Journal of Ethics and Legal Technologies – Volume 6(2) – December 2024

Biometric Data and Artificial Intelligence: EU Standards and Solutions in Bosnia and Herzegovina

Brano Hadži Stević

University of East Sarajevo, Faculty of Law

Thanks to the development of modern technologies, we could claim that personal data are at on a daily basis exposed to risk. There are different types of personal data, but this paper is devoted to biometric data that belongs to the category of particularly sensitive data. Some biometric data are unique, and their use leads to identification and verification. But the use of artificial intelligence can produce different consequences regarding personal data, including biometric data. This paper tends to determine the main concepts regarding biometric data and artificial intelligence in order to determine the European standards on automatic processing of biometric data, particularly those contained in EU regulations regarding personal data and artificial intelligence. The last part of this paper deals with the Bosnia and Herzegovina regulations regarding biometric data protection.

Keywords: personal data, biometric data, artificial intelligence, European standards, Bosnia and Herzegovina.

Introduction

Every person has some unique characteristics that could be used for the purpose of identification. It is not rare today that some of these characteristics are used in order to properly identify someone in order to, e.g., check if an individual is in criminal records, to open a bank safe, etc. Shortly, the main objective is to determine someone's identity without doubt and approve or disapprove the access. We speak about fingerprints, facial recognition, voiceprints, iris scan, etc. These specific characteristics, i.e., personal information that can be used in order to uniquely identify an individual are biometric data.[1] Other ways of authorization, such as PIN codes, are being used simultaneously or even becoming part of history.[2]

But the use of biometric data is not undisputable since, at least, two questions arise: (1) who processes these data (a man or artificial intelligence?) and (2) whether privacy is protected in order to avoid potential abuses of data? This paper tends to analyze a number of questions about the connection between the biometric data and artificial intelligence (hereinafter: AI). The first part is devoted to the biometric data in order to determine the main concepts and analyze the connection between personal data and biometric data. The second part is devoted to the AI issues, i.e., the main concepts regarding AI will be presented and the processing of biometric data will be analyzed. Extraordinary importance in this paper belongs to European Union (hereinafter: EU) legal acts regarding personal data and AI. The first one is the EU General Data Protection Regulation (hereinafter: EU GDPR), while the second one is the European Union's Artificial Intelligence Act - Regulation (EU) 2024/1689 (hereinafter: EU AIR). The third part of this paper is devoted to the Bosnia and Herzegovina personal and, especially, biometric data regulations and their compliance with the EU standards.

Biometric data

The main concepts

The biometric refers to "the measurement and statistical analysis of people's unique[3] behavioral and biological (anatomical and physiological)

[1] "Any information that defines or helps identify an individual can be considered biometric data", i.e., "biometric data derives from an individual's existence" (Kim, 2023, 190, 202).

[2] See also: *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Technische_Grundlagen_pdf.pdf?__blob=publicationFile&v=1* (last visited on 25 August 2024).

[3] Some authors challenged the uniqueness as a characteristic of biometric data since

characteristics or traits".[4] The biometric data are a type of personal data[5] that result from "specific technical processing" related to "the physical, physiological or behavioural characteristics" of an individual, and these data "allow or confirm" the unique identification of that individual.[6] Biometric data today includes physical characteristics[7] like the shape and size of the earlobes, as well as the way a person breathes and walks. According to experts, in the future, it may also be possible to identify the way a person types on a keyboard or writes their name, and the AI will enable to identify an individual using that person's speech and gestures.[8]

But what is the main advantage of identification using biometric[9] data compared to other types of identification or access control, such as PIN codes or passports?[10] The answer lies in the uniqueness of biometric data that causes reliability, i.e., the PIN code for an ATM card can be guessed or a passport can be falsified, while those problems do not exist regarding biometric data. In other words, the biometric data allows to determine who an individual is, while other types of identification rest on the fact that you possess something (a passport, a PIN code, etc.).[11]

Biometric data can allow for the authentication, identification, or categorization of natural persons and for the recognition of emotions of natural persons (Recital 14 of EU AIR). Article 3(35-36) of the EU AIR defines

mistakes are possible. See: Jasserand, 2016, 306 and Yue Liu, 2012, 34. Compare with the ECJ decision in case C-291/12, para. 43.

[4] See: *https://www.innovatrics.com/glossary/biometrics/* (last visited on 15 September 2024). and Yue Liu, 2012, 29. Also see: Gaba, Estremadura, 2020, 959-960.

[5] The right to personal data is guaranteed by the EU Charter of Fundamental Rights (Article 8).

[6] See: Article 5(14) of the EU GDPR and Article 3(34) of the EU AIR. On the concept of biometric data and their dual nature, see Jasserand, 2016, 301.

[7] We could claim that something is a biometric characteristic if the following requirements are fulfilled: universality, distinctiveness, permanence, and collectability (*https://www.innovatrics.com/glossary/biometrics/*). See also: Yue Liu, 2012, 30.

[8] Those ways of identification are not only possibilities since there are some examples like arresting a man in Dubai who had used fake credit cards, thanks to checking the shape of his ears or arresting a man (who was disguised as a woman) thanks to the way he walked and his body measurements. See: *https://www.dw.com/de/nahost-digitale-identifizierung-nutzt-repressiven-regimes/a-66615121* (last visited on 18 September 2024).

[9] Biometrics is "an 'automatic recognition method' based on biometric characteristics", while the biometric data "covers the technical transformation of biometric characteristics into formats that can be used for biometric recognition." See: Jasserand, 2016, 301.

[10] Some payment processing companies are using biometrics to verify a cardholder's identity in order to simplify online shopping. Furthermore, the MasterCard stresses that "existing identity verification methods… can result in a shopper abandoning their purchase" or in transaction declination due to an incorrect password. See: *https://mastercardbelgium.prezly.com/mastercard-makes-fingerprint-and-selfie-payment-technology-a-reality* (last visited on 1 September 2024).

[11] See: *https://www.innovatrics.com/glossary/biometrics/*.

biometric identification and biometric verification.[12] While identification serves for comparing (one-to-many) biometric data with records stored in a database (e.g., comparing with all individuals from the database who have a passport), verification is a one-to-one method for identification of an individual by comparing his/her biometric data with previously provided biometric data, i.e., the biometric verification is used for determination of the trueness of an individual's claim (e.g., I am XY who has a visa to enter the USA).[13] In this case there is comparison[14] between a biometric sample of a person with biometric information contained in a passport, credit card, etc.[15]

The EU AIR (Recital 15) prescribes that biometric identification present "automated recognition of physical, physiological and behavioural human features" like "face, eye movement, body shape, voice, prosody, gait, posture, heart rate, blood pressure, odour, keystrokes characteristics" in order to establish an individual's identity by the above-mentioned comparison, regardless of his/her consent.[16] Also, Recital 15 of excludes "AI systems intended to be used for biometric verification, which includes authentication, whose sole purpose is to confirm that a specific natural person is the person he or she claims to be and to confirm the identity of a natural person for the sole purpose of having access to a service, unlocking a device or having security access to premises". Finally, according to Article 3(40) and Recital 16 of the EU AIR, biometric categorization refers to "assigning natural persons to specific categories on the basis of their biometric data" (e.g., age, tattoos, behavioural or personality traits).

The connection between personal data and biometric data

According to Article 9 of the EU GDPR, the processing of biometric data "for the purpose of uniquely identifying a natural person" is in abstracto

[12] On the difference between authentication and verification, see Jasserand, 2016, 304, and Yue Liu, 2012, 31-32. On the fact that legal documents do not take into account precise biometric terminology, see Jasserand, 2016, 305, and Sumer, 2022, 2.

[13] "Authentication is when you prove that you are who you say you are", while "identification is when you prove that someone else is who they say they are" (*https://www.innovatrics.com/glossary/biometric-data/*). See also: *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Technische_Grundlagen_pdf.pdf?__blob=publicationFile&v=1.*

[14] Biometric verification is "the process of conforming a biometric claim through comparison" (Sumer, 2024, 153).

[15] The biometric information is stored only in a database (in the case of an identification system) or in a database, in a portable medium, or both. See: Yue Liu, 2012, 32.

[16] Some authors claim that the verification/identification difference is not clear, especially because the verification is "a cooperative process" in which the data subject knowingly registers to a biometric system, and this is not the case regarding identification (Sumer, 2024, 154-155).

prohibited, i.e., exceptionally allowed under prescribed requirements, such as the data subject's explicit consent, the necessity of processing for specific purposes and for protecting vital interests, etc. We will not analyze those conditions, but some aspects of biometric systems and biometric data as a type of personal data.

The biometric systems rest on four steps: (1) data acquisition and enrolment of biometric characteristics in database (biometric sample), (2) relevant biometric data extraction into symbols (numbers, labels, etc.), (3) biometric reference (template) creation and (4) comparison of biometric sample with previously saved template. It is necessary to analyze the biometric data through the lens of the definition and characteristics of personal data. The EU GDPR prescribes that biometric data are: (1) personal data that are (2) result of specific technical processing, (3) related to the physical, physiological, or behavioural characteristics of an individual (4) that allow or confirm the unique identification of that individual. Hence, the first step refers to the data collection of an individual; in the second step data are recorded, analyzed, and organized; the third step refers to storing; and the final step implies data usage (compare with Article 4(1-2) of EU GDPR). The European Court of Justice, as well as the European Court of Human Rights, ruled that biometric data, i.e., in concreto fingerprints, are personal data since "they objectively contain unique information about individuals that allows those individuals to be identified with precision".

Biometric characteristics are not eo ipso biometric data, i.e., only those personal data that are result of processing of biometric characteristics could be named as biometric data. Someone's iris or fingerprint is not eo ipso his/her biometric data, but the data generated from them and stored in a database present biometric data. Hence, contrary to the other types of personal data that belong to the category of sensitive data, "biometric data are not treated as sensitive by nature but become sensitive as the result of their use". If signature (as a type of biometric characteristic) allows or confirms the unique identification of an individual, the signature is biometric data. Vice versa, if identification of an individual on the basis of that signature is not possible, the signature is not biometric data. The biometric characteristics are the subject of processing, and the result of that processing are personal data, i.e., a special and sensitive type of personal data - biometric data. The EU GDPR in article 9(1) contains the prohibition of processing of biometric data and other so-called special categories of personal data, but line 2 of this article permits the processing under a number of requirements, such as explicit consent and necessity.

Artificial intelligence and biometrics

The main concepts regarding AI

The term AI covers a wide range of digital technologies and can refer to the faster processing of large amounts of digital data[17] for analysis as well as so-called "generative AI," which "generates" new text or visuals based on huge amounts of data.[18] AI seeks to emulate the human way of thinking regarding a large amount of data in order to use those data for purposes useful for humans. Therefore, AI strives to apply cognitive process,[19] to learn, analyze, and perform tasks instead of man in a faster, i.e., more efficient way. According to Article 3 of the EU AIR, AI system refers to "a machine-based system" that "may exhibit adaptiveness after deployment" and, based on the inputs, generates "outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments".[20]

It is indisputable that the AI technologies can lead to impressive results and impressed individuals. Furthermore, today it is very popular "to play" with AI and advertise AI in order to achieve different goals. For example, some companies "exaggerate the amount of AI technology they use in their products". This phenomenon is called AI washing.[21] In 2023, the Coca-Cola launched the Y3000 drink as a new flavor of cola, claiming that it was "co-created" by AI.[22] An example of a positive use of AI is Polisi's (privacy policy analysis)[23] is a machine learning tool that uses AI for reading and analyzing privacy policies in order to provide a readable summary and graphic flow chart regarding questions such as what kind of data are collected and where they will be sent. This AI tool provides results in about 30 seconds. Probably the best proof of the utility of this AI tool is the fact that only 0.7% of users click on a terms of service link before they click the "agree" button. Using Polisi's, they have the possibility to help themselves with just one click in a half of a minute.[24]

[17] The term "big data" is often used. On the meaning of big data, see: EPRS, "The impact of the General Data Protection Regulation (GDPR) on artificial intelligence", 4.

[18] See: *https://www.dw.com/en/how-extremist-groups-like-islamic-state-are-using-ai/a-69609398*. In order to achieve AI's full potential and prevent errors, "more data is better than less, and there is almost never enough" (CIPL Report, 2018, 25). Hence, "AI has become hungry for data" (EPRS, 16).

[19] See also: CIPL Report, 2018, 5.

[20] See also: Danks, 2014, 151-165.

[21] See: *https://www.techtarget.com/whatis/feature/AI-washing-explained-Everything-you-need-to-know*.

[22] See: *https://www.dw.com/en/ai-washing-what-is-it-and-why-you-should-worry/a-69731038.*

[23] See: Harkous *et al.*, 2018, 531-545.

[24] See: *https://www.wired.com/story/polisis-ai-reads-privacy-policies-so-you-dont-have-to/.*

An important term regarding AI is machine learning, i.e., the capability of a machine to imitate a human's reasoning, to learn and create new algorithms from existing data without being explicitly programmed.[25] A type of machine learning is so-called deep learning, and it processes data in such a way that corresponds to the human brain. Deep learning simulates the decision-making power of the human brain using artificial neural networks in order to reach a conclusion from data.[26] The extraordinary important technology known as computer vision is the consequence of deep learning. The computer vision enables that machines can equally or better than human eyes recognize visual objects, such as images, and compare them with patterns in order to make a decision (for example, unlocking a smartphone using facial recognition). The widespread use of biometrics today is primarily based on "substantial performance improvements due to the use of connectionist artificial intelligence (AI) methods, in particular, deep neural networks (DNNs)".[27]

Although the possibilities of AI are enormous, impressive, and applicable in a number of different areas, there are a number of problems regarding AI. It must not be ignored that AI must be under humans' control, but not vice versa.[28] A man should learn AI to learn itself, but in such a way that will keep AI under control. A serious breach of human rights is possible whenever AI is used for personal data processing, since the presumption for AI functioning is processing of personal data, such as name, photos, location, etc. Sometimes it is necessary to choose between AI benefits and preservation of our privacy. An important place for achieving proportionality between those goals is the existence of legal regulations, such as the EU GDPR[29] and the EU AIR.[30]

The AI processing of biometric data

There are tensions between AI (that demands a huge amount of data) and the EU GDPR (that demands the minimization of data)[31] and it is clear that

[25] "AI is a reality that transforms "our world, our society and our industry" like "the stream engine or electricity in the past" (CIPL Report, 2018, 6-7). Not only AI is "gradually becoming omnipresent", but the likelihood that AI systems will become omnipotent is also growing (Milinković, 2021, 30).

[26] Hence, deep learning is „at the heart of many AI applications", such as voice recognition technologies. See: CIPL Report, 2018, 7. On the connection between neural networks and AI, see: EPRS, 13.

[27] Berghoff, Neu, Von Twickel, 2021, 80.

[28] On this issue, see also: Milinković, 2021, 31 and Article 14 of the EU AIR.

[29] Some authors claim that the EU GDPR is not a "ground-breaking instrument for 21st century protection of rights" (Davies, 2016, 290).

[30] It's hard not to talk about the GDPR when discussing AI policies because the GDPR has had "the most impact on any law globally in terms of creating a more regulated data market", while data represent "the key ingredient for AI application" (Gáti, 2022, 594).

[31] On this issue, see EPRS, 45-46, 76-79.

AI can cause “a complete loss of control of personal information”.[32] According to Article 6(2) and Annex III of the EU AIR, the AI systems related to the biometrics (if their use is permitted under relevant Union or national law) are high-risk AI systems if they are used for: (1) remote biometric identification systems, excluding AI systems used for biometric verification with sole purpose of confirming that “a specific natural person is the person he or she claims to be”; (2) AI systems intended to be used for biometric categorization; (3) AI systems intended to be used for emotion recognition.

Article 14 of the EU AIR prescribes that “high-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which they are in use” in order to “to prevent or minimise the risks to health, safety or fundamental rights that may emerge”. Human oversight measures refer to guarantees that “the system is subject to in-built operational constraints that cannot be overridden by the system itself and is responsive to the human operator” (Recital 73). In compliance with Article 14 and in connection with Annex III of the EU AIR, in the case of remote biometric identification systems, the identification made by the AI system must be confirmed by at least two natural persons. Those persons must possess “the necessary competence, training, and authority to carry out that role” (Recital 73 of the EU AIR).

The main role in (biometric) identification has AI[33] and whenever we talk about it, there is danger that private data will be abused since personal data has become “the food” or “the oxygen” for AI.[34] More precisely, AI is used to “compare newly captured biometric data against previously stored reference data,” and then AI “takes decisions about whether the reference data and newly captured information belong to the same person”.[35] But the prob-

[32] Chałubińska-Jentkiewicz, Nowikowska, 2022, 187-188.

[33] The biometric has become “the most trusted and most widely adopted tool for personal identification” (*https://www.innovatrics.com/glossary/biometrics/*).

[34] Chałubińska-Jentkiewicz, Nowikowska, 2022, 184, and CIPL Report, 2018, 25. “In the process of feeding data to machines or devices”, individuals “unwittingly surrender to networks, giving these networks access to a human’s body, including the bodies’ genomes and minds” (Gaba, Estremadura, 2020, 970). See also: CIPL Report, 2018, 5.

[35] *https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Biometrie/biometrie_node.html* (last visited on 18 September 2024).

lem raises when the AI becomes not only a helpful tool but an attack tool.[36] Hence, the AI is a double-edged sword.[37]

A paradigmatic example of AI misuse regarding biometric data is morphing, which rests on manipulation of stored biometric data and merging the facial images of a number of people together so that the final image contains features of all of them. During the biometric procedure, the face of any of these individuals will be considered as a match for the reference data falsified by morphing.[38] Also, AI is a useful tool for companies since it enables them to collect "a customer's purchasing pattern and tendencies and other behavioral patterns," enabling improvement of efficiency in marketing, distribution, and development. This phenomenon could be named as the commercialization of biometric data using AI.[39]

AI has been of extraordinary importance for "increasing the performance of biometric systems to levels unseen with previous technology".[40] Thanks to the use of cameras, advanced algorithms, and artificial intelligence,[41] the authorities of various countries can now reconstruct to the smallest detail where someone moves and what he/she does. Or even follow it live. The example is the World Cup in Qatar (2024), where the authorities used remote biometric identification techniques and 15,000 cameras with facial recognition technology.[42] Similarly, Saudi Arabia takes "measures to enable swift and irrefutable proof of identity" using biometric characteristics.[43]

The connection between AI and biometric data[44] is extremely complex.[45] The reason for this claim lies in the fact that AI is the object of attacks as

[36] Although biometric AI systems have impressive results, "they exhibit a range of vulnerabilities - many of which can themselves be exploited with the use of AI". Paradoxically, the mitigation of these vulnerabilities is possible, *inter alia*, using AI methods. See: Berghoff, Neu, Von Twickel, 2021, 80-85.

[37] On the question of advantages of AI over human decision-making (e.g., preciseness and impartiality) and potential disadvantages related to mistakes, see: EPRS, 20. AI methods "are not perfect, but they are promising" (Chałubińska-Jentkiewicz, Nowikowska, 2022, 190).

[38] *https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Biometrie/biometrie_node.html.*

[39] See Gaba, Estremadura, 2020, 973-974. On this issue, see also: Kim, 2023, 191-192, and Sumer, 2022, 1. Compare with Article 5(1a) of the EU AIR.

[40] Berghoff, Neu, Von Twickel, 2021, 84.

[41] Today is AI "so reliable that it does not need people". See: Chałubińska-Jentkiewicz, Nowikowska, 2022, 184. See also: Gaba, Estremadura, 2020, 976.

[42] See: *https://www.biometricupdate.com/202208/qatar-equips-15000-cameras-with-facial-recognition-for-soccer-world-cup-2022* (last visited on 18 September 2024).

[43] See: *https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/biometric-borders-saudi-arabia* (last visited on 18 September 2024).

[44] This widespread use of biometrics is primarily based on "substantial performance improvements due to the use of connectionist artificial intelligence (AI) methods, in particular, deep neural networks (DNNs)".

[45] Some authors claim that AI can conduct simultaneously a great amount of our data on

well as the instrument on attack to (biometric) data. Hence, it is necessary to distinguish attacks on AI and attacks using AI, i.e., the AI could be used as "a new target and as a new tool for attackers".[46]

Since the assumptions for AI work are a great amount of data,[47] the attacks on AI[48] imply that a large number of false and malicious data are inserted in a database in order to be classified as legitimate. For example, false biometric samples are inserted in database[49] and presented as biometric data of another person. In such cases, there is so-called stolen identity, since A is presented as B. In future data processing, the person A can use, e.g., the name and (biometric) data of person B, get a passport, and travel worldwide committing crimes since the AI recognizes the biometric data of A as valid.[50]

Although B, for example, lives in Milano and has no idea that he has a passport, "he," i.e., A who presents himself as B travels worldwide using the passport issued on B's name. It is not a rarity that B in such cases finds out about this only when the person who stole his identity commits a crime.[51] A serious consequences are possible before B proves he is not guilty, but the malicious biometric samples were detonators. And when "an AI model is trained using these samples," an attacker will be impersonated as another individual.[52] Also, sometimes it is claimed that "AI is… very easy to deceive at the moment". For example, "a computer vision system can confuse a stop sign with a speed limit sign if a piece of tape is attached to it".[53]

On the other side, there are attacks using AI.[54] Fake inputs, which are produced by altering real biometric data using AI, have the potential to deceive

the web and "AI successfully steals data, while it seems that we are talking to a human" (Chałubińska-Jentkiewicz, Nowikowska, 2022, 184).

[46] Berghoff, Neu, Von Twickel, 2021, 81-82, 84.

[47] On new challenges and threats regarding "AI systems focused on permanent self-development", see Chałubińska-Jentkiewicz, Nowikowska, 2022, 183-184.

[48] Adversarial machine learning is devoted to the study of the attacks on machine learning algorithms and of the defenses against such attacks. See: Biggio *et al.*, 2015, 32.

[49] There is also the possibility to replace a template or to delete a genuine user's biometric template in order to cause a denial of service. See: Biggio *et al.*, 2015, 34-35.

[50] "Biometric recognition systems operate either in enrollment or in recognition mode". See: *Ibidem*, 33.

[51] In some cases, the use of AI for analyzing the biometric characteristic (*in concreto* iris) resulted in arresting the person. Furthermore, *in concreto* it is unknown how the biometric data of the arrested man are obtained. See: *https://www.dw.com/de/nahost-digitale-identifizierung-nutzt-repressiven-regimes/a-66615121*).

[52] Berghoff, Neu, Von Twickel, 2021, 82. "By training a model on inaccurate or intentionally falsified data, it is possible to negatively impact its future performance." - *https://datascientest.com/en/adversarial-attack-definition-and-protection-against-this-threat* (last visited on 19 September 2024).

[53] *Ibidem.*

[54] Trustworthiness is a prerequisite for the uptake of digital technologies, and the best way to build trust regarding AI is creating "clear regulations protecting personal data"

biometric systems. There are a number of ways for this. For example, AI-based voice-generation tools can deceive speaker-verification systems. Similarly, face-swapping techniques are instruments for creating the fake videos by seamlessly replacing the attacker's face with the victim's face. Hence, the viewer of a video has the impression that he is listening to a famous sportsman or politician,[55] although the attacker made a false video using AI and biometric characteristics of a sportsman or politician.[56]

Also, morphing attacks rest on the use of AI, and the facial images of different people can be fused together, resulting in a new image that has characteristics of all source faces. A serious consequence of the morphing attack is the fact that the degree of similarity is enough for verification since "the facial-recognition systems are designed to be robust against natural variances in human faces".[57] Since this paper deals with the biometric data, the consequence of the morphing attack may be the inserting of a morphed image into a passport, and a number of individuals can use the same passport because the biometric data of all of them are built into the verification system, which is enough for passing passport controllers.

The protection of biometric data in Bosnia and Herzegovina

Legal framework on data protection

According to the Constitution of Bosnia and Herzegovina (BiH), Bosnia and Herzegovina and both entities shall ensure the highest level of internationally recognized human rights and freedoms (Article II 2). Furthermore, rights and freedoms from the European Convention on Human Rights have priority over all other laws. Since the right to data protection is doubtless one of the most important rights in international acts, we could claim that BiH has a *constitutional obligation* to ensure private data protection. Also, BiH ratified Convention 108 (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data) and Convention 108+.

(Chałubińska-Jentkiewicz, Nowikowska, 2022, 184-185) and their applying.

[55] Those ways of AI misuse demand a sufficient amount of data of the victim of an attack, and in the case of persons of public interest, such data are publicly available. But it is notable the "reducing the amount of training data required of a victim" since "creating realistic fakes has become much easier", even in real-time. See: Berghoff, Neu, Von Twickel, 2021, 82.

[56] On voice recognition and face recognition as biometric characteristics, see: Alharbi, Alshanbari, 2023, 7-13.

[57] So-called adaptive biometric systems are used to "enable an update of the stored templates automatically during verification" in order to "account for natural changes of biometric traits over time (i.e., biometric aging)", such as template self-update. See: Biggio *et al.*, 2015, 34.

According to the Stabilization and Association Agreement between BIH and EU,[58] BiH accepted obligations to: (1) *harmonize* its legislation related to the protection of personal data with Community law and other European and international legislation on privacy and (2) establish independent supervisory bodies with sufficient financial and human resources in order to effectively monitor and guarantee the implementation of national legislation on the protection of personal data. Hence, BiH also has an international obligation to ensure personal data protection.

The obligation to protect personal data steams not only from international law but also from domestic law. The BiH personal data protection law consists of a number of statutes and some bylaw legal acts. In order to evaluate personal data protection in any country, it is not enough to conclude whether some regulations exist, but to analyze the *quality* of domestic regulations. The highest standards of quality are set by EU and Council of Europe legal acts. Regarding biometric data and AI, the most important legal acts are the EU GDPR and the EU AIR.

The most important statutory law act in Bosnia and Herzegovina regarding protection of personal data is the Law on the Protection of Personal Data (LPPD). Besides, the BiH personal data protection law regarding biometric data consists of a number of statutes and bylaws, such as The Law on Travel Documents of Bosnia and Herzegovina,[59] The Law on Foreigners,[60] The Rulebook on the Registration of Biometric Characteristics of Foreigners, and Rulebook on the Content and Method of Keeping Records. Relevant provisions of those acts will be mentioned in the following lines.

Before we focus on domestic data protection law, we will mention an agency. An important *institution* regarding personal data protection in Bosnia and Herzegovina is the Personal Data Protection Agency. A recent example speaks in favor of this claim. During August 2024, Agency issued a Press release regarding Meta Inc. and warned citizens of BiH "to be careful when publishing personal data" on social networks controlled by Meta. This company changed the privacy policy for its users without notifying users in Bosnia and Herzegovina, as well as some countries in the region that are *not* members of the European Union. The changes regarding private policy refer to "the processing and use of all user data (personal data, photos, videos,

[58] See Agreement on: *http://www.mvteo.gov.ba/attachments/bs_sporazum-o-stabilizaciji-i-pridruzivanju-izme%C4%91u-evropskih-zajednica-i-njihovih-drzava-clanica-i-bih.pdf* (last visited on 20 September 2024).

[59] *Official Gazette of Bosnia and Herzegovina*, no. 4/97, 1/99, 9/99, 27/00, 32/00, 19/01, 47/04, 53/07, 33/08, 39/08 and 60/13.

[60] *Official Gazette of Bosnia and Herzegovina*, no.88/15, 34/21 and 63/23.

posts, comments, etc.)[61] of this company for the development of currently unspecified and unexplained artificial intelligence technology without a clear notification of the purpose and purpose of developing such technology".

Furthermore, the Agency stressed that users from Bosnia and Herzegovina are not given the option to refuse such data use. On the other side, the citizens of the European Union received a warning that the policy was changing and the option to withdraw data from the planned artificial intelligence training.[62] Although the author of this paper is not familiar with the fact whether the mentioned press release caused Meta to change its approach regarding BiH users, it is doubtless that the publicity is familiar with this fact.

Biometric data are extraordinarily important regarding passports, and for that reason, we will present some aspects of this issue in BiH. The Law on Travel Documents of Bosnia and Herzegovina in Article 19c prescribes that the applicant for passport issuance "must provide personal biometric data (picture, two fingerprints and signature)". According to Article 20 of the Rulebook on the Content and Method of Keeping Records (RCMKR),[63] the record of passports consists of, among all, photos, signatures, and fingerprints. In short, this record is a database of biometric characteristics. Furthermore, the record of passport is through the Unique Master Citizen Number (UMCN, Serbian: JMBG) connected with all other records, such as the record of UMCN, identity cards, residence and domicile, etc. This means that civil servants and, potentially, attackers using AI, have access to complete private data of an individual: name, surname, date of birth, place of birth, domicile, UMCN, fingerprints, photo, etc. According to Article 24 of the RCMKR, all data regarding passports will be delivered *electronically* to the Agency for Identification Documents, Registers and Data Exchange of BiH using "operative and technical solutions" established by this agency.

Since the enormous personal data are stored in the mentioned databases, this is a very fertile ground for personal data abuse. The Law on Agency for Identification Documents, Registers and Data Exchange of BiH (LAIDRDE)[64]

[61] Hence, social networks use our data for achieving different goals. Similarly, web cookies serve for identification of an individual and remembering his/her preferences and they are an example of data intrusion (Chałubińska-Jentkiewicz, Nowikowska, 2022, 185). Cookies can store a wealth of data, enough to potentially identify an individual, and are the primary tools that advertisers use to track a user's online activity so that they can target the user with highly specific ads (Gaba, Estremadura, 2020, 974).

[62] See: *http://azlp.ba/saopstenja/default.aspx?id=4243&pageIndex=1&langTag=en-US* (last visited on 18 September 2024).

[63] Rulebook on the Content and Method of Keeping Records, *Official Gazette of Bosnia and Herzegovina*, no. 55/15.

[64] *Official Gazette of Bosnia and Herzegovina*, no. 56/08.

prescribes that the question of keeping[65] and content of all records, especially the question of "special procedures for exchange and protection of biometric and other personal data" will be regulated by the Council of Ministers (hereinafter: CM) decision. In 2009, the CM adopted the Rulebook on the Method of Keeping and Special Measures of Technical Protection of Personal Data (RPPD), and this act prescribes that the method of keeping refers to "organizational and technical measures" as well as "personal data security plan" (Article 3).

Organizational measures include (1) informing and training employees; (2) physical measures of protecting rooms[66] and equipment in which personal data is processed; and (3) prevention of unauthorized duplication, copying, overwriting, and destruction of personal data.[67] *Technical measures* of personal data protection refer to prevention of unauthorized access to the personal data through prohibition of access to equipment, protection from destruction of personal data, etc. The personal data *security plan* rests on a number of principles: confidentiality, integrity, availability, authenticity, possibility of revision, and transparency.[68] Those principles proclaim measures that ensure the determination of person who can access personal data, immutability and completeness of data during processing, measures for determining who, when, and in which way processed the data, etc.

Since automatic data processing is relevant for the topic of this paper, Chapter III of the RPPD contains more precise rules on measures that should ensure personal data protection. Article 7 of the RPPD prescribes seven technical measures related to the username, password, and automatic log-off from the system after inactivity, etc. The purpose of those measures is to avoid unauthorized access to the personal data, although they are not enough instruments for preventing attacks using AI systems. Organizational measures include, *inter alia*, rules regarding downloading and saving documents, destruction of documents that contain personal data after the deadline for processing and removal of any media containing personal data from the rooms (Article 8). Also, the RPPD explicitly forbids duplication of media containing data from "collections of special categories of personal data,"

[65] According to Article 8(5) of LAIDRE, "the Agency is not the owner of the data stored in the records" (data on UMCN, identity cards, residence, domicile, etc.), but it is the source authority. The same article stipulates that "the Agency is exclusively responsible for technical maintenance and electronic archiving of data and information kept in records".

[66] According to Article 60 of the RCMKR, all data from records will be stored on technical devices located in special rooms of Agency. Also, the same article proclaims that those rooms must contain special measures that guarantee safe access and storage of data, while access to those rooms is limited only to certain officials.

[67] *Official Gazette of Bosnia and Herzegovina*, no. 67/09.

[68] See articles 4-6 of the RPPD.

such as biometric data (Article 11). The RCMKR regulates that data regarding fingerprints will be transferred only if the court's or prosecutor's warrant exists or in cases regulated by the BIH LPPD or international treaties.[69] Finally, in order to avoid loss, destroying of personal data, Article 11 prescribes that the controller must create backup of data from databases.

Article 17 of the RPPD is devoted to the protection of special categories of personal data. This article prescribes a number of measures that have accessory character in comparison with measures for protection of "regular," i.e., non-special categories of personal data. Firstly, the controller is obliged to stipulate that *in concreto* processing of special categories of data are in question. Besides, the controller takes "additional technical and organizational measures" during processing those types of data. The RPPD does not stipulate which measures are in question but prescribes that they ensure: (1) the capacity to recognize "each individual authorized access to the information system," (2) the work with data is possible only during "regular working hours of the controller," and (3) "cryptographic protection of data during transmission via telecommunication systems with appropriate software and technical measures".

The Law on Foreigners (LF) as well as the Rulebook on the Registration of Biometric Characteristics of Foreigners (RRBCF)[70] also regulate some issues related to the topic of this paper. According to Article 3 of RRBCF, the biometric data in the sense of this Rulebook refers to taking images, fingerprints[71] and signatures using technical means. Those biometric data are taken during visa issuance, residence approval procedure, procedure of imposing measures against foreigners, and during application for asylum. Some of these data are stored for five years, while other are permanently stored.[72] If a foreigner becomes a citizen of Bosnia and Herzegovina, his/her biometric data will be deleted, while some biometric data regarding refugees can be blocked and unblocked (article 17). All data about foreigners are stored in the Central database of foreigners (Article 122 of the LF). Also, the same article prescribes that the CM of BiH will render a decision on the start of the obligation of giving biometric data. Although the LF was passed in 2015, the decision of CM should be adopted during September 2024.

[69] See article 19, 25, 50 of the RCMKR.

[70] *Official Gazette of Bosnia and Herzegovina*, no. 55/16.

[71] In order to fight against the fake use of biometric characteristics, there are some techniques, such as "liveness detection methods". Those methods are used for checking perspiration patterns during fingerprint acquisition or eye blinking during face verification. See: Biggio *et al.*, 2015, 34.

[72] See articles 13-16.

The Rulebook on Central Database on Foreigners of Bosnia and Herzegovina (RCDF) is also relevant.[73] According to articles 3 and 4 of the RCDF, the Central Database is kept in electronic form, and biometric data are stored on the server of the Ministry of Security, "organized so that they can be easily used and changed". This fact is a ground for the claim that there is the danger of attacks on those data, with or without AI. It is not necessary to discuss about serious consequences that could be produced if those data (which are doubtless "big data") become the object of an AI attack. But who has the right to access data from this database? In order to answer this question, the Convention 108 (Article 2) is relevant since this act distinct controller, processor, and recipient. The controller is the subject who has "decision-making power with respect to data processing," the processor is the subject who "processes personal data on behalf of the controller," and the recipient is the subject "to whom data are disclosed or made available".[74] Biometric data controllers and, at the same time, authorities with the right to access database are ministries of foreign affairs and security, the Border Police, and Service for Foreigner's Affairs. The recipients of data from the Central Database are the mentioned authorities as well as to the Intelligence-Security Agency of Bosnia and Herzegovina and police (Article 4). Hence, the scope of institutions that have access is not large, and this fact is a good normative solution, but the real question is whether the BiH data protection law indeed ensures a good normative framework. The next subsection is devoted to the evaluation of domestic law.

BiH data protection law evaluation

Taking into consideration the previous subsection, we can draw some conclusions about the status of the (biometric) data protection law in Bosnia and Herzegovina.

Firstly, does BiH has data protection acts? We could say that BiH has a number of data protection legal acts, but some of them lack. More precisely, some bylaws acts that are very important for the implementation of personal data protection do not exist. When we speak on biometric data protection, this issue is mainly regulated as a part of rules concerning special categories of data protection, although some rulebooks are devoted to biometric data, such as Rulebook on the registration of biometric characteristics of foreigners. But the biometric data protection is not only relevant regarding foreigners, and domestic institutions should consider rendering an act that would exclusively refer to the protection of biometric data, perhaps even a statute

[73] *Official Gazette of Bosnia and Herzegovina*, no. 55/17.

[74] On these subjects, see Lindstad, Ludvigsen, 2023, 324-325.

on this issue. Concerning the AI, there are no acts devoted to this issue, although the LPPD forbids the automatic processing of special categories of personal data (that includes biometric data).

Secondly, are the domestic data protection law in accordance with EU standards? In short - no. Current BiH data protection law is not compatible with the EU GDPR; more precisely, the LPPD is in accordance with Directive 95/46/EC, which is repealed by the EU GDPR.[75] The biometric data are mentioned in Article 3 of the BIH LPPD that proclaims the special categories of personal data, including biometric data. The LPPD in abstracto prohibits the processing of special categories of personal data, with some exceptions (Article 9). According to Article 9(2g), the processing of the special categories of personal data can be prescribed by other statutes, but in those cases the statute "must contain specific provisions on adequate protection mechanisms".

It is necessary to take several steps in order to improve existing legal solutions and harmonize domestic law with the EU law. The main role belongs to domestic legislator since such an important question as personal data protection needs to be regulated predominantly by statutes. The legislator should, at first place, take into consideration the EU GDPR and the EU AIR and ensure harmonization. Also, the European Court of Justice and the European Court of Human Rights decisions should be taken into account, i.e., the main legal views and interpretations of those European institutions should be implemented in BiH personal data protection law. The judgments of BiH courts regarding biometric data protection are rarity.[76] Hence, we could claim that there is barely any case law on those questions. If it existed, it would certainly be useful for the legislator to spot the key problems and to serve him as a guideline.

In our opinion, an important aspect concerning domestic data protection law is, among all, connected with the fact that citizens are not enough informed on their rights. More precisely, the citizens' awareness regarding biometric (and in general personal data) data protection is at a low level. Hence, it is also important to take steps in order to make citizens aware of their rights as well as the dangers that are connected with the processing of their personal data. This is also a precondition to develop a case law, and domestic courts could be an important (even first) step in the process of improving data protection in BiH. Ordinary courts and especially the Constitutional Court of BiH could apply the ECtHR standards in their case law

[75] See Article 94 of the EU GDPR.

[76] See, for example: *http://azlp.ba/upravni_sporovi/default.aspx?id=3168&langTag=sr-SP-Cyrl*. On the contrary, there are more judgments regarding personal data protection in general, especially regarding video surveillance (CCTV). See: *http://azlp.ba/upravni_sporovi/Default.aspx?id=257&langTag=sr-SP-Cyrl&template_id=149&pageIndex=1.*

(on the basis of constitution norms related to the ECHR) when they interpret domestic law provisions on personal data.

When it comes to AI, the term "AI" in personal data processing is completely unknown regarding BiH data protection law. But Article 10 of the LPPD forbids "the automatic processing of special categories of personal data" (inter alia, biometric data), unless the statute prescribes "adequate protection". Regarding the EU AIR standards and the fact that this regulation is a new one, it is understandable that BiH law is not in accordance with this act. But the hazards concerning AI are present worldwide, and the fact the BiH is not a technological giant should not be an excuse for the ignoration of European regulations on AI.

Also, the BiH has an international obligation regarding personal data from the Stabilization and Association Agreement. It is not fulfilled since there are no independent supervisory bodies and sufficient financial and human resources that are capable of ensuring effective protection of personal data.[77]

Therefore, we could conclude that domestic law regarding personal data is outdated. Taking this in consideration, the CM of BiH rendered a decision about the nomination of a working group for drafting the new Law on the Protection of Personal Data[78] that will be in accordance with EU and Council of Europe law (according to Article 5). Since the new law is still not adopted, it is necessary to implement EU GDPR as well as EU AIR standards in future act(s). That will be (i.e., should be) not only fulfillment of the Agreement's obligation but an important step toward a better normative framework for private data protection.

Conclusion

One of the most challenging contemporary issues is the preservation of personal data. Among different types of personal data, biometric data are particularly sensitive, and the development of artificial intelligence presents a serious threat to private data since the presumption for AI work are large amounts of data. We showed that AI brings not only benefits but serious problems. In other words, AI is used for attacks on personal data.

In order to provide a decisive answer, the EU rendered two extraordinary important acts – the EU GDPR and the EU AIR. The main provisions of those acts, related to biometric data processing, were analyzed. Although we are impressed with the AI possibilities, we need to be aware that AI knows so

[77] See: Report on personal data protection in Bosnia and Herzegovina for 2023, *http://azlp.ba/publikacije/?id=4222*.

[78] *Official Gazette of Bosnia and Herzegovina*, no. 88/23.

much about us and has the potential to know even more. Thanks to machine learning, deep learning, computer vision, and biometric characteristics, the performances of biometric systems are impressive. Thanks to them, it is possible to find out where someone is or follow it in real time, i.e., live. AI recognizes our fingerprints, faceprints, signatures, and the way a person breathes, walks, or types on a keyboard.

But are there any limits? The law needs to react since everyone wants to get benefits from AI, but no one wants that AI knows everything about her/ him. But how to reconcile conflicting ideas: preservation of personal data if AI is "hungry" for data? The best way to react is to render a clear normative framework and apply it. That task is not easy since the AI is always one step ahead and the domestic law and case law need to be often updated as well as the knowledge of citizens, as we showed on the case of Bosnia and Herzegovina. The EU GDPR and the EU AIR are doubtless extraordinary important, but AI is still hungry for our data.

References

Alharbi, B., Alcantara, H. S., *Face-voice based multimodal biometric authentication system via FaceNet and GMM*, in *PeerJ Computer Science*, 2023, 9(1), pp. 1-18.

Berghoff, C., Neu, M., Von Twickel, A., *The Interplay of AI and Biometrics: Challenges and Opportunities*, *Computer*, 2021, 54(9), pp. 80-85.

Biggio,B., Fumera, G., Russu, P., Didaci L., Roli, F., *Adversarial biometric recognition: A review on biometric system security from the adversarial machine-learning perspective*, in *IEEE Signal Processing Magazine*, 2015, vol. 32(2), pp. 32-41.

Chałubińska-Jentkiewicz, K., Nowikowska, M., *Artificial Intelligence v. Personal Data*, in *Polish Political Science Yearbook*, 2022, 51(3), pp. 183-191.

Danks, D., *Learning*, in *The Cambridge Handbook of Artificial Intelligence*, 2014, pp. 151-165.

Davies, S., *The Data Protection Regulation: A Triumph of Pragmatism over Principle?*, in *EDPL*, 2016 2(3), pp. 290-296.

Gaba, J. P. M., Estremadura, J. J. M., *Data Protection of Biometric Data and Genetic Data*, in *Ateneo Law Journal*, 2020, 64(3), pp. 949-982.

Gáti, B., *Some Data Protection Issues of the EU Regulation of Artificial Intelligence*, in *Collection of Papers "Controversies of the Contemporary Law"*, 2022, pp. 588-605.

Harkous, H., Fawaz, K., Lebret, R., Schaub, F., Shin, K. G., Aberer, K., *Polisis: Automated Analysis and Presentation of Privacy Policies Using Deep Learning, Proceedings of the 27th USENIX Security Symposium*, 2018, pp. 531-548.

Jasserand, C., *Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data: Which Changes Does the New Data Protection Framework Introduce?*, in *European Data Protection Law Review*, 2016 2(3).

Kim, H., *Protecting Biometric Data*, in *Southern California Interdisciplinary Law Journal*, 2023, 33(1), pp. 185-207.

Lindstad, S., Ludvigsen, K. R., *When is the processing of data from medical implants lawful? The legal grounds for processing health-related personal data from ICT implantable medical devices for treatment purposes under EU data protection law*, in *Medical Law Review*, 2023, 31(3), pp. 317-339.

Milinković, I., *The Moral and Legal Status of Artificial Intelligence (Present Dilemmas and Future Challenges)*, in *Law and Business*, 2021, 1(1), pp. 29-36.

Sumer, B. *When do the images of biometric characteristics qualify as special categories of data under the GDPR?: a systemic approach to biometric data processing*, in *Lecture Notes in Informatics*, 2022, pp. 1-10.

Sumer, B., *The Al Act's Exclusion of Biometric Verification: Minimal Risk by Design and Default?*, in *EUPLR*, 2024, 10(2), pp. 150-161.

Yue Liu, N., *Bio-Privacy. Privacy Regulations and the Challenge of Biometrics*, Abingdon 2012.

Legal and internet sources

Adversarial Attack: Definition and protection against this threat, *https://datascientest.com/en/adversarial-attack-definition-and-protection-against-this-threat.*

AI washing explained: Everything you need to know, *https://www.techtarget.com/whatis/feature/AI-washing-explained-Everything-you-need-to-know.*

AI washing: How to detect it and why it's a growing problem, *https://www.dw.com/en/ai-washing-what-is-it-and-why-you-should-worry/a-69731038.*

An AI That Reads Privacy Policies So That You Don't Have To, *https://www.wired.com/story/polisis-ai-reads-privacy-policies-so-you-dont-have-to/.*

Biometrics, *https://www.innovatrics.com/glossary/biometrics/.*

Biometrie als KI-Anwendungsfeld, *https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Biometrie/biometrie_node.html.*

Centre for Information Policy Leadership Policy Report (CIPL Report), *Artificial Intelligence and Data Protection in Tension*, *https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_first_ai_report_-_ai_and_data_protection_in_tension__2_.pdf.*

Decision on the Formation of the Interdepartmental Working Group for the Drafting of the Draft Law on the Protection of Personal Data*, Official Gazette of Bosnia and Herzegovina*, no. 88/23.

ECJ decision in case C-291/12, *https://curia.europa.eu/juris/document/document.jsf?docid=143189&mode=lst&pageIndex=1&dir=&occ=first&part=1&text= &doclang=HR&cid=6302642*).

Einführung in die technischen Grundlagen der biometrischen Authentisierung, *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Technische_Grundlagen_pdf.pdf?__blob=publicationFile&v=1.*

EU Charter of Fundamental Rights.

European Parliamentary Research Service (EPRS), "The impact of the General Data Protection Regulation (GDPR) on artificial intelligence", *https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf.*

European Union's Artificial Intelligence Act - Regulation (EU) 2024/1689.

General Data Protection Regulation - Regulation (EU) 2016/679.

How extremist groups like "Islamic State" are using AI, *https://www.dw.com/en/how-extremist-groups-like-islamic-state-are-using-ai/a-69609398.*

Law on Agency for Identification Documents, Registers and Data Exchange of BiH, *Official Gazette of Bosnia and Herzegovina*, no. 56/08.

Mastercard makes fingerprint and 'selfie' payment technology a reality, *https://mastercardbelgium.prezly.com/mastercard-makes-fingerprint-and-selfie-payment-technology-a-reality.*

Nahost: Digitale Identifizierung nutzt repressiven Regimes, *https://www.dw.com/de/nahost-digitale-identifizierung-nutzt-repressiven-regimes/a-66615121.*

Press release - Warning to users of Meta company services in Bosnia and Herzegovina, *http://azlp.ba/saopstenja/default.aspx?id=4243&pageIndex=1&langTag=en-US.*

Qatar equips 15,000 cameras with facial recognition for soccer World Cup 2022, *https://www.biometricupdate.com/202208/qatar-equips-15000-cameras-with-facial-recognition-for-soccer-world-cup-2022.*

Rulebook on Central Database on Foreigners of Bosnia and Herzegovina, *Official Gazette of Bosnia and Herzegovina*, no. 55/17.

Rulebook on the Content and Method of Keeping Records, *Official Gazette of Bosnia and Herzegovina*, no. 55/15;

Rulebook on the registration of biometric characteristics of foreigners, *Official Gazette of Bosnia and Herzegovina*, no. 55/16.

Saudi Arabia builds a safer future with biometric borders, *https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/biometric-borders-saudi-arabia.*

Stabilization and Association Agreement between BIH and EU, *http://www.mvteo.gov.ba/attachments/bs_sporazum-o-stabilizaciji-i-pridruzivanju-izme%C4%91u-evropskih-zajednica-i-njihovih-drzava-clanica-i-bih.pdf.*

The ECtHR decision, *S. and Marper v. United Kingdom.*

The Law on Foreigners, *Official Gazette of Bosnia and Herzegovina*, no.88/15, 34/21 and 63/23.

The Law on Travel Documents of Bosnia and Herzegovina, *Official Gazette of Bosnia and Herzegovina*, no. 4/97, 1/99, 9/99, 27/00, 32/00, 19/01, 47/04, 53/07, 33/08, 39/08 and 60/13.