BIOMETRIC DATA, PRACTICAL ASPECTS OF THE PROCESSING OF SUCH DATA

Juris Madžuls[1], Jolanta Gaigalniece-Zelenova[2]

[1]Mg.soc.sc., State Border Guard College of the Republic of Latvia Border Guard and Immigration Services Subjects' Department, Docent, juris.madzuls@rs.gov.lv, Rezekne, Latvia

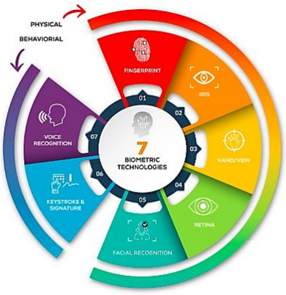
[2]Mg.soc.sc., State Border Guard College of the Republic of Latvia, Border Guard and Immigration Services Subjects' Department, Lecturer, jolanta.gaigalniece-zelenova@rs.gov.lv, Rezekne, Latvia

Abstract. *The authors of the paper explores the content of the qualification improvement course "The use of the AFIS and Eurodac systems" implemented in the State Border Guard College of the Republic of Latvia, the questionnaires given to the course participants in order to develop the guidelines for more effective processing of biometric data with main focus to the fingerprinting. The paper is aimed to identify the possibilities of improving the border guards' professional background in performing fingerprinting. The research was done in the State Border Guard College of the Republic of Latvia* (State Border Guard College Rezekne Academy of Technologies, 2022). *For this purpose analysis and evaluation of documents and officials work experience were performed and suggestions for the improvement of border guard fingerprinting methods were compiled. The author concludes that the effectiveness of biometric data processing depends not only on technology but also on the human factor - the knowledge, skills and professionalism of border officials. Therefore, continuous training and professional development is an integral part of the successful processing and use of biometric data in the national security system. The author recommends SBGC to invest in modern technologies and equipment to ensure efficient and accurate biometric identification technology processing.*

Keywords: *biometrics, identification, fingerprints, processing, verification.*

With the growth in data storage capacity and the development of biometrics, the possibilities for automatic identification of people are on the rise. Biometrics refers to the unique physical or behavioral characteristics of an individual that are used to identify and authenticate their identity.

All biometric characteristics can be divided into groups (Figure 1).



1.Physical: Fingerprint, facial, iris, hand, and retina are considered physical biometrics, based on direct measurements of a part of the human body.

2.Behaviour: Voice and signature are considered behavioural biometrics; they are based on measurements and data derived from an action and therefore indirectly measure characteristics of the human body (Biometric System, 2024).

Fig. 1. Biometric technologies (Source: Assured. Enterprises, 2024)

https://doi.org/10.17770/bsm.v5i10.8300

Biometric data allows the identification of a person and their genotype. Fingerprints - the epidermis of the skin forms a pattern of lines, or papillary lines, whose position depends on the anatomical structure of the inner layers of the skin (dermis). As the dermis lies on the subcutaneous layer of fat, it determines the structure of the skin's surface. The eccrine or sweat glands secrete an oily substance through the pores in the papillary glands, which allows accurate identification of blood type, sex, age, past and present diseases, or identification of the person. Papillary lines are individual, unchangeable; only disease, trauma or decomposition can alter them. In close relatives, and especially in twins, the pattern of collateral lines may be similar (Arājs et al., 2005).

According to Section 3(3) of the Immigration Law, the State Border Guard Service (hereinafter - SBGS) is required to establish and maintain electronic information systems for the performance of its functions.

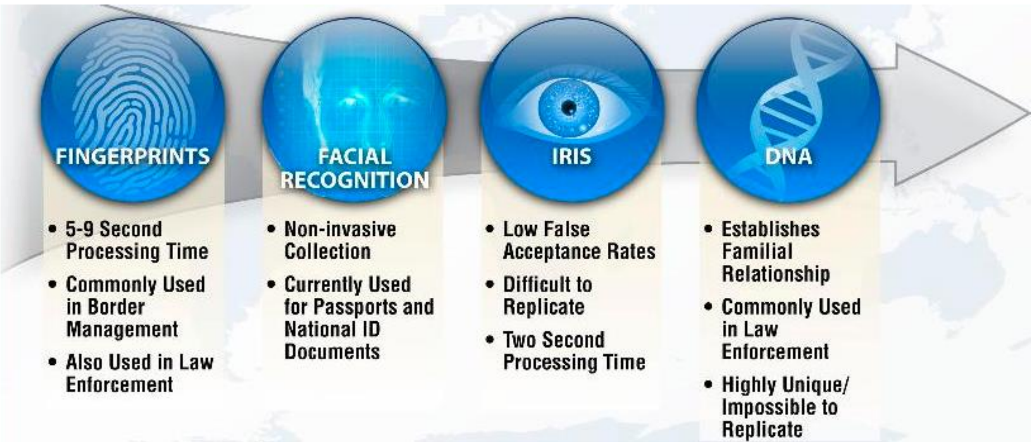

FINGERPRINTS
• 5-9 Second Processing Time
• Commonly Used in Border Management
• Also Used in Law Enforcement
FACIAL RECOGNITION
• Non-invasive Collection
• Currently Used for Passports and National ID Documents
IRIS
• Low False Acceptance Rates
• Difficult to Replicate
• Two Second Processing Time
DNA
• Establishes Familial Relationship
• Commonly Used in Law Enforcement
• Highly Unique/ Impossible to Replicate

Fig. 2. Most popular Biometric Security Systems (Source: Biometric System, 2024)

The SBGS uses biometric data (Figure 2) in various ways to ensure security and border control:

Verifying or entering data (face and fingerprint identification) into the Automated Fingerprint Identification System (hereinafter referred to as "AFIS"/ Asylum Seekers Fingerprint Information System or European Dactyloscopy (hereinafter "Eurodac") (Regulation (EU) of the European Parliament and of the Council, 2024) about asylum seekers, refugees, irregular immigrants and foreigners who have violated the conditions of entry, transit or exit. Since 2009, SBGC units have been using the Biometric Data Processing System (Latvian: *Biometrisko datu apstrādes sistēma* ore BDAS System) (Biometrisko datu apstrādes sistēmu likums, 2009), which allows fingerprints to be verified, attached and stored. This system significantly improves and speeds up the identification and verification of irregular migrants, making the fight against illegal immigration more effective and ensuring compliance with the Schengen Agreement

(Agreement between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic,1985);

- Verifying biometric data (face and fingerprint identification) in an electronic microprocessor chip within the passport. Malaysia was the first country to introduce biometric passports in 1998. More than 150 countries now use them. Using contactless smart card technology, they are used to authenticate the identity of the passport holder when travelling and have supported the growth of electronic passport gates at many international borders (Seon, 2024).
- Resisting technology, 1 February 2024, The Finnish Border Guard has announced a major expansion of its digital travel document pilot program at Helsinki Airport. Finnish citizens will now be able to test the Digital Travel Credentials (DTC) when traveling on 22 Finnair routes to and from Helsinki, up from just three previously. The DTC could greatly improve the travel experience for both visitors and immigrants once implemented more broadly. With the upcoming European Travel Information and Authorisation System (hereinafter ETIAS) (Regulation (EU) of the European Parliament and of the Council, 2018) visa waiver program launching in May 2025, the possibility of integrating digital credentials could facilitate immigration for legitimate travellers (Etias, 2024). The next stage in the digitalisation of the EU border process will be the EU's much-delayed Entry-Exit System (EES) launching on 10 November 2024 as well the introduction of the ETIAS travel system will go live in the first half of 2025 (Gils, 2024). This will require visitors from 60 visa-free countries to obtain a new electronic travel authorisation to enter 30 European countries (ETIAS.COM, 2024);
- Verifying biometric data (full group of ten fingerprints) in the Visa Information System when checking or issuing visas;
- Verifying facial image (IRIS recognition – real face vs photo in an electronic microprocessor chip within the passport ore/ and in the data base). It uses biometrics to map unique facial features from a live image and compares it to a previously captured image to verify that the two are the same person (Biometric ID | London Gatwick Airport, 2024);
- Data exchange with other countries: verifying DNA profiles and dactyloscopic data in combating terrorism and cross-border crime (Council Decision, 2008).

The SBGS is the custodian and holder of these information systems and is responsible for the use and exchange of data between national information systems in electronic form.

It should be noted that the processing of biometric data is strictly regulated by data protection principles and legal acts, such as Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the General Data Protection Regulation), which establishes the protection of individuals regarding personal data processing and the free movement of such data, while repealing the previous Directive 95/46/EC and national data protection laws. It is essential that biometric data is used only for specific, clearly defined purposes, such as security and border control, while ensuring that individuals' privacy rights are respected and adequate data protection is maintained. Data processing must be conducted in strict compliance with regulatory requirements, guaranteeing both privacy protection and transparent, responsible data usage. This approach helps balance security requirements with the need to protect individual rights and freedoms, fostering public trust and ensuring compliance with legal regulations.

Every company, public organisation or authority, including the SBGS, has a constant need for information. Identifying the required information and its location (databases, registers, etc.) is an essential factor in performing daily tasks, solving problems, making decisions, processing, searching for information or answers to questions.

Nowadays, information systems are computerised and operate in all Latvian public administrations and institutions, to the extent that some of them cannot function at all without information systems. Well-established information systems and trained staff increase the efficiency of the institution and allow it to carry out activities that were previously impossible.

In Latvia, the collection, storage, and use of biometric data involves several state institutions and organizations, which, in accordance with current regulatory requirements, process this data for specific purposes. To ensure that biometric data processing is conducted lawfully, all parties involved must comply with the applicable regulations and principles of personal data protection. Additionally, it is essential that individuals are fully informed about how and for what purposes their biometric data will be collected, stored, and used, thereby ensuring transparency and accountability. This disclosure of information and the responsible processing of biometric data strengthens public trust and helps to secure lawful data protection.

Fingerprint verification and retrieval

Border officials carry out biometric checks as part of their duties. Most popular biometric technology is the finger print biometric systems (Biometric System, 2024).

Fingerprints are taken by border officials when checking the entry conditions of a third-country national or when registering a detained foreigner or asylum seeker.

Fingerprints have been collected, studied and verified for over 100 years as a unique means of personal identification. Over the course of human evolution, nature has created a volar (ridged) skin surface on the fingertips to help grip objects and prevent them from slipping out of the hand. This has resulted in a unique pattern of papillary lines that is individual to each person. This pattern remains constant throughout life, from the seventh month of development in the womb until the body matures (Kavaliers, 1997).

In Latvia, the majority of criminologists, developing the ideas of R.Belkin (Belkins,1993), put forward the definition of dactyloscopy (from the Greek words daktylos - finger and skopein - to look) is a special section of the forensic technique component trasology, the subject of which is the examination of the papillary skin surface of the palms of human hands, soles of feet and their fingers for the identification of persons, as well as for the registration and search for criminals (guilty persons) (Arājs et al., 2005).

If the SBGS territorial board' unit do not have a BDAS system equipped with a Livescan data input device, border guards will need to use black fingerprint ink and a roller or paint stick in addition to a photo camera and fingerprint cards. Border guards will also need extra sheets of paper ore piece of glass to roll out the fingerprint ink, as well as personal hygiene wipes (alcohol-based) to wet and clean the fingers, to clean the roller and table top, and a sink with water and detergent (such as liquid soap, which is preferable to abrasive pastes) for washing hands.

It is important for border officials to get good quality fingerprints.

The quality of the biometric data (fingerprints) has a direct impact on the accuracy of the biometric system. As the quality of the data decreases, the accuracy can drop to 0%. Therefore, when working with systems such as the Visa information system or BDAS System, it is important that every border official is familiar with the basics of fingerprinting.

In the absence of a detailed methodology for fingerprinting in the SBGC, the authors of the study made a compilation of best practices for border officials during refresher courses, which may help border officials to avoid problems in the future.

Before starting a fingerprinting operation on a person, it is important to ensure that all operations are carried out in accordance with the applicable laws and regulations governing fingerprinting and data processing. It is important to respect the rights and obligations of the person as defined by the legislation. It is necessary to verify the identity and age of the person using available documents and information. At the same time, it is important to ensure that fingerprinting takes place in a secure and private environment in order to protect the privacy of the individual, and that data protection regulations are respected to guarantee the confidentiality of any data obtained.

Prior a fingerprint scan, the relevant equipment and software shall be checked to ensure that they are in working order and meet the technical requirements. It is important to check that all necessary tools and materials, such as disinfectants, are available. It is also important that the SBGC officials who will be taking the fingerprints are properly trained and familiar with the whole process. It should be ensured that the officials know how to deal with unforeseen situations. Finally, it is important to guarantee that the person is physically able to participate in the fingerprinting process and that there are no obstacles that could affect the success of the process.

When taking fingerprints, it is important to look carefully at the person's fingers and assess their condition, because:

1. Person may have previously used various means to alter or remove the papillary lines of their fingers, such as acids, cauterisation, cutting the skin or even amputation.
2. The position of fingers and ridges and the arrangement of parts can make fingerprinting difficult. People who have physically demanding jobs, such as construction workers or fishermen, tend to have very worn ridges. In such cases, official must try to keep the fingernail ink as light as possible and press down on the paper as lightly as possible. Some people may not have the papillary line details in the centre of the finger, which can cause problems when taking control impressions.
3. Person may have damaged fingers, such as scars, blisters, dislocations or fractures, which can affect the fingerprinting process.
4. Older people may have deformed fingers at the joints (phalanges) due to medical conditions such as arthritis. For these people, special techniques such as using a matchbox with a strip of paper attached can be used to take fingerprints in order to obtain high quality prints.

There are a number of important nuances that border guards have to consider before fingerprinting a person to ensure a successful process. Firstly, special attention should be paid to women with long nails. Dactyloscopic ink can get onto the nail lacquer, making it darker, or under the nail. In addition, long nails can make obtaining a complete fingerprint more difficult. Secondly, if the person wears watches, bracelets or rings, this can cause problems with fingerprinting. Some women may have several rings on a finger, making it difficult to take a print. If rings are removed, care must be taken to ensure that jewellery cannot be lost. If the rings are not removed, the fingerprint ink may get on them, especially if the rings are jewelled or intricately shaped, as the ink is difficult to wash off. Thirdly, it is important to be informed if the person is allergic to dactyloscopic ink in order to avoid possible health risks.

Before fingerprinting, the person must wash his/her hands with soap, preferably in warm water, to soften the surface of the skin and to remove any excess sweaty substance. The fingerprinting equipment should also be thoroughly cleaned to remove any residual paint or sweaty substances.

When checking or taking fingerprints, a border official may come across a person who is sweating profusely or has very dry hands. In the case of sweating, the fingers can be dried with toilet paper or the person can be asked to blow on their hands. If the hands are dry, the person can be asked to breathe on them or use wet wipes. In winter, ask the person to keep their hands warm by putting them in their pockets or under their armpits.

After washing the hands, they should be wiped with a dry towel or personal wipe to ensure that the fingers are clean and dry before the fingerprinting process.

If a roller is used, one or two 5x5 mm drops of ink shall be applied evenly to the glass, paper or plate and rolled out. The same roller shall be used to roll the ink onto another clean plate of the same type, without applying additional ink, in order to achieve an even and optimum amount of ink on the roller.

Officials must remember that it is forbidden to renew the paint on the roller every time a finger is smudged. It is important to keep track of the amount of paint on the finger so that the papillary lines are clearly visible. If there is too much paint on the finger, it is advisable to wash the finger and blot again or press it gently against the paper. Using a roller or pad, the fingerprint examiner can choose the most suitable position for standing or sitting. The main thing is to avoid standing between the legs of the person to be fingerprinted and to reflect on the presence of the service weapon and special equipment. The border guard may ask the person to turn around to avoid discomfort and to reduce the possibility of the person seeing the border guard's body movements. The fingerprint examiner shall choose the most comfortable position (preferably to the left of the person to be fingerprinted) and receive the thumb and forefinger of the right hand of the person from the side. The other fingers of the person shall be closed so as not to interfere with the fingerprinting and, holding the thumb, the person shall lightly touch the paint-covered plate and move the pad. If a roller is used, the person's hand shall be held with one hand and the dye smeared with the other. If a pad is used, do the same or place it on the edge of the table and roll it over. It is recommended to roll the finger from the most uncomfortable side to the most comfortable side.

Biometric authentication

According to Jain et al, biometrics is an effective means of personal authentication because they are unique to each individual and difficult to forge or steal. In addition, biometric technologies are increasingly being used in security systems because they provide a higher level of security than traditional methods such as passwords or access cards (Jain et al., 2004).

The use of biometrics also poses a number of challenges, including privacy and data protection. Mr Bowyer points out that the protection of biometric data is essential to prevent potential security threats and to protect the privacy of individuals (Bowyer, 2004). Unfortunately, biometric authentication can be hacked or falsified. The fact that biometric authentication is mistakenly believed by many to be impossible to hack only exacerbates the problem.

Advantages of a Biometric Security Systems (Ekemp, 2004), (Biometric System, 2024):

- Portability: biological characteristics are inherent characteristics of the human body, and the human body is the only binding, with portability.
- Security: human characteristics are the best proof of personal identity to meet higher security needs: can deliver greater security than username/ password authentication (EKEMP, 2021). The individual biometric systems can be connected together in a multilevel authentication system which further increase the security of the whole system. Should one of them fail or be cheated the others are able to negotiate the possibility of the break through (Biometric System, 2024).
- Uniqueness: everyone has different biological characteristics.
- Stability: biological characteristics such as fingerprint, iris and other human features will not change with time and other conditions.
- Universality: everyone has this characteristic.
- Convenience: biometric identification technology does not need to memorize passwords and carry special tools (such as keys), so it will not be lost (EKEMP, 2021).
  - Less friction than having to carry an item or remember a passphrase.
  - Delivers improved time-management efficiencies;
  - Can accelerate time of access to the premises/ data bases;
  - Allows officials to focus more on daily tasks due to reduction in necessary to change passwords or conduct service a check by the service on incorrect or illegal data processing.
- Collectability: the selected biometrics are easy to measure.

- Acceptability: users are willing to accept the selected personal biometrics and their applications (EKEMP, 2021).

Disadvantages:

- Can be hacked, but many do not realize;
- Can be expensive to implement;
- Time implication to move all the officials from a non-biometric system to a biometric as well as to upskill officers to adopt Biometric Security Systems;
- The sheer technological complexity can put SBGS off;
- Cooperation unwillingness/ privacy concerns for individuals who are not happy with acquiring their biometric features as now all their entries and exits will be recorded and the scope of misuse decreases (Biometric System, 2024).

The authors believe that the SBGS, in response to pressure from hybrid war, should unleash the use of biometric authentication as the grant access to phones, computers and buildings and as part of a multi-modal authentication process. For example, accessing a building or separate room through a combination of a retinal scan and voice identification, or accessing a laptop through both facial recognition and a fingerprint scan (Seon, 2024).

Conclusion and suggestions

Biometric data is crucial in the identification and authentication of personal it is individual and provides a high level of security. The use of fingerprints in person identification is reliable method that has deep roots in history – more than thousands of years, underlining its durability and accuracy.

Law enforcement officials must be properly trained and must have appropriate level of knowledge in laws and procedures in order to prevent potential irregularities and improve the process of persons` identification. Such procedures include a thorough assessment of the condition of the fingerprint of the person and the use of appropriate technical equipment for scanning fingerprint. Acting in line with the data protection regulations and observing human rights is essential and fundamental in performing service duties on a daily basis. Persons who don't allow the collection of fingerprints should be explained the importance of this procedure and the possible consequences of refusal. Processing and use of biometric data brings forward the issue on privacy and security, which in addition require extra mechanisms to protect personal data from potential threats (Data Protection Laws of the World, 2024). In order to tackle these challenges is essential to maintain public awareness and ensure effective control of national borders. The authors would like to stress that the effectiveness of biometric data processing depends not only on technology but also on the human factor - the knowledge, skills and professionalism of border officials. Therefore, continuous training and professional development is an integral part of the successful processing and use of biometric data in the national security system.

It is important to underline that the processing of biometric data is essential for national security and effective border control. The modern AFIS and Eurodac systems are helping SBGS units to quickly and accurately identify irregular migrants and overstayers. The quality of the biometric data has a direct impact on the accuracy and efficiency of the system, so it is important to ensure that correct data entry procedures are followed.

The SBGS is one of the organizations who are highly targeted by fraudsters and need to consider combining biometrics with additional security such as device fingerprinting, which looks at a device hash, cookie hash and browser hash to identify a returning user as well as spot other irregularities (Seon, 2024).

Based on the above characteristics, biometric identification technology has incomparable advantages over traditional identification methods. With biometric technology, it is no longer necessary to memorize and set passwords. It can be used to encrypt important files, data and transactions. It can effectively prevent malicious embezzlement and is more convenient to use (EKEMP, 2021).

SBGS need to invest in modern technologies and equipment to ensure efficient and accurate biometric identification technology processing.

References

1. Agreement between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany, and the French Republic on the gradual abolition of checks at their common borders. (1985, June 14).
2. Arājs, O., Čentoricka, M., Silarāja, S., & Evardsons, A. (2005). *Daktiloskopija.* Latvijas Vēstnesis.
3. Assured Enterprises. (n.d.). *Biometric technology cybersecurity.* Retrieved from https://www.assured.enterprises/cyber-products/biometric-technology-cybersecurity/
4. Autoru grupa profesora A. Kavaliera vadībā. (1997). *Kriminālistika. Mācību grāmata I daļa. Kriminālistiskā tehnika.* Latvijas Policijas akadēmija.
5. Belkin, R. S. (1993). *Kriminalistika. Kratkaia entsiklopediia.* M.
6. *Biometric Data Processing System Law.* (2009). Latvijas Vēstnesis, 90, 10.06.2009.; Latvijas Republikas Saeimas un Ministru Kabineta Ziņotājs, 13, 09.07.2009.
7. *Biometric ID | London Gatwick Airport.* (2024). *Biometric ID.* Retrieved from https://www.gatwickairport.com/biometric-id/biometric-id.html
8. *Biometric System.* (2024). Learn about the most popular biometric systems - Security360 solutions. Retrieved from https://www.security360.in/biometrics/
9. Bowyer, K. W. (2004). *Face recognition technology: Security versus privacy.* Retrieved from https://www3.nd.edu/~kwb/Bowyer_Tech_Soc_2004.pdf

10. *Business Travel News Europe.* (n.d.). *EU confirms long-awaited launch date for Entry-Exit System.* Retrieved from https://www.businesstravelnewseurope.com/Management/EU-confirms-long-awaited-launch-date-for-Entry-Exit-System
11. Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.
12. *Data Protection Laws of the World.* (2024). Retrieved from https://www.dlapiperdataprotection.com/index.html?t=about
13. EKEMP. (2021). *Traditional identification technology vs. biometric identification technology method.* Retrieved from https://www.ekemp.com.cn/post/biometric-identification-technology
14. *ETIAS.COM.* (2024). Finland greatly expands digital passport testing at Helsinki Airport. Retrieved from https://etias.com/articles/finland-helsinki-airport-digital-passport-expansion
15. Jain, A. K., Ross, A., & Prabhakar, S. (2004). *An introduction to biometric recognition.* Retrieved from https://ieeexplore.ieee.org/document/1262027
16. PMLP nepublicētie materiāli.
17. Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226.
18. Regulation (EU) 2024/1356 of the European Parliament and of the Council of 14 May 2024 introducing the screening of third-country nationals at the external borders and amending Regulations (EC) No 767/2008, (EU) 2017/2226, (EU) 2018/1240 and (EU) 2019/817.
19. Seon. (2024). *What is biometric authentication? - How does it work? | SEON.* Retrieved from https://seon.io/resources/dictionary/biometric-authentication/
20. State Border Guard College, Rezekne Academy of Technologies. (2022). *IXth International scientific and practical conference: Border security and management scientific journal of internal security and civil defence.* Retrieved from https://journals23.rta.lv/index.php/BSM/issue/download/189/710