Available at: <http://www.nsoud.cz/. – neodpovídá normě>.

[228.] PARLAMENTNÍ INSTITUT. Odpověď na dotaz: Právní úprava biometriky. Červenec 2014, p. 6, 7 – Kanada. Personal Information Protection and Electronic Documents Act. S. C. 2000.

[229.] Parliamentary Press no. 973/0 of 29 November 2016, a government bill amending Act no. 300/2013 Coll., on the Military Police and on the Amendments to Certain Acts (Military Police Act), as amended.

[230.] Parliamentary Press no. 1059/0 of 21 March 2017, a government payment bill. In: *Poslanecká sněmovna Parlamentu České republiky* [online]. 16. 10. 2017 [2017-10-16]. Available at: <http://www.psp.cz/sqw/historie.sqw?o=7&t=1059>.

[231.] PETERKA, J. Elektronický podpis na rozcestí. In: *LUPA* [online]. 6. 6. 2011 [2011-12-28]. Available at: <http://www.lupa.cz/clanky/elektronicky-podpis-na-rozcesti>.

[232.] PLAISIER, J. – VAN DITZHUIJZEN, J. Risico taxatie bij verlof van gedetineerden. Een (inter)nationale vergelijking van instrumenten en procedures. In: *Impact R&D* [online]. 2008 [2016-05-14]. Available at: <http://mpct.eu/wp-content/uploads/downloads/2013/03/Risicotaxatie-Verlof-Gedetineerden-1556_volledige_tekst_tcm44-167941-1.pdf>.

[233.] Privacy & HIPAA. In: *Medici* [online]. [2018-08-16]. Available at: <https://medici.md/hipaa-privacy/>.

[234.] PRIVACY INTERNATIONAL. Briefing to the UN Counter-Terrorism Executive Directorate on the responsible use and sharing of biometric data to tackle terrorism. In: *Privacy International* [online]. 2019 [2019-12-04]. Available at: <https://www.privacyinternational.org/sites/default/files/2019-07/PI%20briefing%20on%20biometrics%20final.pdf>.

[235.] Privacy Policy. In: *Nokia.com* [online]. Available at: <https://www.nokia.com/en_int/privacy>.

[236.] Privacy Policy. In: *Zocdoc* [online]. [2018-08-16]. Available at: <https://www.zocdoc.com/about/privacypolicy/>.

[237.] Protecting personal data when being used by police and criminal justice authorities. In: *EUR-Lex* [online]. 2017 [2019-01-30]. Available at: <https://eur-lex.europa.eu/legal-content/ENG/TXT/?uri=LEGISSUM:310401_3>.

[238.] Průmysl 4.0 významně ovlivní budoucnost profesí, změny čekají i vzdělávací systém. In: *EkonTech.cz* [online]. 25. 5. 2018 [2019-12-15]. Available at: <https://www.ekontech.cz/clanek/prumysl-40-vyznamne-ovlivni-budoucnost-profesi-zmeny-cekaji-vzdelavaci-system>.

[239.] Recommentation CM/Rec(2010)12 Judges: independance, efficiency, and responsabilities. In: *Council of Europe* [online]. 2003. Available at: <https://rm.coe.int/16807096c1>.

[240.] ROSS, A. – JAIN, A. Information Fusion in Biometrics. *Pattern Recognition Letters*. 2003, Vol. 24, no. 13, pp. 2115–2125 [2017-11-02]. Available at: <https://www.sciencedirect.com/science/article/pii/S0167865503000795?via%3Dihub>. ISSN 0167-8655.

[241.] ROUVROY, A. L'algorithme n'est «pas un système de prédiction mais d'intervention». In: *Medipart* [online]. 2015 [2016-04-30]. Available at: <https://www.academia.edu/12603930/Lalgorithme_nest_pas_un_système_de_prédiction_mais_d_intervention_Entretien_réalisé_par_Jérôme_Hourdeaux_pour_Mediapart_25_mai_2015>.

[242.] ROUVROY, A. "Of Data and Men".Fundamental Rights and Freedoms in a World of Big Data. In: *Bepress* [online]. 2011 [2016-05-04]. Available at: <http://works.bepress.com/antoinette_rouvroy/64>.

[243.] 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/>.

[244.] 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>.

[245.] STARR, S. Evidence-Based Sentencing and the Scientific Rationalization of Discrimination. In: *Michigan Law* [online]. 2013 [2016-05-31]. Available at: <http://repository.law.umich.edu/law_econ_current/90>.

[246.] STARR, S. Sentencing, by the Numbers. In: *The New York Times* [online]. 10. 8. 2014 [2016-05-31]. Available at: <http://repository.law.umich.edu/law_econ_current/90>.

[247.] STEWART, K. 10 Algorithms That Are Changing Healthcare. In: *University of Utah Health* [online]. Available at: <http://uofuhealth.utah.edu/innovation/blog/2015/10/10AlgorithmsChangingHealthCare.php>.

[248.] ŠČUREK, R. Biometrické metody identifikace osob v bezpečnostní praxi. Studijní text. In: *Rucnepsanypodpis.cz* [online]. 2008 [2019-12-15]. Available at: <http://www.rucnepsanypodpis.cz/PDF/biometricke_metody.pdf>.

[249.] Terms and Conditions for your use of the Hedia Application. In: *Hedia.co* [online]. [2018-08-16]. Available at: <http://hedia.dk/terms-and-conditions/>.

[250.] Terms and conditions of web use. In: *Mediscan* [online]. [2018-08-16]. Available at: <https://www.medicsen.com/en/privacy_policy> or Terms and Conditions for your use of the Hedia Application. Available from: <http://hedia.dk/terms-and-conditions/>.

[251.] Terms of Use. In: *HealthTap.com* [online]. [2018-08-16]. Available at: <https://www.healthtap.com/terms>.

[252.] THE COMMITTEE ON SCIENCE AND LAW. Are Your Thoughts Your Own?: "Neuroprivacy" and the Legal Implications of Brain Imaging. In: *New York City Bar* [online]. 2005 [2019-12-15]. Available at: <https://www.nycbar.org/pdf/report/Neuroprivacy-revisions.pdf>.

[253.] THUY, O. Dubai Airport is going to use face-scanning virtual aquariums as security checkpoints. In: *The Verge* [online]. 10. 10. 2017 [2018-02-24]. Available at: <https://www.theverge.com/2017/10/10/16451842/dubai-airport-face-recognition-virtual-aquarium>.

[254.] UN. United Nations Compendium of Recommended Practices for the Responsible Use & Sharing of Biometrics in Counter-Terrorism. In: *UN* [online]. 2018 [2019-12-04]. Available at: <https://www.unodc.org/pdf/terrorism/Compendium-Biometrics/Compendium-biometrics-final-version-LATEST_18_JUNE_2018_optimized.pdf>.

[255.] VOORHEES, T. Jr. – SPIEGEL, D. L. – COOPER, D. Neuromarketing: Legal and Policy Issues. *A Covington White Paper* [online]. 2011 [2016-06-15]. Available at: <https://www.cov.com/files/upload/White_Paper_Neuromarketing_Legal_and_Policy_Issues.pdf >.

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

[257.] WILSON, C. R. Biometric Accuracy Standards. In: *National Institute of Standards and Technology* [online]. 2003 [2017-11-20]. Available at: <https://csrc.nist.gov/CSRC/media/Events/ISPAB-MARCH-2003-MEETING/documents/March2003-Biometric-Accuracy-Standards.pdf>.

[258.] Your Privacy when Using Nokia Health Products and Services. In: *Nokia* [online]. [2018-08-16]. Available at: <https://health.nokia.com/cz/en/legal/privacy-policy-supplement>.

Legislation:

[259.] Act no. 40/1995 Coll., on Regulation of Advertising, as amended.

[260.] Act no. 40/2009 Coll., the Criminal Code, as amended.

[261.] Act no. 88/2011 Coll., on the technical conditions and procedure in collecting foreigners' biometric data and signatures for issuing their residence permits, as amended.

[262.] Act no. 89/2012 Coll., the Civil Code, as amended.

[263.] Act no. 101/2000 Coll., on the Protection of Personal Data and on amending certain acts, as amended.

[264.] Act no. 110/2019 Coll., on Personal Data Processing.

[265.] Act no. 141/1961 Coll., on Criminal Proceedings (Criminal Procedure Code), as amended.

[266.] Act no. 197/2009 Coll., on the certification of public documents containing biometric data and the amendments to certain Acts, as amended.

[267.] Act no. 218/2003 Coll., on youth responsibility for unlawful acts and the judiciary in suits of youth and on the amendments to certain Acts (Youth Judiciary Act), as amended.

[268.] Act no. 221/2003 Coll., on Temporary Protection of Foreigners, as amended.

[269.] Act no. 255/2012 Coll., on inspection (Inspection Code).

[270.] Act no. 262/2006 Coll., Labour Code, as amended.

[271.] Act no. 263/2016 Coll., the Nuclear Act, as amended.

[272.] Act no. 269/1994 Coll., on the Criminal Register, as amended.

[273.] Act no. 273/2008 Coll., on the Police of the Czech Republic, as amended.

[274.] Act no. 297/2016 Coll., on trust services for electronic transactions, as amended.

[275.] Act no. 300/2008 Coll., on electronic acts and the authorized conversion of documents, as amended.

[276.] Act no. 300/2013 Coll., on the Military Police and on the Amendments to Certain Acts, as amended.

[277.] Act no. 325/1999 Coll., on Asylum, as amended.

[278.] Act no. 326/1999 Coll., on the Residence of Foreigners in the Czech Republic and on the Amendments to Certain Acts.

[279.] Act no. 328/1999 Coll., on identity cards, as amended.

[280.] Act no. 329/1999 Coll., on Travel Documents, as amended.

[281.] Act no. 329/1999 Coll., on travel documents and on the amendment to Act no. 283/1991 Coll., on the Police of the Czech Republic, as amended, (Travel Documents Act), as amended.

[282.] Act no. 372/2011 Coll., on health services and conditions of their provision (Health Services Act).

[283.] Act no. 480 /2004 Coll., on certain information society services, as amended.

[284.] Act no. 493/2004 Coll., Amending Act no. 101/2000 Coll., On the protection of personal data and on amending certain acts, as amended.

[285.] Act no. 500/2004 Coll., Code of Administrative Procedure.

[286.] Act no. 563/1991 Coll., on Accounting, as amended.

[287.] Act no. 634/1992 Coll., on Consumer Protection, as amended.

[288.] Charter of Fundamental Rights of the European Union.

[289.] Code de procédure penal (France)

[290.] Commission Decision 2009/767/EC of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the points of single contact under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market (notified under document C(2009) 7806) (Text with EEA relevance)

[291.] Commission Regulation (EU) No 383/2012 of 4 May 2012 laying down technical requirements with regard to driving licences which include a storage medium (microchip) (Text with EEA relevance).

[292.] Consolidated version of the Treaty on European Union and the Treaty on the Functioning of the European Union.

[293.] Constitutional Act no. 1/1993 Coll., Constitution of the Czech Republic.

[294.] Convention 108+. Convention for the protection of individuals with regard to the processing of personal data. In: *Council of Europe* [online]. 2018 [2019-09-15]. Available at: <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1>.

[295.] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. In: *Council of Europe* [online]. [2019-12-14]. Available at: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>.

[296.] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.

[297.] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.

[298.] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States.

[299.] Council Regulation (EU) No 1417/2013 of 17 December 2013 laying down the form of the laissez-passer issued by the European Union.

[300.] Czech National Council's Resolution no. 2/1993 Coll., On the Declaration of the Charter of Fundamental Rights and Freedoms as part of the constitutional order of the Czech Republic.

[301.] Data Protection Act 2018. (United Kingdom).

[302.] Decree no. 361/2016 Coll., On safeguarding nuclear installations and nuclear material, as amended.

[303.] Decree no. 361/2016 Coll., on Security of Nuclear Installation and Nuclear Material.

[304.] Decree no. 400/2011 Coll., implementing the Identity Cards Act, as amended, and the Travel Documents Act, as amended.

[305.] Decree no. 415/2006 Coll., laying down the technical conditions and procedure in the collection and further processing of biometric data contained in travel document data carriers.

[306.] 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.

[307.] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[308.] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (Text with EEA relevance).

[309.] Directive 2006/126/EC of the European Parliament and of the Council of 20 December 2006 on driving licences (Recast) (Text with EEA relevance).

[310.] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

[311.] Directive of the European Parliament and of the Council (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[312.] Directive of the Ministry of the Interior concerning Act no. 133/2000 Coll., on the resident register and personal identification numbers and on the amendments to certain Acts (Resident Registration Act), as amended.

[313.] European Convention on Human Rights. In: *Council of Europe* [online]. [2019-12-14]. Available at: <https://www.echr.coe.int/Documents/Convention_ENG.pdf>.

[314.] European Parliament legislative resolution of 16 April 2019 on the amended proposal for a regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399, Regulation (EU) 2017/2226, Regulation (EU) 2018/XX [the ETIAS Regulation], Regulation (EU) 2018/XX [the Regulation on SIS in the field of border checks] and Regulation (EU) 2018/XX [the eu-LISA Regulation] (COM(2018)0478 – C8-0294/2018 – 2017/0351(COD)).

[315.] Explanatory Memorandum to the Act no. 89/2012 Coll., Civil Code.

[316.] Explanatory Memorandum to the Act of 9 December 2015 no. 378/2015 of the Collection of Laws on Amendment of the Act no. 634/1992 of the Collection of Laws on Consumer Protection, as amended

[317.] Explanatory Report on Act no. 150/2016 Coll. amending Act no. 141/1961 Coll., on criminal proceedings (Criminal Procedure Code), as amended.

[318.] Explanatory Report on Act no. 186/2016 Coll., on Gambling, as amended.

[319.] Explanatory Report on Act no. 263/2016 Coll., the Nuclear Act.

[320.] Explanatory Report on Act no. 304/2008 Coll. amending Act no. 563/1991 Coll., on Accounting, as amended, and certain Acts.

[321.] Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) vom 30. Juni 2017 (BGBl. I v. 5.7.2017, S. 2097). (Germany).

[322.] International Covenant on Civil and Political Rights. In: *United Nations* [online]. [2019-12-14]. Available at: <https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf>.

[323.] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. (France).

[324.] Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles. (France).

[325.] Methodological Instruction of the Ministry of the Interior ref. no. SC-243/2006 of 6 September 2006, regulating the procedure of municipal authorities with extended competencies in the processing of applications for, and the issuance of, passports containing machine-readable data and biometric data carriers.

[326.] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[327.] 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).

[328.] Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726.

[329.] Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA.

[330.] Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816.

[331.] Resolution of the Presidium of the Czech National Council of 16 December 1992 on the declaration of the CHARTER OF FUNDAMENTAL RIGHTS AND FREEDOMS as a part of the constitutional order of the Czech Republic. In: Ústavní soud [online]. [2019-12-15]. Available at: <http://www.usoud.cz/fileadmin/user_upload/ustavni_soud_www/prilohy/Listina_English_version.pdf>.

[332.] Strafprozeßordnung (Germany)

[333.] Ustawa z dnia 10 maja 2018 r. – o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000). (Poland).

[334.] Wet van 16 mei 2018, houdende regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119) (Uitvoeringswet Algemene verordening gegevensbescherming). Stb. 2018, 144. (Netherlands).

[335.] Wet 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, BS 5 september 2018, C-2018/40581. (Belgium).

[336.] Zákon č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon) a o zmene a doplnení niektorých zákonov. (Slovak Republic).

[337.] Zákon č. 18/2017 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. (Slovak Republic).

[338.] Zakon o provedbi Opće uredbe o zaštiti podataka (Narodne novine, br. 42/2018). (Croatia).

Cases:

[339.] Decision of the Court of Justice of the European Union from 5 March 2015 case no. C-503/13 and C-504/13 (Boston Scientific Medizintechnik).

[340.] Decision of the European Court of Human Rights, 8 July 1978, no. 7572/76 (Ensslin, Baader, Raspe against Germany).

[341.] Decision of the European Court of Human Rights, 9 October 1979, no. 6289/73 (Airey against Ireland).

[342.] Decision of the European Court of Human Rights, 18 February 1991, no. 12033/86 (Fredin against Sweden).

[343.] Decision of the European Court of Human Rights, 6 April 2000, no. 34369/97 (Thlimmenos against Greece).

[344.] Decision of the European Court of Human Rights, 9 May 2000, no. 34129/96 (Sander against the United Kingdom).

[345.] Decision of the European Court of Human Rights, 24 July 2003, no. 40016/98 (Karner against Austria).

[346.] Decision of the European Court of Human Rights, 12 April 2006, no 65731/01 and no. 65900/01 (Stec and others against the United Kingdom).

[347.] Decision of the European Court of Human Rights, 31 July 2007, no. 11106/04, no. 11108/04, no. 11116/04, no. 11311/04 and no. č.13276/04 (Ekeberg and others against Norway).

[348.] Decision of the European Court of Human Rights, 25 May 2010, no. 37193/07 (Paraskeva Todorova against Bulgaria).

[349.] Decision of the European Court of Human Rights, 24 July 2012, no. 47159/08 (B.H. against Spain).

[350.] Decision of the Federal Constitutional Court of Germany BVerfg GE 65.

[351.] Decision of Human Rights Committee, 6 November 1997, no. 577/1994 (Polay Campos against Peru). In: *Office of the United Nations High Commissioner for Human Rights* [online]. [2016-05-15]. Available from: <https://www.ohchr.org/Documents/Publications/SDecisionsVol6en.pdf>.

[352.] Decision NS 29 Odo 14/2001 or NS 2 Odon 76/97.

[353.] Finding of the Constitutional Court of 12 October 1994 no. Pl. 4/94 (Anonymous Witness).

[354.] Finding of the Constitutional Court of 10 January 2001 no. Pl. ÚS 33/2000.

[355.] Finding of the Constitutional Court published under number 405/2002 Coll.

[356.] Finding of the Constitutional Court of 17 July 2007, no. IV. ÚS 23/05.

[357.] Finding of the Constitutional Court of 1 December 2008, no. I. ÚS 705/06.

[358.] Judgment of the Constitutional Court of the Czech Republic no. Pl. ÚS 4/94.

[359.] Judgment of the Constitutional Court of the Czech Republic no. Pl. ÚS 15/96.

[360.] Judgment of the Constitutional Court of the Czech Republic no. Pl. ÚS 16/98.

[361.] Judgment of the Constitutional Court of the Czech Republic, 28 April 2005, no. Pl. ÚS 60/04.

[362.] Judgment of the Constitutional Court of the Czech Republic no. Pl. ÚS 40/08.

[363.] Judgment of the Constitutional Court of the Czech Republic, 13 January 2010, no. II. ÚS 1174/09.

[364.] Judgment of the Constitutional Court of the Czech Republic no. Pl. ÚS 24/10 of 22 March 2011.

[365.] Judgment of the ECHR of 2 August 1984 no. 8691/79, Malone vs. United Kingdom.

[366.] Judgment of the ECHR of 26 March 1987 no. 9248181, Leander vs. Sweden.

[367.] Judgment of the ECHR of 16 February 2000 no. 27798/95, Amanna vs. Switzerland.

[368.] Judgment of the ECHR of 25 September 2001 no. 44787/98, p. G. and J. H. vs. United Kingdom.

[369.] Judgment of the ECHR of 14 February 2006 no. 57986/00, Turek vs. Slovakia.

[370.] Judgment of the ECHR of 3 April 2007 no. 62617/00, Coplad vs. United Kingdom.

[371.] Judgment of the ECHR of 15 November 2007 no. 12556/03, Pfeifer vs. Austria.

[372.] Judgement of the ECHR of 18 November 2008, no. 22427/04, Cemalettin Canlı *against Turkey.*

[373.] Judgment of the ECHR of 4 December 2008 no. 30562/04, S. and Marper vs. United Kingdom.

[374.] Judgment of the ECHR of 17 December 2009, Application no. 16428/05, Gardel vs. France.

[375.] Judgment of the ECHR of 2 September 2010, Application no. 35623/05 , Uzun vs. Germany.

[376.] Judgment of the Supreme Administrative Court of 28 June 2013, file number 5 As 1/2011 – 156.

[377.] Judgment of the Supreme Court no. NS 2 Odon 76/97.

[378.] Judgment of the Supreme Court no. NS 29 Odo 14/2001.

[379.] Judgment of the Supreme Court no. NS 29 Cdo 3919/2014.

[380.] Judgement of the United States Supreme Court, 23 April 1956, Griffin v. Illinois, 351 U.S. 12 (1956).

[381.] Judgement of the United States Supreme Court, 24 May 1983, Bearden v. Georgia, 461 U.S. 660 (1983).

[382.] Judgement of the United States Supreme Court, 26 June 1996, United States v. Virginia, 518 U.S. 515 (1996).

[383.] Opinion of the Supreme Court's plenum of 5 January 2017 on the filings made electronically and the delivery of documents electronically issued by the court through public data network, no. Plsn 1/2015.

Annex I. Report on Augmented Indicative Values of Biometric Data

Scope of the Report

Five main biometric technologies were chosen: fingerprint, face, iris, voice, and keystroke dynamics. Vast literature review was performed to indicate augmented indicative values of data gathered with help of these technologies. This literature is not included in the List of References above.

Overview of Augmented Indicative Values of Biometric Data

Augmented indicative values of biometric data at each examined type of biometric technology have been classified in five basic categories according to which class of traits of an individual they refer to. Categories that refer to certain aspects of a healthy individual are identity, mental state, and other (detailed description see below). Fourth category refers to diseases that can be identified from gathered data. Fifth category is derived from the fourth category and indicates complications that are likely connected with the identified disease.

Category	Description
Identity	General information about age, gender, racial, ethnic or cultural origin, or social status of an individual
Mental state	Momentary emotions of an individual
Other	Other information, such as evaluation of biological functioning, personal traits or prediction of performance of an individual
Disease	Anomalies from healthy state resulting in possible complications related to the disease as well as to special needs of an individual
Complications	Health complications usually occurring together with a certain disease

1. Fingerprint

1.1 Identity

Type of information	Resource
Determination of gender	Kaushal, N., Kaushal, P. Human Identification and Fingerprints: A Review. In: Journal of Biometrics & Biostatatistics, 2011, 2:123. doi:10.4172/2155-6180.1000123. Available at: <https://www.omicsonline.org/human-identification-and-fingerprints-a-review-2155-6180.1000123.php?aid=2581>. Soanboon, P., Nanakorn, S., Kutanan, W. Determination of sex difference from fingerprint ridge density in northeastern Thai teenagers. In: Egyptian Journal of Forensic Sciences, Volume 6, Issue 2, June 2016, Pages 185-193. Available at: <https://www.sciencedirect.com/science/article/pii/S2090536X15000738>.
Ancestral background	Fournier, N. A., Ross, A. H. Sex, Ancestral, and pattern type variation of fingerprint minutiae: A forensic perspective on anthropological dermatoglyphics. In: American Journal of Physical Anthropology, 23 September 2015. doi: 10.1002/ajpa.22869. Available at: <http://onlinelibrary.wiley.com/doi/10.1002/ajpa.22869/abstract>.

1.2 Mental state

Type of information	Resource
State of relaxation or anxiety based on fingertip temperature	Shivakumar, G., Vijaya, P. A. Emotion Recognition Using Finger Tip Temperature: First Step towards an Automatic System. In: International Journal of Computer and Electrical Engineering, Vol. 4, no. 3, June 2012. Available at: <http://www.ijcee.org/papers/489-P005.pdf>.
Intensity of acute stress	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. In: Physiology & Behavior, 2015, 152(Pt A), p. 225–230. Available at: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4664114/>.

1.3 Other

Type of information	Resource
Prediction of performance in attentional tasks	Vergara, R., Moënne-Loccoz, C., Maldonado, P. E. Cold-Blooded Attention: Finger Temperature Predicts Attentional Performance. In: Frontiers in Human Neuroscience, 12 September 2017. Available at: <https://www.frontiersin.org/articles/10.3389/fnhum.2017.00454/full>.
Indication of sympathetic responses	Kistlera, A., Mariauzoulsb, C., von Berlepscha, K. Fingertip temperature as an indicator for sympathetic responses. In: International Journal of Psychophysiology, Volume 29, Issue 1, 1 June 1998, Pages 35-41. Available at: <http://www.sciencedirect.com/science/article/pii/S0167876097000871>.

Measurement of pulse and possible detection of heart abnormalities	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>. 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>.
Cuts on fingers as indication of injury	

1.4 Disease and related complications

Disease	Related complications	Resource
Klinefelter's syndrome	Probability of sterility and small testicles, weaker muscles, greater height, poor coordination, less body hair, breast growth, and less interest in sex, reading difficulties and problems with speech	Dermatoglyphics. In: Wikipedia [online], 17.12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Dermatoglyphics>. Klinefelter syndrome. In: Wikipedia [online], 17.12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Klinefelter_syndrome>.
Cri du chat	Problems with the larynx and nervous system, probability of feeding problems because of difficulty in swallowing and sucking, low birth weight and poor growth, severe cognitive, speech, and motor delays, behavioral problems such as hyperactivity, aggression, outbursts, and repetitive movements, unusual facial features which may change over time, excessive drooling, small head and jaw, wide eyes, skin tags in front of eyes, Other common findings include hypotonia, microcephaly, growth retardation, a round face with full cheeks, hypertelorism, epicanthal folds, down-slanting palpebral fissures, strabismus, flat nasal bridge, down-turned mouth, micrognathia, low-set ears, short fingers, single palmar creases, and cardiac defects (e.g., ventricular septal defect [VSD], atrial septal defect [ASD], patent ductus arteriosus [PDA], tetralogy of Fallot).	Dermatoglyphics. In: Wikipedia [online], 17.12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Dermatoglyphics>. Cri du chat. In: Wikipedia [online], 17.12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Cri_du_chat>.

Naegeli–Franceschetti–Jadassohn syndrome	Rare autosomal dominant form of ectodermal dysplasia, probability of reticular skin pigmentation, diminished function of the sweat glands, the absence of teeth and hyperkeratosis of the palms and soles, absence of fingerprint lines on the fingers.	Dermatoglyphics. In: Wikipedia [online], 17.12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Dermatoglyphics>. Naegeli–Franceschetti–Jadassohn syndrome. In: Wikipedia [online], 11.12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Naegeli%E2%80%93Franceschetti%E2%80%93Jadassohn_syndrome>.
Noonan syndrome	Probability of congenital heart defect (typically pulmonary valve stenosis with dysplastic pulmonary valve also atrial septal defect and hypertrophic cardiomyopathy), short stature, learning problems, pectus excavatum, impaired blood clotting, and a characteristic configuration of facial features including a webbed neck and a flat nose bridge.	Dermatoglyphics. In: Wikipedia [online], 17.12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Dermatoglyphics>. Noonan syndrome. In: Wikipedia [online], 3.12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Noonan_syndrome>.
Patau syndrome	Probability of intellectual disability and motor disorder, Microcephaly, Holoprosencephaly (failure of the forebrain to divide properly), structural eye defects, including microphthalmia, Peters' anomaly, cataract, iris or fundus (coloboma), retinal dysplasia or retinal detachment, sensory nystagmus, cortical visual loss, and optic nerve hypoplasia, Meningomyelocele (a spinal defect), Polydactyly (extra digits), Cyclopia, Proboscis, congenital trigger digits, low-set ears, prominent heel, deformed feet known as rocker-bottom feet, Omphalocele (abdominal defect), abnormal palm pattern, overlapping of fingers over thumb, Cutis aplasia (missing portion of the skin/hair), Cleft palate, abnormal genitalia, kidney defects, heart defects (ventricular septal defect) (Patent Ductus Arteriosus), Dextrocardia, Single umbilical artery.	Dermatoglyphics. In: Wikipedia [online], 17.12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Dermatoglyphics>. Patau syndrome. In: Wikipedia [online], 17.12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Patau_syndrome>.

Edwards syndrome	Probability of kidney malformations, structural heart defects at birth (i.e., ventricular septal defect, atrial septal defect, patent ductus arteriosus), intestines protruding outside the body (omphalocele), esophageal atresia, intellectual disability, developmental delays, growth deficiency, feeding difficulties, breathing difficulties, and arthrogryposis (a muscle disorder that causes multiple joint contractures at birth, small head (microcephaly) accompanied by a prominent back portion of the head (occiput), low-set, malformed ears, abnormally small jaw (micrognathia), cleft lip/cleft palate, upturned nose, narrow eyelid folds (palpebral fissures), widely spaced eyes (ocular hypertelorism), drooping of the upper eyelids (ptosis), a short breast bone, clenched hands, choroid plexus cysts, underdeveloped thumbs and/or nails, absent radius, webbing of the second and third toes, clubfoot or rocker bottom feet, and in males, undescended testicles.	Dermatoglyphics. In: Wikipedia [online], 17.12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Dermatoglyphics>. Edwards syndrome. In: Wikipedia [online], 17.12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Patau_syndrome>.
Down syndrome	Probability of mental impairment, abnormal teeth, stunted growth, slanted eyes, Umbilical hernia, shortened hands, increased skin back of neck, short neck, low muscle tone, Obstructive sleep apnea, narrow roof of mouth, bent fifth finger tip, flat head, brushfield spots in the iris, flexible ligaments, single transverse palmar crease, proportionally large tongue, protruding tongue, abnormal outer ears, congenital heart disease, flattened nose, Strabismus, separation of first and second toes, undescended testicles.	Dermatoglyphics. In: Wikipedia [online], 17.12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Dermatoglyphics>. Down syndrome. In: Wikipedia [online], 17.12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Down_syndrome>.

Turner syndrome	Probability of short stature, Lymphedema (swelling) of the hands and feet of a newborn, broad chest (shield chest) and widely spaced nipples, low posterior hairline, low-set ears, reproductive sterility, rudimentary ovaries gonadal streak (underdeveloped gonadal structures that later become fibrotic), Amenorrhoea, the absence of a menstrual period, increased weight, obesity, shortened metacarpal IV, small fingernails, characteristic facial features, webbed neck from cystic hygroma in infancy, aortic valve stenosis, coarctation of the aorta, bicuspid aortic valve (most common cardiac problem), horseshoe kidney, visual impairments – sclera, cornea, glaucoma, etc., ear infections and hearing loss, high waist-to-hip ratio (the hips are not much bigger than the waist), attention deficit hyperactivity disorder (problems with concentration, memory, attention with hyperactivity seen mostly in childhood and adolescence), nonverbal learning disability (problems with maths, social skills, and spatial relations).	Dermatoglyphics. In: Wikipedia [online], 17.12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Dermatoglyphics>. Turner syndrome. In: Wikipedia [online], 17.12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Down_syndrome>.
Rubinstein–Taybi syndrome	Probability of broad thumbs and broad first toes and clinodactyly of the 5th finger, mental disability, small height, low bone growth, small head, Cryptorchidism in males, unusual facies involving the eyes, nose, and palate.	Dermatoglyphics. In: Wikipedia [online], 17.12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Dermatoglyphics>. Rubinstein–Taybi syndrome. In: Wikipedia [online], 25.11. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Rubinstein%E2%80%93Taybi_syndrome>.

Schizophrenia	Probability of mental disorder, abnormal social behavior and failure to understand what is real, false beliefs, unclear or confused thinking, hearing voices that others do not, reduced social engagement and emotional expression, and a lack of motivation, anxiety, depressive, or substance-use disorders, hallucinations, delusions (often bizarre or persecutory in nature), and disorganized thinking and speech.	Dermatoglyphics. In: Wikipedia [online], 17.12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Dermatoglyphics>. Schizophrenia. In: Wikipedia [online], 17.12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Schizophrenia>.
Congenital blindness	Probability of abnormal triradius and excess of arches on fingertips.	Dermatoglyphics. In: Wikipedia [online], 17.12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Dermatoglyphics>.

2. Face

2.1 Identity

Type of information	Resource
Age	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>.
Gender	Khan, S. A., Nazir, M., Akram, S., Riaz, N. Gender classification using image processing techniques: A survey. 2011 IEEE 14th International Multitopic Conference (INMIC). 2011, [2017-12-17]. Available at: <http://ieeexplore.ieee.org/document/6151483/>.
Ethnic origin	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>.

2.2 Mental state

Type of information	Resource
Emotion classification	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>.

2.3 Other

Type of information	Resource
Facial attractiveness	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>.

2.4 Disease and related complications

Disease	Related complications	Resource
Acromegaly	Possibility of severe headache, arthritis and carpal tunnel syndrome, enlarged heart, liver fibrosis and bile duct hyperplasia, hypertension, diabetes mellitus (excess of GH leads to insulin resistance), heart failure, kidney failure, colorectal cancer, compression of the optic chiasm leading to loss of vision in the outer visual fields (typically bitemporal hemianopia.), increased palmar sweating and sebum production over the face (seborrhea) are clinical indicators of active GH-producing pituitary tumors. These symptoms can also be used to monitor the activity of the tumor after surgery, although biochemical monitoring is confirmatory.	Catalog of Clinical Diseases. Images of the Head. In: University of California, San Diego [online]. [2017-12-17]. Available at: <https://meded.ucsd.edu/clinicalimg/head_neck.htm>. Acromegaly. In: Wikipedia [online]. 17. 12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Acromegaly>.
Angioedema	Possibility of swelling of the lower layer of skin and tissue just under the skin or mucous membranes.	Catalog of Clinical Diseases. Images of the Head. In: University of California, San Diego [online]. [2017-12-17]. Available at: <https://meded.ucsd.edu/clinicalimg/head_neck.htm>. Angioedema. In: Wikipedia [online]. 17. 12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Angioedema>.

Central CN7 Palsy	Possibility of note preservation of forehead movement bilaterally, subtle loss of left nasolabial fold and slightly impaired ability to raise left corner of mouth with smile.	Catalog of Clinical Diseases. Images of the Head. In: University of California, San Diego [online]. [2017-12-17]. Available at: <https://meded.ucsd.edu/clinicalimg/head_neck.htm>. Catalog of Clinical Diseases. Central CN7 Palsy. In: University of California, San Diego [online]. [2017-12-17]. Available at: <https://meded.ucsd.edu/clinicalimg/neuro_central_cn7_palsy.htm>.
Cervical Adenopathy	Possibility of metastatic, intraoral squamous cell cancer.	Catalog of Clinical Diseases. Images of the Head. In: University of California, San Diego [online]. [2017-12-17]. Available at: <https://meded.ucsd.edu/clinicalimg/head_neck.htm>. Catalog of Clinical Diseases. Cervical Adenopathy. In: University of California, San Diego [online]. [2017-12-17]. Available at: <https://meded.ucsd.edu/clinicalimg/head_cervical_adenopathy.htm>.
External Jugular Vein Distention	Possibility of elevated central venous pressure, hepatojugular reflux.	Catalog of Clinical Diseases. Images of the Head. In: University of California, San Diego [online]. [2017-12-17]. Available at: <https://meded.ucsd.edu/clinicalimg/head_neck.htm>. Catalog of Clinical Diseases. External Jugular Vein Distention. In: University of California, San Diego [online]. [2017-12-17]. Available at: <https://meded.ucsd.edu/clinicalimg/head_ejdistension1.htm>.
Scalp Hematoma and Cellulitis	Possibility of blunt head trauma.	Catalog of Clinical Diseases. Images of the Head. In: University of California, San Diego [online]. [2017-12-17]. Available at: <https://meded.ucsd.edu/clinicalimg/head_neck.htm>. Catalog of Clinical Diseases. Scalp Hematoma and Cellulitis. In: University of California, San Diego [online]. [2017-12-17]. Available at: <https://meded.ucsd.edu/clinicalimg/head_scalp_hematoma&cellulitis.htm>.

Distribution Zoster (Shingles)	Possibility of headache, fever, malaise, burning pain, itching, hyperesthesia (oversensitivity), or paresthesia (“pins and needles”: tingling, pricking, or numbness).	Catalog of Clinical Diseases. Images of the Head. In: University of California, San Diego [online]. [2017-12-17]. Available at: <https://meded.ucsd.edu/clinicalimg/head_neck.htm>. Shingles. In: Wikipedia [online]. 17. 12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Shingles>.
Parotitis	Possibility of inflammation of one or both parotid glands.	Catalog of Clinical Diseases. Images of the Head. In: University of California, San Diego [online]. [2017-12-17]. Available at: <https://meded.ucsd.edu/clinicalimg/head_neck.htm>. Parotitis. In: Wikipedia [online]. 17. 12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Parotitis>.
Parotid Gland	Possibility of lymphadenopathy or swelling of lymph nodes, fever, night sweats, weight loss, loss of appetite or anorexia, fatigue, respiratory distress or dyspnea, itching.	Catalog of Clinical Diseases. Images of the Head. In: University of California, San Diego [online]. [2017-12-17]. Available at: <https://meded.ucsd.edu/clinicalimg/head_neck.htm>. Lymphoma. In: Wikipedia [online]. 17. 12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Lymphoma>.
Temporalis Muscle Wasting	Possibility of l significant catabolism and/or generalized nutritional deficiency, rapidly progressive malignancy.	Catalog of Clinical Diseases. Images of the Head. In: University of California, San Diego [online]. [2017-12-17]. Available at: <https://meded.ucsd.edu/clinicalimg/head_neck.htm>. Catalog of Clinical Diseases. Temporalis Muscle Wasting. In: University of California, San Diego [online]. [2017-12-17]. Available at: <https://meded.ucsd.edu/clinicalimg/head_temporal_wasting2.htm>.

Craniofacial Disorders		
Apert Syndrome	Probability of cleft palate – about 30% of children with Apert Syndrome are affected, slower learning rates and abilities – about 50% of children with Apert Syndrome are affected; however, as the children grow older, they often catch up with others, vision problems caused by imbalance of the eye muscles, recurrent ear infections which can cause hearing loss, noisy breathing – the smaller nose and airway passages may make breathing difficult, hyperactive sweat glands may cause your child to sweat a lot, especially while sleeping, problems with acne are more likely, especially during puberty.	Apert Syndrome. In: FACES: The National Craniofacial Association [online]. [2017-12-17]. Available at: <http://www.faces-cranio.org/Disord/Apert.htm>.
Basal Cell Carcinoma Nevus Syndrome	Probability of basal cell carcinoma, jaw cysts (keratocystic odontogenic tumors), pits of the palms and soles, enlarged skulls and prominent foreheads, benign skin cysts, calcifications in the midline of the brain, rib abnormalities, spina bifida of the thoracic and cervical spine, ovarian cysts, hydrocephalus, boney abnormalities of the hands and feet.	Basal Cell Carcinoma Nevus Syndrome. In: FACES: The National Craniofacial Association. Available at: <http://www.faces-cranio.org/Disord/Apert.htm>. Basal Cell Carcinoma Nevus Syndrome. In: Basal Cell Carcinoma Nevus Syndrome Life Support Network [online]. [2017-12-17]. Available at: <https://bccns.org/>.
Cleft Lip and Palate	Probability of dental development – teeth in the area of the cleft may be missing or improperly positioned. This may affect your child's appearance and chewing ability, speech difficulties – cleft lip does not usually result in speech problems; however, often children with cleft palates benefit greatly from early speech therapy, frequent colds, sore throats, fluid in the ears and tonsil and adenoid problems.	Cleft Lip and Palate. In: FACES: The National Craniofacial Association [online]. [2017-12-17]. Available at: <http://www.faces-cranio.org/Disord/Cleft.htm>.

Cleidocranial Dysplasia	Probability of delayed closure (ossification) of the space between the bones of the skull (fontanels), premature closing of the coronal suture, protruding jaw (mandible) and protruding brow bone (frontal bossing), wide nasal bridge due to increased space between the eyes (hypertelorism), high arched palate or possible cleft palate, short stature, scoliosis of the spine, dental abnormalities – failure to lose the baby teeth (deciduous) at the expected time; slow eruption of secondary teeth; extra teeth; delayed or absent formation of teeth, ability to touch the shoulders together in front of the body, wide pelvic bone, loose joints, hearing loss and/or frequent infections.	Cleidocranial Dysplasia. In: FACES: The National Craniofacial Association [online]. [2017-12-17]. Available at: <http://www.faces-cranio.org/Disord/CCD.htm>.
Craniosynostosis	Probability of abnormal skull shape, abnormal forehead, asymmetrical eyes and or ears, intracranial pressure (pressure inside the skull) which can cause delays in development or permanent brain damage if not corrected.	Craniosynostosis. In: FACES: The National Craniofacial Association [online]. [2017-12-17]. Available at: <http://www.faces-cranio.org/Disord/Cranio.htm>.
Crouzon Syndrome	Probability of craniosynostosis, ocular proptosis, a small underdeveloped upper jaw, downward slanting eyelids, curved, parrot-like nose, high, narrow, arched palate, darkened, rough patches of skin found in the folds of the body (armpits, neck, groin, elbows, knees, chin/mouth area, eye area, or stomach), dental problems due to crowded teeth and a narrow palate, poor vision, ear diseases and hearing loss in about 50% of children, difficulty breathing due to small airway, possible fluid on the brain (hydrocephalus).	Crouzon Syndrome. In: FACES: The National Craniofacial Association [online]. [2017-12-17]. Available at: <http://www.faces-cranio.org/Disord/Crouzon.htm>.

Freeman-Sheldon Syndrome	Probability of a squinting eye, drooping upper eyelids, scoliosis (lateral curvature of the spine), during infancy, vomiting and feeding problems which usually improve with age, hearing loss, difficulty walking, club feet, contracted muscles of the joints of the fingers and hands, underdeveloped nose cartilage.	Freeman-Sheldon Syndrome. In: FACES: The National Craniofacial Association [online]. [2017-12-17]. Available at: <http://www.faces-cranio.org/Disord/Freeman.htm>.
Goldenhar Syndrome	Probability of hearing problems, weakness in moving the side of the face that is smaller, dental problems – the soft palate may move to the unaffected side of the face, the tongue may be smaller on the affected side of the face, fusion of the bones of the neck.	Goldenhar Syndrome. In: FACES: The National Craniofacial Association [online]. [2017-12-17]. Available at: <http://www.faces-cranio.org/Disord/Golden.htm>.
Hallerman-Streiff Syndrome	Probability of shortness than the average person, under development hair in many places, including in the facial, leg and pubic areas, eye problems including reduced eye size, bilateral cataracts and glaucoma.	Hallerman-Streiff Syndrome. In: FACES: The National Craniofacial Association [online]. [2017-12-17]. Available at: <http://www.faces-cranio.org/Disord.htm>. Hallerman-Streiff Syndrome. In: Wikipedia [online], 17.12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Hallermann%E2%80%93Streiff_syndrome>.
Hemifacial Microsomia	Probability of hearing problems depend on the structures that are involved, weakness in movement on the affected side of the face.	Hemifacial Microsomia. In: FACES: The National Craniofacial Association [online]. [2017-12-17]. Available at: <http://www.faces-cranio.org/Disord/Hemi.htm>
Hydrocephalus	Probability of increased intracranial pressure, dilation of the ventricles (the cavities of the brain), rapidly increasing head circumference, downward deviation of the eyes, full or bulging fontanel (the soft spot on an infant's head), prominent scalp veins.	Hydrocephalus. In: FACES: The National Craniofacial Association [online]. [2017-12-17]. Available at: <http://www.faces-cranio.org/Disord/Hydro.htm>.
Microtia	Probability of about a 40% reduction of hearing in the affected ear, problems locating the direction from which a sound comes, ear infections.	Microtia. In: FACES: The National Craniofacial Association [online]. [2017-12-17]. Available at: <http://www.faces-cranio.org/Disord/Microtia.htm>.

Moebius Syndrome	Probability of delayed crawling and/ or walking due to low muscle tone, respiratory illnesses due to low muscle tone, speech problems, hearing problems caused by fluid in the ears, limited movement of the tongue, teeth problems, sensitivity to loud sounds, sensitivity to bright light.	Moebius Syndrome. In: FACES: The National Craniofacial Association [online]. [2017-12-17]. Available at: http://www.faces-cranio.org/Disord/Microtia.htm>.
Nager Syndrome	Possibility of underdevelopment of the cheek and jaw area, down-sloping of the opening of the eyes, lack or absence of the lower eyelashes, lack of development of the internal and external ear, possible cleft palate, underdevelopment or absence of the thumb, shortened forearms and poor movement in the elbow, limited range of arm motion, stomach and kidney reflux, temporary or long-term hearing loss.	Nager Syndrome. In: FACES: The National Craniofacial Association [online]. [2017-12-17]. Available at: <http://www.faces-cranio.org/Disord/Nager.htm>.
Miller Syndrome	Possibility of incomplete limb development, webbing of fingers or toes, absence of certain fingers and /or toes, underdevelopment of the ulna (bones on the “pinkie” side) and the radius (bones on the thumb side) causing the forearms to appear unusually short, micrognathia.	Miller Syndrome. In: FACES: The National Craniofacial Association [online]. [2017-12-17]. Available at: <http://www.faces-cranio.org/Disord/Miller.htm>.
Nasal Encephaloceles	Probability of neurologic problems, hydrocephalus (cerebrospinal fluid accumulated in the brain), spastic quadriplegia (paralysis of the limbs), microcephaly (an abnormally small head), ataxia (uncoordinated muscle movement), developmental delay, vision problems, mental and growth retardation, and seizures.	Nasal Encephaloceles. In: FACES: The National Craniofacial Association [online]. [2017-12-17]. Available at: <http://www.faces-cranio.org/Disord.htm>. Encephalocele. In: Wikipedia [online], 29.11. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Encephalocele>.
Neurofibromatosis	Probability of learning and behavior problems, light brown spots on the skin, freckles in the armpit and groin, small bumps within nerves, and scoliosis, hearing loss, cataracts at a young age, balance problems, flesh colored skin flaps, and muscle wasting.	Neurofibromatosis. In: FACES: The National Craniofacial Association [online]. [2017-12-17]. Available at: <http://www.faces-cranio.org/Disord.htm>. Neurofibromatosis. In: Wikipedia [online], 16.12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Neurofibromatosis>.

Orbital Hypertelorism	Probability of piebaldism, prominent inner third of the eyebrows, irises of different color, spondyloepiphyseal dysplasia, mucopolysaccharide metabolism disorders, deafness and also in hypothyroidism.	Orbital Hypertelorism. In: FACES: The National Craniofacial Association [online]. [2017-12-17]. Available at: <http://www.faces-cranio.org/Disord.htm>. Hypertelorism. In: Wikipedia [online], 24.06. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Hypertelorism>.
Parry Romberg Syndrome	Probability of slowly progressive deterioration (atrophy) of the skin and soft tissues of half of the face (hemifacial atrophy), usually the left side, neurological abnormalities including seizures and episodes of severe facial pain (trigeminal neuralgia)	Parry Romberg Syndrome. In: FACES: The National Craniofacial Association [online]. [2017-12-17]. Available at: <http://www.faces-cranio.org/Disord/parryromberg.htm>.
Pfeiffer Syndrome	Probability of underdevelopment of the midface ,skull is prematurely fused and unable to grow normally (craniosynostosis),bulging wide-set eyes due to shallow eye sockets (occular proptosis), broad, short thumbs and big toes, possible webbing of the hands and feet, dental problems due to crowded teeth and often a high palate, poor vision, hearing loss.	Pfeiffer Syndrome. In: FACES: The National Craniofacial Association [online]. [2017-12-17]. Available at: <http://www.faces-cranio.org/Disord/Pfeiffer.htm>.
Pierre Robin Sequence	Possibility of small lower jaw (micrognathia), a tongue which tens to ball up at the back of the mouth and fall back towards the throat (glossoptosis), breathing problems, horseshoe-shaped cleft palate, feeding problems in infancy, ear infections, reduced hearing.	Pierre Robin Sequence. In: FACES: The National Craniofacial Association [online]. [2017-12-17]. Available at: <http://www.faces-cranio.org/Disord/PierreRobin.htm>.
Saethre-Chotzen Syndrome	Possibility of fusion of the cranial structures which sometimes produces an asymmetric head and face, low-set hairline, droopy eyelids (ptosis) and/or widely spaced eyes, “beaked” nose and possible deviated septum, abnormalities of the fingers and/or toes.	Saethre-Chotzen Syndrome. In: FACES: The National Craniofacial Association [online]. [2017-12-17]. Available at: <http://www.faces-cranio.org/Disord/Saethre.htm>.
Stickler Syndrome	Possibility of joint pain, scoliosis, hearing loss, mitrovalve prolapse.	Stickler Syndrome. In: FACES: The National Craniofacial Association [online]. [2017-12-17]. Available at: <http://www.faces-cranio.org/Disord/Stickler.htm>.

Sturge Weber	Possibility of glaucoma, seizures, vascular headache, developmental (Cognitive) Delay, hemianopsia, hemiparesis.	Sturge Weber. In: FACES: The National Craniofacial Association [online]. [2017-12-17]. Available at: <http://www.faces-cranio.org/Disord.htm>. Sturge–Weber syndrome. In: Wikipedia [online], 17.12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Sturge%E2%80%93Weber_syndrome>.
Treacher Collins Syndrome	Possibility of breathing problems and/or eating difficulties, most children have a 40% hearing loss in each ear due to abnormalities of the outer and middle ear, which conduct sound to the nerve endings, the eyes have a tendency to dry out, which can lead to infection, cleft palate.	Treacher Collins Syndrome. In: FACES: The National Craniofacial Association [online]. [2017-12-17]. Available at: <http://www.faces-cranio.org/Disord/Treacher.htm>.
Vascular Birthmarks	Possibility of hemangiomas (non-cancerous tumors) and Vascular Malformations (non-cancerous lesions).	Vascular Birthmarks. In: FACES: The National Craniofacial Association [online]. [2017-12-17]. Available at: <http://www.faces-cranio.org/Disord/Vascular.htm>.
Velo-cardio-facial Syndrome	Possibility of multiple abnormalities of the heart, learning disabilities in one or more areas, hearing loss, problems with speech, leg pain, extremes of behavior.	Velo-cardio-facial Syndrome. In: FACES: The National Craniofacial Association [online]. [2017-12-17]. Available at: <http://www.faces-cranio.org/Disord/Velo.htm>.

3. Iris

3.1 Disease and related complications

Disease	Related complications	Resource
Cataract	Possibility of reduction of vision, glare, decrease in vision, faded colors, blurry vision, halos around light, trouble with bright lights, and trouble seeing at night.	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 2nd International Conference on Cybernetics (CYBCONF). 2015 [2017-12-17]. Available at: <http://ieeexplore.ieee.org/document/7175984/>. Cataract. In: Wikipedia [online]. 17. 12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Cataract>.

Acute glaucoma	Possibility of vision loss, eye pain, blurred vision, mid-dilated pupil, redness of the eye, and nausea.	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 2nd International Conference on Cybernetics (CYBCONF). 2015 [2017-12-17]. Available at: <http://ieeexplore.ieee.org/document/7175984/>. Acute glaucoma. In: Wikipedia [online]. 17. 12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Glaucoma>.
Posterior and anterior synechiae	Not identified.	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 2nd International Conference on Cybernetics (CYBCONF). 2015 [2017-12-17]. Available at: <http://ieeexplore.ieee.org/document/7175984/>.
Retinal detachment	Possibility of increased number of floaters, flashes of light, worsening of the outer part of the visual field.	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 2nd International Conference on Cybernetics (CYBCONF). 2015 [2017-12-17]. Available at: <http://ieeexplore.ieee.org/document/7175984/>. Retinal detachment. In: Wikipedia [online]. 26. 11. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Retinal_detachment>.

Rubeosis iridis	Not identified.	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 2nd International Conference on Cybernetics (CYBCONF). 2015 [2017-12-17]. Available at: <http://ieeexplore.ieee.org/document/7175984/>.
Corneal vascularization	Possibility of threaten eyesight.	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 2nd International Conference on Cybernetics (CYBCONF). 2015 [2017-12-17]. Available at: <http://ieeexplore.ieee.org/document/7175984/>. Corneal neovascularization. In: Wikipedia [online]. 02. 12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Corneal_neovascularization>.
Corneal ulcers, haze or opacities	Possibility of reduced visual acuity, ciliary flush (circumcorneal injection), corneal abnormalities including edema or opacities (“corneal haze”), corneal staining, abnormal pupil size, abnormal intraocular pressure	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 2nd International Conference on Cybernetics (CYBCONF). 2015 [2017-12-17]. Available at: <http://ieeexplore.ieee.org/document/7175984/>. Red eye (medicine). In: Wikipedia [online]. 26. 11. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Red_eye_(medicine)#Diagnostic_approach>.

Corneal grafting	Not identified.	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 2nd International Conference on Cybernetics (CYBCONF). 2015 [2017-12-17]. Available at: <http://ieeexplore.ieee.org/document/7175984/>.
Iris damage and atrophy	Not identified.	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 2nd International Conference on Cybernetics (CYBCONF). 2015 [2017-12-17]. Available at: <http://ieeexplore.ieee.org/document/7175984/>.

4. Voice

4.1 Identity

Type of information	Resource
Gender	Johar, S. Emotion, Affect and Personality in Speech. The Bias of Language and Paralanguage. Springer, 2016. Available at: <http://www.springer.com/gp/book/9783319280455>.
Age	Johar, S. Emotion, Affect and Personality in Speech. The Bias of Language and Paralanguage. Springer, 2016. Available at: <http://www.springer.com/gp/book/9783319280455>.

4.2 Mental state

Type of information	Resource
Identification of anger, joy, fear, sadness, boredom, happiness, distress, extreme fear	Johar, S. Emotion, Affect and Personality in Speech. The Bias of Language and Paralanguage. Springer, 2016. Available at: <http://www.springer.com/gp/book/9783319280455>.

Depression, suicidal tendencies, level of self-consciousness	Singh, R., Baker, J., Pennant, L., Morency, L. p. Deducing the Severity of Psychiatric Symptoms from the Human Voice. 15. 3. 2017. Available at: <https://arxiv.org/pdf/1703.05344.pdf>.

4.3 Other

Type of information	Resource
Dominance and attractiveness, threat potential, social status, personality, sexual orientation, hormone level, use of prescription medication	Singh, R., Baker, J., Pennant, L., Morency, L. P. Deducing the Severity of Psychiatric Symptoms from the Human Voice. 15. 3. 2017. Available at: <https://arxiv.org/pdf/1703.05344.pdf>.
Lie detection	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>.
Perception of difference in social status	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>.

4.4 Disease and related complications

Disease	Related complications	Resource
State of health in general	*Does not apply*	Johar, S. Emotion, Affect and Personality in Speech. The Bias of Language and Paralanguage. Springer, 2016. Available at: <http://www.springer.com/gp/book/9783319280455>.

Parkinson's disease	Possibility of movement ("motor") related disease, autonomic dysfunction, neuropsychiatric problems (mood, cognition, behavior or thought alterations), and sensory (especially altered sense of smell), sleep difficulties, tremor, slowness of movement (bradykinesia), rigidity (stiffness and resistance to limb movement caused by increased muscle tone, an excessive and continuous contraction of muscles), and postural instability (impaired balance and frequent falls ,bone fractures, loss of confidence, and reduced mobility), executive dysfunction (problems with planning, cognitive flexibility, abstract thinking, rule acquisition, inhibiting inappropriate actions, initiating appropriate actions, working memory, and control of attention, slowed cognitive processing speed, impaired recall and impaired perception and estimation of time), Nevertheless, improvement appears when recall is aided by cues, Visuospatial difficulties are also part of the disease, seen for example when the individual is asked to perform tests of facial recognition and perception of the orientation of drawn lines), sleep problems (daytime drowsiness (including sudden sleep attacks resembling narcolepsy), disturbances in REM sleep, or insomnia).	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/>. Parkinson's disease. In: Wikipedia [online]. 17. 12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Parkinson%27s_disease>.
Schizophrenia	Probability of mental disorder, abnormal social behavior and failure to understand what is real, false beliefs, unclear or confused thinking, hearing voices that others do not, reduced social engagement and emotional expression, and a lack of motivation, anxiety, depressive, or substance-use disorders, hallucinations, delusions (often bizarre or persecutory in nature), and disorganized thinking and speech.	Singh, R., Baker, J., Pennant, L., Morency, L. P. Deducing the Severity of Psychiatric Symptoms from the Human Voice. 15. 3. 2017. Available at: <https://arxiv.org/pdf/1703.05344.pdf>. Schizophrenia. In: Wikipedia [online], 17.12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Schizophrenia>.

Autism	Possibility of impairments in social interaction; impairments in communication; and restricted interests and repetitive behavior, stereotyped behaviors: repetitive movements, such as hand flapping, head rolling, or body rocking, compulsive behaviors: time-consuming behaviors intended to reduce anxiety that an individual feels compelled to perform repeatedly or according to rigid rules, such as placing objects in a specific order, checking things, or hand washing, sameness: resistance to change; for example, insisting that the furniture not be moved or refusing to be interrupted, ritualistic behavior: unvarying pattern of daily activities, such as an unchanging menu or a dressing ritual, restricted interests: interests or fixations that are abnormal in theme or intensity of focus, such as preoccupation with a single television program, toy, or game, self-injury: behaviors such as eye-poking, skin-picking, hand-biting and head-banging, superior skills in perception and attention, sensory abnormalities, deficits in motor coordination.	Singh, R., Baker, J., Pennant, L., Morency, L. P. Deducing the Severity of Psychiatric Symptoms from the Human Voice. 15. 3. 2017. Available at: <https://arxiv.org/pdf/1703.05344.pdf>. Autism. In: Wikipedia [online]. 17. 12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Autism>.
Huntington's disease	Possibility of jerky, random, and uncontrollable movements called chorea, restlessness, small unintentionally initiated or uncompleted motions, lack of coordination, or slowed saccadic eye movements, rigidity, writhing motions, abnormal posturing, physical instability, abnormal facial expression, difficulties chewing, swallowing, and speaking, sleep disturbances.	Singh, R., Baker, J., Pennant, L., Morency, L. P. Deducing the Severity of Psychiatric Symptoms from the Human Voice. 15. 3. 2017. Available at: <https://arxiv.org/pdf/1703.05344.pdf>. Huntington's disease. In: Wikipedia [online]. 17. 12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Huntington%27s_disease>.
Praedementia	See Alzheimer's disease below.	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. Available at: <http://www.sciencedirect.com/science/article/pii/S2352872915000160>.

Alzheimer's disease	Possibility of short term memory loss, which shows up as difficulty in remembering recently learned facts and inability to acquire new information, executive functions of attentiveness, planning, flexibility, and abstract thinking, or impairments in semantic memory (memory of meanings, and concept relationships), apathy, depressive, difficulties with language, executive functions, perception (agnosia), or execution of movements (apraxia), language problems are mainly characterized by a shrinking vocabulary and decreased word fluency, progressive deterioration, illusionary misidentifications and other delusional symptoms, frequent incorrect word substitutions (paraphasias).	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. Available at: <http://www.sciencedirect.com/science/article/pii/S2352872915000160>. Alzheimer's disease. In: Wikipedia [online]. 17. 12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Alzheimer%27s_disease>.

5. Keystroke dynamics

5.1 Identity

Type of information	Resource
Age detection	Tsimperidis, G., Katos, V. and Rostami, S. Age Detection Through Keystroke Dynamics From User Authentication Failures. In: International Journal of Digital Crime and Forensics (IJDCF), 2017, 9 (1), pp. 1-16. Available at: <http://eprints.bournemouth.ac.uk/25123/>.
Determination of gender	Tsimperidis, I., Katos, V., & Clarke, N. Language-independent gender identification through keystroke analysis. In: Information and Computer Security, 2015, 23(3), 286-301. Available at: <http://www.emeraldinsight.com/doi/abs/10.1108/ICS-05-2014-0032>. Fairhurst, M., Da Costa-Abreu, M. Using keystroke dynamics for gender identification in social network environment. 4th International Conference o n Imaging for Crime Detection and Prevention 2011 (ICDP 2011). doi:http://dx.doi.org/10.1049/ic.2011.0124. Available at: <http://ieeexplore.ieee.org/document/6203675/>. Antal, M., Nemes, G. Gender recognition from mobile biometric data. 2016 IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI). doi:10.1109/SACI.2016.7507379. Available at: <http://ieeexplore.ieee.org/document/7507379/>.

5.2 Mental state

Type of information	Resource
Prediction of emotional states, such as happiness or stress	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. IEEE; 2014:74-79. doi:10.1109/BIOMS.2014.6951539. Available at: <http://ieeexplore.ieee.org/document/6951539/>. References made to: C. Epp, M. Lippold, and R. L. Mandryk. Identifying emotional states using keystroke dynamics. In: Proc. 2011 Annu. Conf. Hum. factors Comput. Syst.-CHI '11, p. 715, 2011 L. M. Vizer, L. Zhou, and A. Sears. Automated stress detection using keystroke and linguistic features: An exploratory study. In: Int. J. Hum. Comput. Stud., vol. 67, no. 10, pp. 870–886, Oct. 2009. H.-R. Lv, Z.-L. Lin, W.-J. Yin, and J. Dong. Emotion recognition based on pressure sensor keyboards. In: 2008 IEEE Int. Conf. Multimed. Expo, pp. 1089–1092, Jun. 2008. J. Hernandez and p. Paredes. Under pressure: sensing stress of computer users. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '14, 2014, pp. 51–60. A. Kolakowska. A review of emotion recognition methods based on keystroke dynamics and mouse movements. In: 2013 6th International Conference on Human System Interactions (HSI), 2013, pp. 548–555.

5.3 Other

No relevant research was identified that could identify other information with regard to keystroke dynamics analysis.

5.4 Disease and related complications

Disease	Related complications	Resource
Parkinson's disease	Possibility of movement ("motor") related disease, autonomic dysfunction, neuropsychiatric problems (mood, cognition, behavior or thought alterations), and sensory (especially altered sense of smell), sleep difficulties, tremor, slowness of movement (bradykinesia), rigidity (stiffness and resistance to limb movement caused by increased muscle tone, an excessive and continuous contraction of muscles), and postural instability (impaired balance and frequent falls ,bone fractures, loss of confidence, and reduced mobility), executive dysfunction (problems with planning, cognitive flexibility, abstract thinking, rule acquisition, inhibiting inappropriate actions, initiating appropriate actions, working memory, and control of attention, slowed cognitive processing speed, impaired recall and impaired perception and estimation of time), Nevertheless, improvement appears when recall is aided by cues, Visuospatial difficulties are also part of the disease, seen for example when the individual is asked to perform tests of facial recognition and perception of the orientation of drawn lines), sleep problems (daytime drowsiness (including sudden sleep attacks resembling narcolepsy), disturbances in REM sleep, or insomnia).	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>. Parkinson's disease. In: Wikipedia [online]. 17. 12. 2017 [2017-12-17]. Available at: <https://en.wikipedia.org/wiki/Parkinson%27s_disease>.
Psychomotor impairment due to sleep inertia	Not identified.	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>.