BRAIN. Broad Research in Artificial Intelligence and Neuroscience
ISSN: 2068-0473 | e-ISSN: 2067-3957
Covered in: Web of Science (WOS); PubMed.gov; IndexCopernicus; The Linguist List; Google Academic; Ulrichs; getCITED; Genamics JournalSeek; J-Gate; SHERPA/RoMEO; Dayang Journal System; Public Knowledge Project; BIUM; NewJour; ArticleReach Direct; Link+; CSB; CiteSeerX; Socolar; KVK; WorldCat; CrossRef; Ideas RePeC; Econpapers; Socionet.

2023, Volume 14, Issue 4, pages: 124-139 | https://doi.org/10.18662/brain/14.4/496

Ethical Aspects of Biometric Identification

Madalina Maria DIAC[1],
Simona Irina DAMIAN[2],
Bianca Diana BUTINCU[3],
Anton KNIELING[4],
Diana BULGARU-ILIESCU[5],

[1] Forensic Medicine Sciences Department, University of Medicine and Pharmacy Grigore T Popa Iasi, Institute of Legal Medicine Iasi, Romania, madalina-maria.diac@umfiasi.ro

[2] Forensic Medicine Sciences Department, University of Medicine and Pharmacy Grigore T Popa Iasi, Institute of Legal Medicine Iasi, Romania, simona.damian@umfiasi.ro , si_damian@yahoo.com

[3] MD, University of Medicine and Pharmacy Grigore T Popa Iasi, Romania, bianca.butincu@yahoo.com

[4] Forensic Medicine Sciences Department, University of Medicine and Pharmacy Grigore T Popa Iasi, Institute of Legal Medicine Iasi, Romania, tony_knieling@yahoo.com

[5] Forensic Medicine Sciences Department, University of Medicine and Pharmacy Grigore T Popa Iasi, Institute of Legal Medicine Iasi, Romania, bulgarudiana@yahoo.com

Abstract: *The term biometrics derives from Greek (bio=life and metrics=measure) and implies the measurement of biological signs. Biometrics is the science of recognizing people based on their physical, behavioral, and physiological attributes, such as fingerprint, face scan, iris, retina, and voice. The present paper aims to develop a study on biometric identification. The major objective of the study is to conduct a survey among the Romanian population on the importance and knowledge of biometric identification methods. This objective was achieved by assessing the knowledge held by the general population of Romania regarding biometric indicators and the degree of adaptability and openness of citizens related to the widest possible implementation of biometrics. The study was based on conducting a quantitative analysis using a questionnaire. Due to the high degree of accessibility, the online environment was chosen as a method of application, distribution being made through social networks. A biometric template digitizes the human body, it has been argued that the collection of biometric identifiers not only interferes with the privacy and right to protection of a person's data, but also with the integrity of an individual's body. In conclusion, the creation and storage of a unique biometric template must be seen in relation to the purpose of the operation. The protection of citizens from criminal activities is a primary obligation of the state. However, it must be exercised with due respect for a number of fundamental ethical values and in the light of modern human rights law.*

Keywords: *biometry, identification, ethical aspects, questionnaire study, database.*

How to cite: Diac, M. M., Damian, S. I., Butincu, B. D., Knieling, A., & Bulgaru-Iliescu, D. (2023). Ethical aspects of biometric identification. *BRAIN. Broad Research in Artificial Intelligence and Neuroscience, 14*(4), 124-139. https://doi.org/10.18662/brain/14.4/496

Introduction

The first historically recognized application of a procedure of biometric identification took place in Ancient Egypt, with the aim of ensuring that the food supplied by the state would be divided fairly. To this end, a system was developed to document the distinct physical and behavioral characteristics of workers, together with their name, place of residence and age (Ashbourn, 2000; Smith et al. 2018).

The term *biometrics* derives from Greek (*bio=life and metrics=measure) and implies the measurement of biological signs (*Jain et al, 2008*)*. Biometrics is defined as the science of recognizing people on the basis on individual physical, physiological and behavioral characteristics, such as fingerprints, face scans, iris, retina, and voice. A classic biometric system acquires data from a person (e.g. fingerprints), extracts a specific set of features and compares them with templates from a database in order to either determine identity or to verify a claimed one (Belhadj, 2017).

A typical biometric system consists of four main modules: biometric sensor (responsible for capturing biometric features and converting them into a digital form), a quality assessment and trait extraction module (template generation), a matching module and a database. Biometric systems can be both static (fingerprint, hand geometry, iris, retina, face) and dynamic (voice and signature) (Jain et al. 2008).

A significant development occurred in the middle of the XIX century, when Czech scientist Jan Evangelista Purkinje (1787-1869) determined that fingerprints are unique (Ashbourn, 2000). The first-generation biometric systems were focused on uniquely identifying or authenticating specific individuals. It was not until the late 1990s that the first cases of widespread use of such systems began in the US, followed by a significantly increased spread after the 2001 terrorist attacks with the introduction of biometric passports, which contain fingerprints and facial data (Wolf, 2017; Ramalingam et al. 2018).

As time passed, the first-generation biometric systems advanced due to an increased performance of computer systems, substantially reducing error rates (especially in facial recognition techniques). These first-generation biometric systems have developed into a fast and reliable identification and authentication tool, used in a wide variety of situations, such as law enforcement purposes or electoral voting. Apps using fingerprint and facial recognition technologies have even reached the private sector, being used for unlocking smartphones or recognizing customers. These techniques replace traditional security measure (such as text-based passwords) due to the latest facial recognition technology, which allows for an individual to be identified in less than a second (Ramalingam et al. 2018).

The public sector increasingly relies on biometric techniques in various sections, such as healthcare, law enforcement and border security. The global trends of hyper-individualization, heightened security concerns and continuous need for improvement of digital services continue to be strong driving factors for the development of better, more accurate biometric technologies in the following years (Sohnemann et al. 2020). Adopting them will undoubtedly increase the probability that more and more people will come into contact with this kind of technology, which will certainly lead to a broader discussion of ethical concerns.

The present paper aims to develop a study on biometric identification. The major objective of the study is to conduct a survey among the Romanian population on the importance and knowledge of biometric identification methods. This objective was achieved by assessing the information held by the general population of Romania regarding biometric indicators and the degree of adaptability and openness of citizens in relation to the widest possible implementation of biometric systems.

Material and method

The study was based on conducting a quantitative analysis using a questionnaire. Due to the high degree of accessibility, the online environment was chosen as a method of application, distribution being made through social networks (*Facebook-Questionnaires made by students, master students, doctoral students and researchers*, WhatsApp, Yahoo Mail), and data processing was done with the help of Microsoft Office tools - Excel. For the questionnaire, questions relevant to the topic were used, with the help of which a wide range of opinions were obtained on the methods of identification of an individual by biometric means.

The tool used to highlight the importance of databases and ethical issues raised by biometric identification methods is a questionnaire containing a limited number of questions with mixed answers. Closed-ended questions with predetermined answer options guide people to tick off one of the proposed answers. The individual will express his/her own opinion and approach situations with personal examples regarding the subject of the question through open-ended questions.

The questionnaire was applied to a number of 130 people, consisting of both women and men aged from under 20 to 70 years, with higher education, but also secondary or incomplete, for a period of three months. The surveyed group consists mainly of employees, but also includes students and pensioners. The questionnaire was anonymous and will not be communicated in full form. This method of data collection also met the provisions of the Personal Data Protection Regulation.

The elaborated questionnaire was divided as follows: i) demographic data: age, sex, background, education, profession; ii) current knowledge of biometric identification methods and benefits; iii) the possibility of introducing biometric indicators in identity documents in compliance with fundamental rights and their securing capability; iv) indication of biometric features for the creation of databases, giving reasons for choice, indication of easily falsifiable biometric indicators and those that would violate fundamental rights.

Results and discussion

The results of the survey on the demographic structure of respondents are shown in the figures below (Figure 1-4) - Authors own conception (statistical analysis). Regarding demographic data, it was found that people aged between 20 and 29 responded with the highest percentage of 36%, the percentage of response decreasing with age. It is also noted that there were responses with a higher distribution among women present in the age group of 20-29 years.

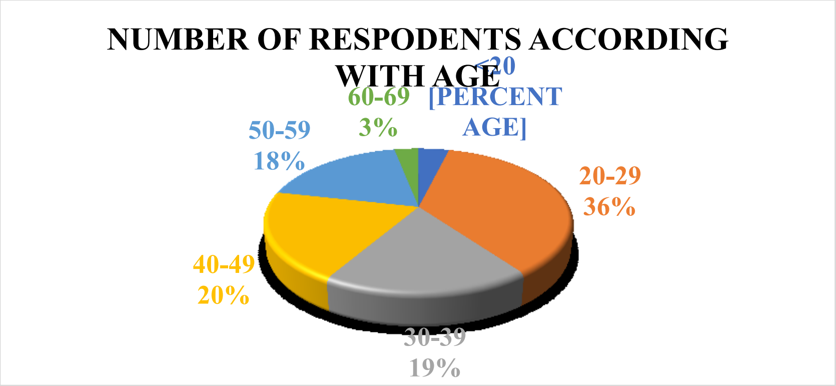

Figure 1 Respondents according with age (Authors own conception (statistical analysis))

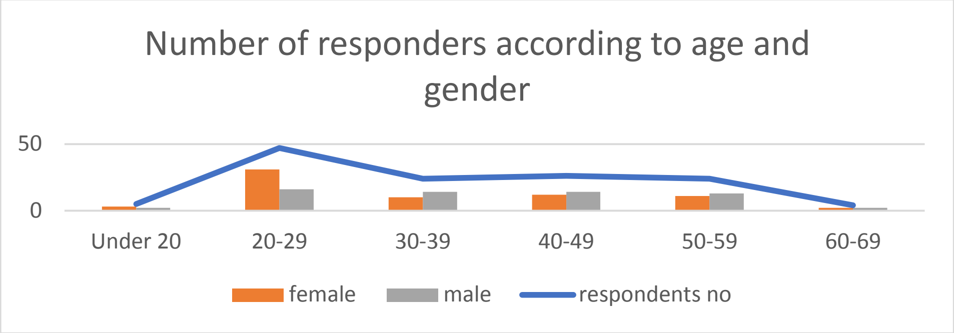

Figure 2 Respondents according to age and gender (Authors own conception (statistical analysis)

There is a higher number of respondents from urban areas and less from rural areas, as well as a higher share of women in the category aged 20-29 in urban areas. At the same time, the largest share of respondents is represented by those with higher university and postgraduate education, representing over 67% of the total number of the sample.

Regarding the current degree of knowledge on biometrics-based identification methods, 108 respondents (83.07%) claim to have heard about the possibility of recognizing a person based on physical and behavioral characteristics. Analyzing the respondents' answers, we find that the level of knowledge of biometrics-based identification methods is increased within each age category but does not differ among female and male respondents. Also, depending on the last form of education graduated, the largest share is occupied by that of people with higher education (university and postgraduate), but within each subcategory there is a degree of knowledge of over 80% both in the category of high school graduates (82.85%) and in the subcategories "university studies" (88.88%) and "postgraduate" studies (88.88%).

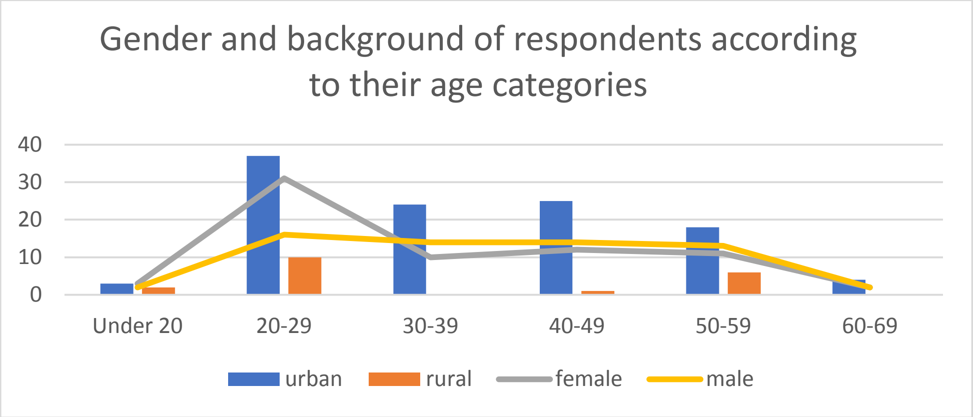

Figure 3 Gender and background of respondents according to their age categories (authors own conception – statistical analysis)

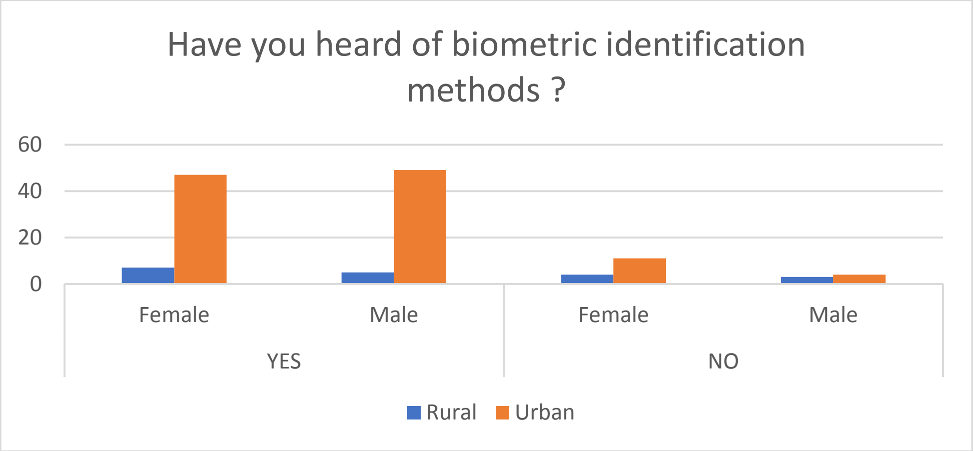

Figure 4 Quantitative analysis of biometric identification knowledge (authors own conception – statistical analysis)

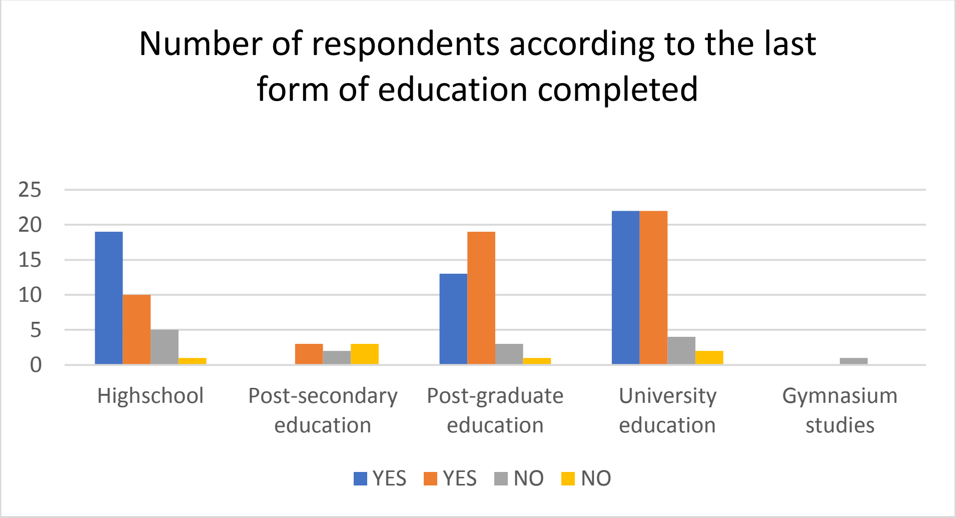

Figure 5 Number of respondents according to the last form of education completed (authors own conception – statistical analysis)

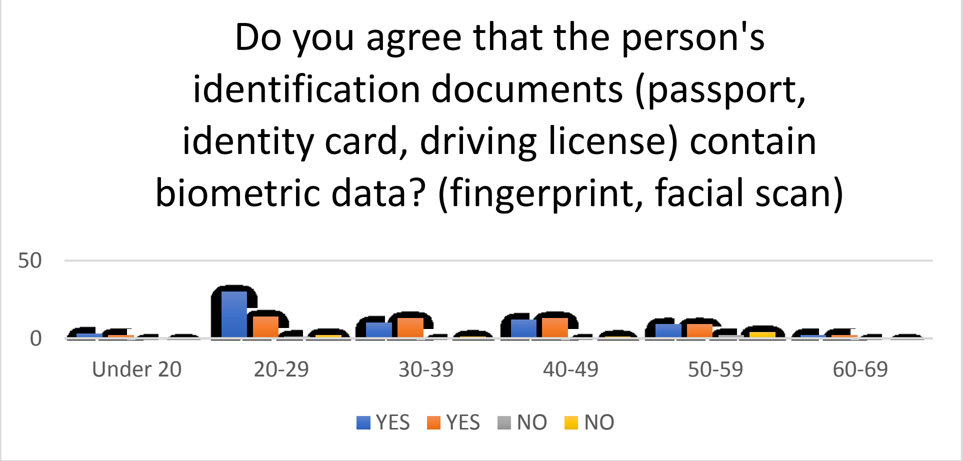

Figure 6 Quantitative analysis of agreement of biometric data (authors own conception – statistical analysis)

In this questionnaire, we were also interested in the possibility of introducing biometric indicators in identity documents in compliance with fundamental rights and the ability to secure their biometric indicators. Thus, regarding the agreement on the introduction of biometric data on the identification documents of persons, it is found that 91.54% agree and only 8.46% expressed disagreement. Of the 119 affirmative answers (most of them in the 20-29 age group), 66 belong to the female gender and 53 to the male one.

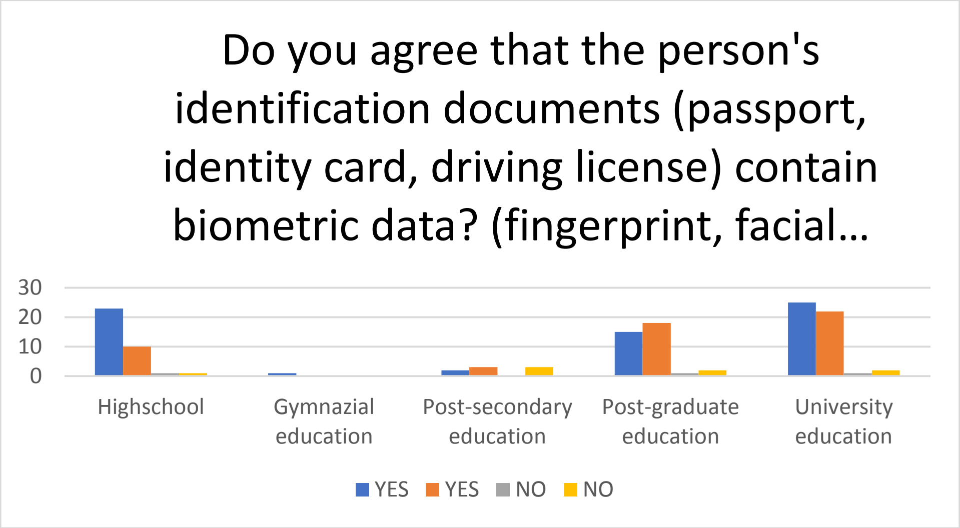

Figure 7 Quantitative analysis of agreement of biometric data (authors own conception – statistical analysis)

Respondents who disagreed that the identification documents (passport, identity card, car license) contain biometric data (fingerprint, facial scan) had the opportunity to argue their choice through the open answer question (number 8), supporting various reasons. Out of the number of respondents who do not want identification documents to contain biometric indicators, 27.27% claim that their right to privacy is violated, others summoning reasons related to their own religion and safety.

No.	Reason(s)	No. of respondents
1	**Violation of fundamental rights:** My fundamental rights are violated/ Violation of private freedom/ Right to privacy.	3
2	**Necessity: I don't** *consider them necessary yet/ I don't agree with these ways of identifying a person. The identity card, the non-biometric passport is enough.*	2
3	**Religious reasons**: *Religion*	2
4	**Safety**: *May be used illicitly by others/ Biometric technology is vulnerable to cyberattacks.*	2
5	*I don't answer.*	1
6	*I don't know*	1

Table 1 the number of respondents who do not want identification documents to contain biometric indicators (authors own conception – statistical analysis)

Retaining fingerprints and biological samples is generally more controversial than taking such bioinformation. Given the information that could be revealed, keeping biological samples in databases raises greater ethical concerns than digitized fingerprints. Thus, in case of mandatory biometric data entry in identity documents, 16.92% (22 answers) of respondents consider that their fundamental rights are violated. The share of those who consider that their fundamental rights are violated is higher among respondents in rural areas (26.31%), compared to those in urban areas of 15.31%. Depending on the age category, the highest rate of respondents who consider that their fundamental rights may be violated in case of mandatory biometric data is in the category of 50-59 years old (33.33%), followed by people aged 60-69 years (20%).

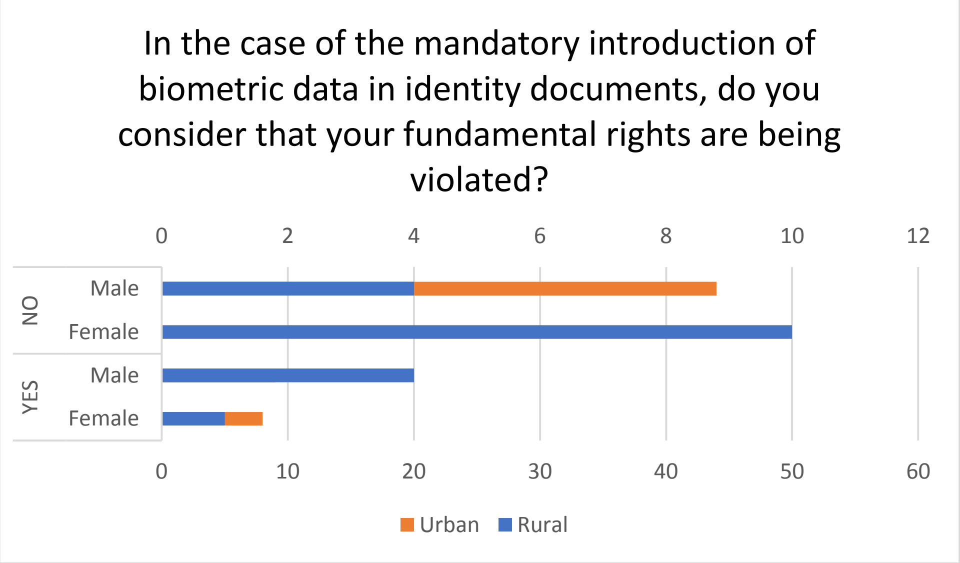

Figure 8 Opinions regarding the fundamental rights (autors own conception – statistical analysis)

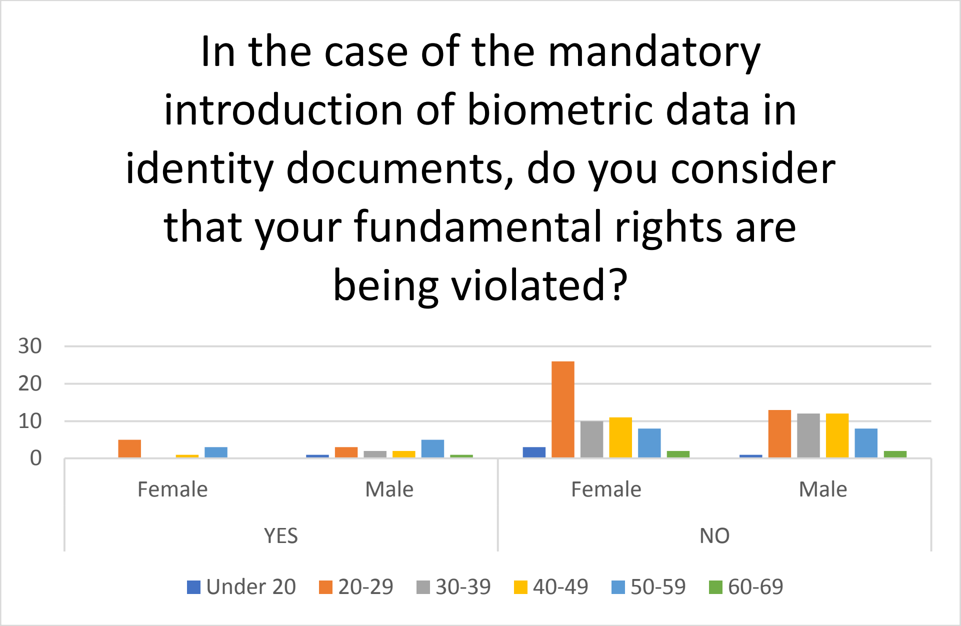

Figure 9 Opinions regarding the fundamentals right 2 (authors own conception – statistical analysis)

Of the 22 people who consider that their rights are violated in case of mandatory biometric data, 36% consider that their right to a private life is restricted and 27% their right to confidentiality is violated.

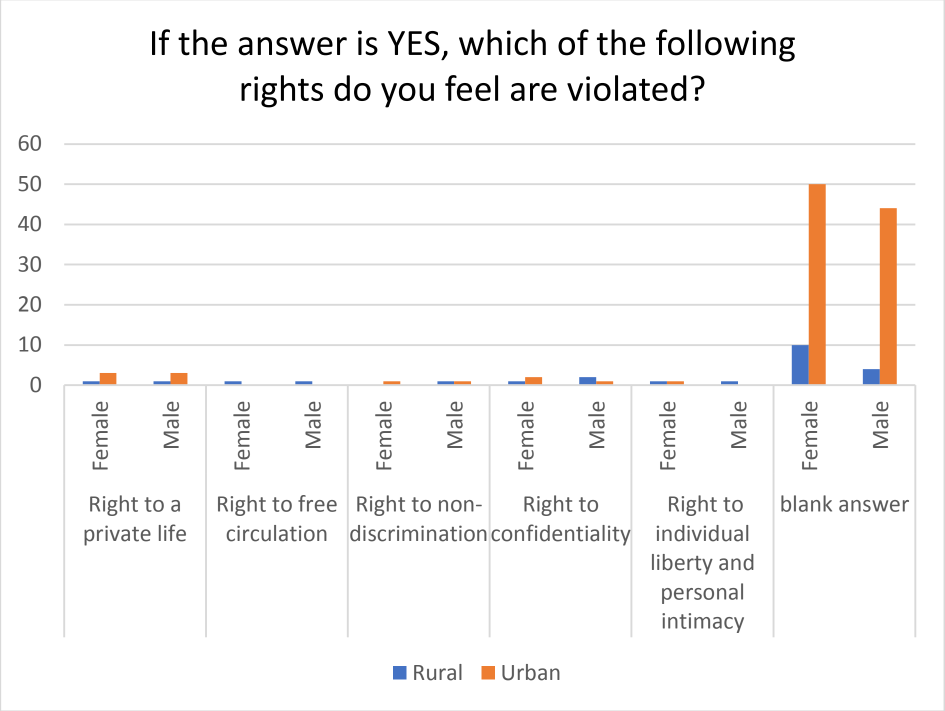

Figure 10 The types of fundamental rights with potential to be violated during the biometric identification (authors own conception – statistical analysis)

Out of the total number of respondents, the majority (82%) consider that Romania does not yet have a system that could guarantee the safety of biometric data included in the database. Taking into account the open answer questions (e.g. question number 8), some individuals believe that biometric technology is increasingly subjected to cyberattacks. In order to prevent unpleasant consequences in case of identity theft (given that biometric indicators are unique to each individual), high safety measures are needed. The percentage of those who consider that Romania does not yet have a system capable of security of biometric indicators included in the database is high both in rural areas (89.47%) and urban areas (80.18%), regardless of gender and age category. It is found that among people aged 50 to 59 it even reaches 91.66%.

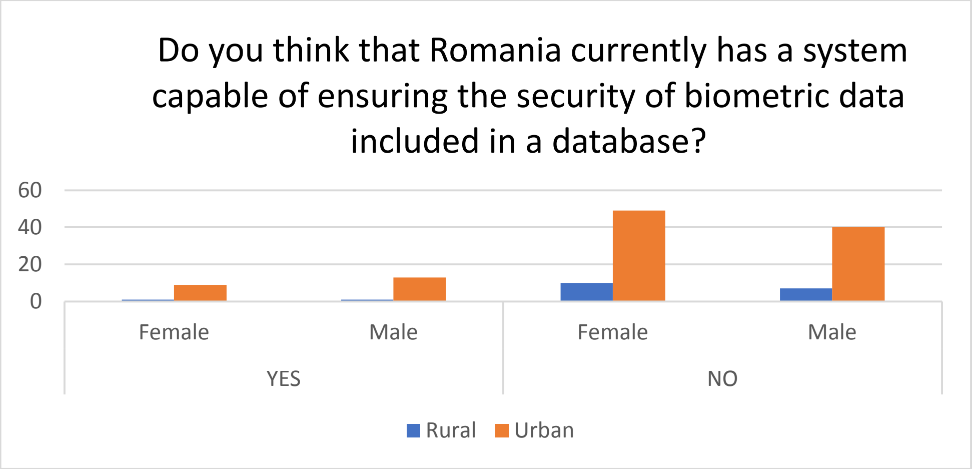

Figure 11 Quantitative analysis regarding the possibility of Romania to ensure the security of biometric data (authors own conception – statistical analysis)

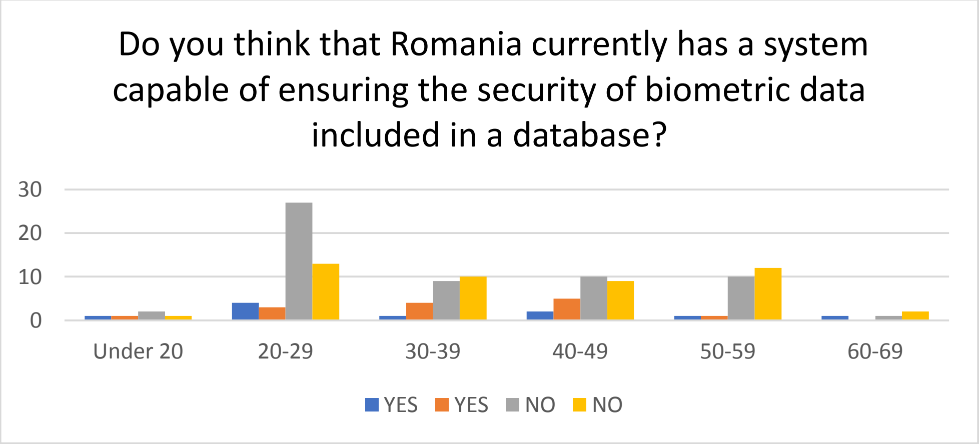

Figure 12 Quantitative analysis regarding the possibility of Romania to ensure the security of biometric data (authors own conception – statistical analysis)2

The retention of biological samples requires the highest standards of operation in terms of data responsibility and security, as the potential uses and abuses of databases are considerable.

The questionnaire also focused on finding out from the population which indicator they consider could violate one or more fundamental rights. Thus, an open question was made regarding this subpoint, this question having a lower number of respondents than the total number involved in the study. Of these, over 20% believe that no biometric indicator could violate fundamental human rights as long as they are used within a well-defined legal framework and then stored securely in a database. Equally, respondents consider DNA evidence and facial image indicators that give them insecurity, with some individuals claiming that the facial image may violate their right to privacy (mass surveillance). Of the respondents, only 5% consider that all indicators would violate the rights of individuals who refuse digitalization (right to prohibit discrimination, right to free movement). Moreover, there are opinions about the invasive, aggressive and intrusive nature of these technologies that would go beyond the purpose for which they are used (for example, according to some studies, fingerprints can reveal data on a person's ethnic origin).

Analyzing the above, and the specialized literature, we find that the impact of ethical issues depends especially on the concrete purpose of identification, on the biometric methods used (invasive or non-invasive, high or low precision) as well as on their ability to be reproducible / easy to falsify, the consequences (arrest for example) triggered by a high probability score / match, the security of biometric data included in the database, as well as concerns associated with modern large-scale surveillance (respect for fundamental rights).

The rapid evolution of biometric technology has allowed its wide use in commercial, governmental, medical applications, becoming a method of identification known to the general public. It is considered that in order to increase citizens' safety, the contribution of each person with biometric features in the implementation of such a national database is important. But, at the same time, it should be mentioned that new laws and systems capable of ensuring the security of biometric data included in the event of the development of such a database must be introduced and applied.

Schomberg (2007) provided an overview of ethical issues related especially to new technologies, adapted today to the issues surrounding the use of biometrics. His works include: respect for fundamental principles (EU Charter of Human Rights and national constitutions) and secondary rights (access to information, data protection); issues of human dignity and the surveillance society; data status (identification of medical conditions not foreseen and consented); non-discrimination, social exclusion, and equity (Jain et al. 2008).

The process of biometric identification involves several characteristic steps, each of which raising specific ethical concerns. The first step is the development of technology which includes processing of biometric data, evidence the use of which must be justified both legally and ethically. Due to the extreme sensitivity of biometric identification systems, particular attention is needed against any potentially discriminatory effects. The critical stage in biometric identification is the enrollment phase, i.e. creating biometric templates by collecting information, extracting specific features from the data collected, assembling the data into a template and storing it in a reference database. Once the system is up and running, the next step is to collect and process templates, specifically biometric input data taken from persons to be identified. This information requires specific processing, including the extraction of particular characteristics. Next comes comparing templates with stored ones and calculating a match score that will trigger different attitudes. Depending on what kind of reactions are triggered (severity, reversibility, possibility of being challenged), several ethical issues may surface, generally associated with the decision-making process (Buolamwini, 2017; Cooper et al. 2019).

Thus, the main ethical issue in the case of biometric identification is related to the enrollment stage, namely the creation and storing of unique templates. Since traits that individually identify a particular person belong to one's own body, the process of collection and usage interferes with human autonomy and dignity. Once such a template is created and stored in a reference database, anyone can get hold of it.

The stored template can be used to identify the person for an indefinite range of purposes and in various situations. The aspect which makes the possession of biometric templates so influential and potentially risky from the perspective of human fundamental rights is that individuals, all throughout their lifetime, will not be able to modify their biometric characteristics. Other people's use of biometric characteristics for the purpose of identification is seen as a contradiction of Immanuel Kant's fundamental principle that "*humans should be treated as ends in themselves, never merely as a means.*" (Alterman, 2003*)*

Given that biometric templates digitize the human body, there have been concerns that the process of collecting biometric identifiers not only interferes with the privacy and right to protection of a personal data, but also with the integrity of an individual's body. Therefore, it has been paralleled to body searches or other measures that interfere with a person's physical integrity. According to this interpretation, the *digitized body* created throughout biometric templates could be searched remotely and indeterminately without the 'owner' ever knowing (; Wendehorst et al. 2021).

First-generation biometrics makes it easy to create profiles by providing deep insights into a person's privacy. Behavioral detection techniques amplify this ethical problem because individuals' profiles could be augmented with information about their intentions. In addition, they may disclose information about personal health problems and disabilities that were not previously known. This often rises an ethical problem because, on the one hand, the affected person has the right to receive complete information about the result of biometric detection, but, on the other hand, informing the individual about a particular condition without their consent interferes with the right not to know (Sanchez-Monedero & Dencik, 2020).

Conclusions

Due to the need of increased accuracy, biometric technologies are combined into multimodal systems. They use multiple biometric identifiers to identify a person. Biometric systems can minimize the risk of fraud and assist in overcoming the difficulties caused by poor quality or missing data, but they also raise ethical concerns as they allow for greater supervisory efficiency and can be used for profiling.

In conclusion, the creation and storage of a unique biometric template must be considered in the context of the specific purpose of this process: the protection of all citizens from any and all criminal activities, as a primary obligation of every state. However, this obligation must be exercised with due respect for the fundamental ethical values and in the light of modern human rights law.

References

Buolamwini, J. A. (2017). *Gender shades: intersectional phenotypic and demographic evaluation of face datasets and gender classifiers* (Doctoral dissertation, Massachusetts Institute of Technology).

Alterman A. (2003). A piece of yourself: Ethical issues in biometric identification. *Ethics and Information Technology* pp. 139.

Ashbourn J. (2000). *Biometrics: Advanced identity verification: The complete guide*. Springer-Verlag, London, pp. 1-13

Belhadj F. (2017). *Biometric system for identification and authentication. Computer vision and pattern recognition*. Ecole nationale Supérieure en Informatique Alger, English. pp. 5-8, 14-18, 20-28, 85.

Cooper, I., & Yon, J. (2019). Ethical issues in biometrics. *Sci Insigt*, *30*(2), 63-69.

Jain A.K., Flynn P., Ross A.A. (2008). *Handbook of biometrics*. Springer Science & Business Media, pp. 1-4, 15-17.

Sánchez-Monedero, J., & Dencik, L. (2022). The politics of deceptive borders:'biomarkers of deceit'and the case of iBorderCtrl. *Information, Communication & Society*, *25*(3), 413-430

Ramalingam S., Shenoy A., Viet N.T. (2018). Fundamentals and advances in 3D face recognition In Mohammad S. Obaidat, Issa Traore and Isaac Woungang (eds), *Biometric-Based Physical and Cybersecurity Systems,* pp. 125-135.

Von Schomberg, R. (2007). From the ethics of technology towards an ethics of knowledge policy & knowledge assessment. *Available at SSRN 2436380.*

Smith M., Mann M., Urbas G. (2018). *Biometrics, crime and security*. London, Routledge, pp. 55-64.

Sohnemann N., Uffrecht L.M, Hartkopf M.C.,Kruse J.P., Noellen L.M. (2020). *New developments in digital services, Short-(2021), Medium-(2025) and Long-Term (2030) perspectives and the implications for the digital services*. European Asylum Support Office. Malta https://policycommons.net/artifacts/2055435/new-developments-in-digital-services/2808526/

van der Ploeg I.: Genetics, biometrics and the informatization of the body. Ann Ist Super Sanita. 2007;43(1):44-50. PMID: 17536153

Wendehorst C., Duller Y. (2021). *Biometric recognition and behavioural detection, policy department for citizens rights and constitutional affairs*. European Parliament, European Union, pp. 13-20, 28-29, 38-42 , 45-50, 58-59.