TOWARDS THE DEVELOPMENT OF READINESS FOR THE APPLICATION OF THE PRINCIPLES OF ELECTRONIC BUSINESS FOR THE EXCHANGE OF BIOMETRIC DATA KEPT IN AUTOMATED SYSTEMS AS A BASIS FOR ESTABLISHING THE IDENTITY OF PERSONS

Snežana Stojičić[1]
Ministry of the Interior of the Republic of Serbia

Nataša Petrović[2],
Ministry of the Interior of the Republic of Serbia

Radovan Radovanović[3], **PhD**
University of Criminal Investigation and Police Studies, Belgrade

Abstract: Some of the classical methods of identification, which according to the general characteristics of biometrics, acquire a completely new meaning in the digital environment. Namely, the development aimed at achieving interoperability, standardization and application of the principles of electronic business in the environment of modern technological solutions enables identification methods based on biometric data to experience their flourishing and new affirmation. The technical technological solution of the system for AFIS (Automated finger identification system) and FIIS (Facial image identification system) are systems that are being developed as one of the answers to the need for quick identification of persons. The application of the system for automatic identification of persons with the help of fingerprints and photographs modernizes and improves performance and efficiency of the police work around the world and other investigative bodies in order to combat crime.

Keywords: identification, biometric data, AFIS and FIIS, interoperability, police cooperation, traces, data exchange

INTRODUCTION

To meet the development of readiness to apply the principles of electronic business for the exchange of biometric data which are kept in automated systems as a basis for determining the identity of persons, we consider systems which store this type of data and have become usual and necessary (Nilsson, 2019). AFIS and FIIS systems are specialist programs and technologies intended primarily for the criminal police for registration, identification, and verification of the identity of perpetrators of crimes that are prosecuted ex officio, and which are carried out on the basis of orders issued by the public prosecutor or the competent court (Biometric Standards for Law Enforcement, 2020). However, nowadays, the application of these systems is more and more widespread among private entities in the tasks of authorization of access and data protection (banks, access control ...) (Jasserand, 2016). Identification of a person in AFIS and FIIS involves the use of biometric data, fingerprints and / or facial photographs (Campbell, Chandler & Jones, 2020). The exchange of data between automated identification systems based on biometric data is one of the current challenges, especially in the field of international police cooperation (Guidance Biometric data-sharing, 2016; Biometric data-sharing process (FCC), 2016). The possibilities of these systems for the needs of the civil sector in the form of introduction of security systems, entrance control, secure identification of persons in the banking sector, etc. were also recognized. With the introduction of these systems in the Republic of Serbia and their improvement based on the application of the principles of electronic business, the preconditions for harmonization with standards and exchange of data according to European and world standards, as well as for preventing misuse of personal identity data are realized (Herr, & Podio, 2015). To meet the development of readiness to apply the principles of electronic business for the exchange of biometric data kept in automated systems as a basis for determining the identity of persons, the need to connect in existing systems for exchanging dactyloscopic and other data internationally such as Prum and EURODAC was recognized (Biometrics and the Schengen Information System – Fostering identification capabilities, 2020).

BIOMETRIC DATA AND IDENTIFICATION

The information which we are using to confirm the identity of the person is verified during the registration of the person and the acquisition of the necessary biometric data. The connection between a person and a print or photograph is unambiguous. There is a justified requirement for reliable and rapid identification of persons either perpetrators of crimes or other persons who are not from that category, and for whom such a need has arisen (mass accidents, identification of a person who does not know his identity or does not want to be identified, accidental death of persons who do not have identification documents on them, etc.). The systems, which are designed for the purpose of identification of persons using these data, consist of two components: the first is a component that processes biometric data of persons for the issuance of ID documents and the second is a component that processes data of persons in criminal-technical registration. Furthermore, apart from the purpose, they also differ in the number of data that are taken during the acquisition. Thus, in the first component, the acquisition of rolled and touch prints of one finger of the left and right hand and one face photograph is performed, and its task is to provide unambiguous biometric identification of citizens, providing preconditions for production of new identification documents for all citizens, control of access to facilities for the purpose of preventing access by persons without authorization. The purpose of the second component is to enable automation in the process of registration and biometric identification of perpetrators. There is an acquisition of fingerprints of all ten fingers, rolled and to the touch, both palms and edges and photos of faces, full face, left profile, right half profile, tattoo, and scars. The data is stored in central databases and it is anticipated that the exchange of data with appropriate organizations will take place according to world standards.

The importance and need for the exchange of dactyloscopic data between countries (PRUM, PCC SEE, EURODAC)

The modern world is increasingly facing the problem of cross-border organized crime, terrorism and migration, and there is a need for rapid exchange of data between countries, so that every person belonging to these categories can be efficiently recognized and identified in the shortest possible time (Policy Framework for the Regional Biometric Data Exchange Solution, 2015; Campbell, Z. & Jones, C., 2020).

The countries of the European Union have established a system for the exchange of biometric, DNA and vehicle data, the so-called Prum Convention and the Prum Agreement. For the needs of combating illegal migration, the EURODAC system has been established.

The Prum Convention is a law enforcement agreement signed on 27 May 2005 by Austria, Belgium, France, Germany, Luxembourg, the Netherlands and Spain in the town of Prum, Germany, and is open to all EU members wishing to access this type of data. .

The key elements of the convention were gathered by the Council of the European Union Decision 2008/615 / JHA of 23 June 2008 on strengthening cross-border cooperation, in particular in the fight against terrorism and cross-border crime (Council Decision 2008/615/JHA, 2008; Council Decision 2008/616/JHA, 2008).

The Convention has been adopted to allow signatories to exchange data on DNA, fingerprints and data on registered vehicles. It also contains provisions on the deployment of armed celestial marshals on flights between States Parties, joint police patrols, the entry of (armed) police forces into the territory of another state to prevent imminent danger (hot search) and cooperation in the event of a mass event or disaster, but these provisions are not discussed below.

The Convention has been adopted outside the framework of the European Union (and its enhanced cooperation mechanism), and is open to accession by any EU Member State that meets the conditions for the provisions of this Convention to apply only if they are compatible with European Union law (Figure 1).

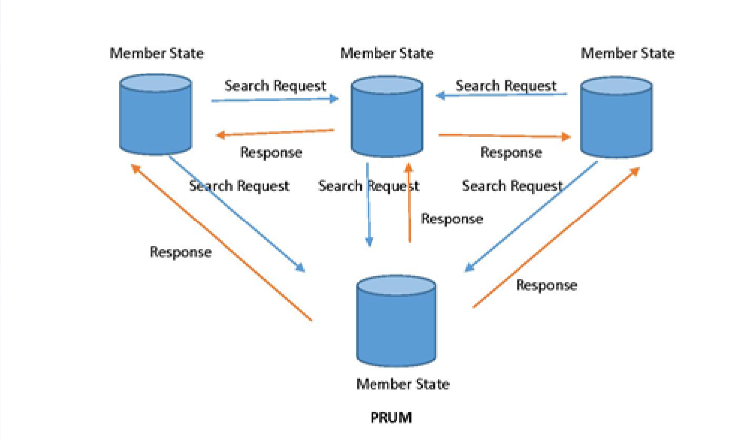

Figure 1 Scheme of data exchange transactions in the Prum Agreement

“European Dactyloscopy” (EURODAC) is a database of fingerprints that serves to identify asylum seekers and detect illegal border crossings in the European Union. Fingerprints are taken from asylum seekers and illegal migrants over the age of 14 on the basis of the EU law. In the following procedure, they are digitally sent to the central system of the European Commission and automatically checked against other fingerprints in the database (Figure 2). This makes it possible to determine whether the asylum seeker has already applied in another EU Member State or has illegally passed through another EU Member State in which he or she is registered (“first contact principle”). The automated fingerprint identification system is the first of its kind at the level of the European Union and has been operating since 2003.

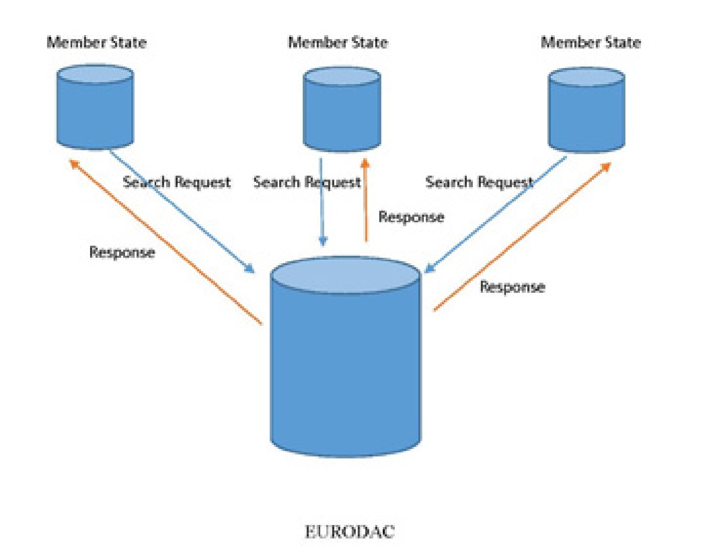

Figure 2 Image of data exchange transactions in the EURODAC system

In order for police and judicial cooperation between states to be effective, it is necessary that the essential information can be exchanged quickly and efficiently between the competent authorities of the Member States, and in order for such exchange to take place, it is necessary to establish appropriate systems. The data shared in cross-border cooperation should guarantee the accuracy and security of data during transmission, processing and storage, recording and exchange of data, as well as guarantee the limited use of data exchanged, according to the Data Protection Act of the country whose data are processed (Biometric data and data protection regulation, 2020).

AFIS AND FIIS DATA STORAGE

Storing paper documents in endless archives that contained demographic and dactyloscopic data on faces, the so-called dactyloscopic cards, is a thing of the past. The AFIS and FIIS systems allow demographic and biometric data to be stored in central databases and processed at high speed and reliability. Databases are standardized and adapted to the needs of data exchange. The data are distributed in the corresponding databases, namely in the ten-fingered database - the database for registered perpetrators of crimes, the two-fingered database - the database of persons requesting the issuance of identification documents, the database of palms, the database of unresolved cases of fingerprints, and fingerprints and the database of photographs. The ten-person database of registered persons contains demographic data, ten fingerprints, palms, control prints, edges, troposal photographs, photographs of tattoos, birthmarks and scars. The two-fingered database contains demographic data for all persons with two forefingerprints (valid and tactile), or some other two fingers if the forefingers are not available. The palm database contains demographic data of faces and prints of their palms and edges. The database of unresolved traces of palms and fingers contains fingerprints found at the crime scene. The database of demographics contains demographic data and one full-face photograph of a person, and 1: N fast search based on a photograph is enabled for persons who are particularly interesting and who need to be identified in this way. Basic demographic data for AFIS and FIIS databases can also be downloaded from other systems in which data for persons are stored. In the Republic of Serbia, they are taken over from the Unified Information System, which is also updated daily with changes from the AFIS and FIIS systems. Decentralized uniform entry, control, verification, identification and search are enabled. Database administration is performed centrally.

AFIS AND FIIS – DATA TYPES AND DATABASES

The primary objectives of the AFIS and FIIS systems include:

(a) Transferring and processing dactyloscopic evidence, as well as fingerprints of citizens and persons deprived of their liberty, as well as performing fingerprint and image searches in order to identify individuals.

(b) Acquisition, processing and comparison of fingerprint and palm prints - nn traces from the spot with indisputable prints from the corresponding databases.

(c) Acquisition, processing and comparison of fingerprints and photographs for the purpose of issuing identification documents.

The configuration of the AFIS and FIIS systems consists of a central system and workstations with appropriate peripherals positioned at remote locations. At the central location of the AFIS system, there are servers that manage the complete system and databases, as well as communication with workstations, i.e. system users. There is also a server that manages the match subsystem on which electronic characteristics of the prints are searched. The speed of the search depends on the number and strength of the swordsmen. To establish the system is necessary to provide all network connections. That will connect remote workstations to the central system. Remote workstations include workstations for registration of perpetrators of criminal offenses and identification of traces from the scene, as well as workstations that serve for the acquisition of biometric data for the production of identification documents (Libert, Grantham, Bandini, Ko, Orandi, & Watson, 2020; Libert, Grantham, Bandini, Wood, Garris, Ko, Byers, at al., 2018)

AFIS and FIIS, which are used for the registration of persons and the identification of perpetrators of criminal acts using nn traces from the scene, the so-called “The criminal component” consists of 5 databases:

1. TPF -Ten Print Finger,
2. PP - Palm Print,
3. ULF – Unsolved Latent Finger,
4. ULP – Unsolved Latent Palm and
5. Face.

Databases numbered above as 1, 2 and 5 are also related to personal data such as: identification number (JMBG), name, surname, name of father, mother, date of birth, date of registration, etc.

Databases numbered above as 3 and 4 are related to a specific crime offence and data related to the date and place of the crime offence, the injured party, the contact number, etc. This data depend on state legislation where systems are in use.

The database of undisputed fingerprints consists of 10 rolled prints and control prints - control thumbs and 4 control fingers of the right and left hand (Figure 3).

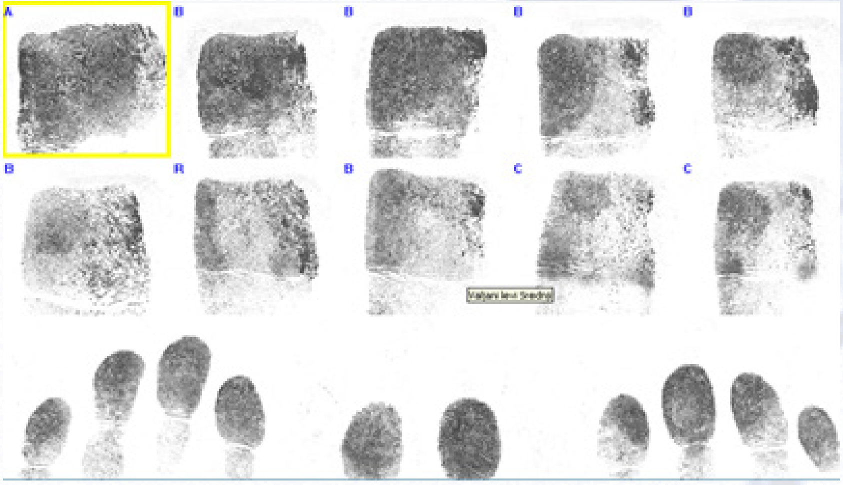

Figure 3 Fingerprint database

The database of undisputed palm prints consists of palm prints and edge prints of both hands. The database of undisputed photographs of faces consists of photographs of faces taken from the front, left profile and right semi profile, image of the whole figure and photograph of tattoos, scars and marks.

Bases of nn traces from the site consist of images of traces caused and processed by dactyloscopic methods (Latent Print AFIS Interoperability Working Group, 2020).

The so-called "The civilian component" consists of two types of databases:

1. Fingerprint database (2FF) and
2. Face.

The fingerprint database consists of rolled and touch fingerprints of both index fingers. The database of photographs consists of one photograph of a face taken from the front (Figure 4). If the index fingers of the person to whom the identification document is issuing are not available (one or both) due to amputation or permanent damage, a sweetening fingerprint is taken according to a predetermined schedule: thumb, middle finger, ring finger and little finger. The ordinal number of the finger is stored as data in the central system (NIST Study Measures Performance Accuracy of Contactless Fingerprinting Tech, 2020).

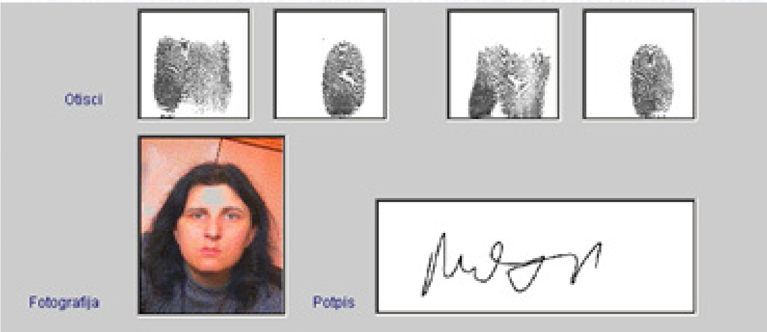

Figure 4 Biometric data taken for the purpose of issuing ID documents

TYPES OF SEARCH

Searches were also performed on such systems on the basis of the identification number. In the Republic of Serbia, a PERSONAL ID or a CASE ID might be used. The search filter might be set to be the number of processed items, fingerprints, traces and photographs. It should be noted that the reliability of identification using the AFIS system (97%) is higher compared to the FIIS system (80%) due to the higher number of coded characteristics (ID System Statement of Work for MOI AFIS and FIIS, 2003).

Searches can be: one to one (1:1) and one to many (1: N).

Searching or more accurately comparing 1:1 fingerprint means verifying a person's identity (Figure 5). This search takes place with the person present and compares the acquired biometric data with the data on the document (for example, ID card, passport, etc.), or when we have fingerprints of the person in the system and submitted fingerprints in electronic or paper form with the request to a person's identity verification (readmission operations and requests forwarded through Interpol).

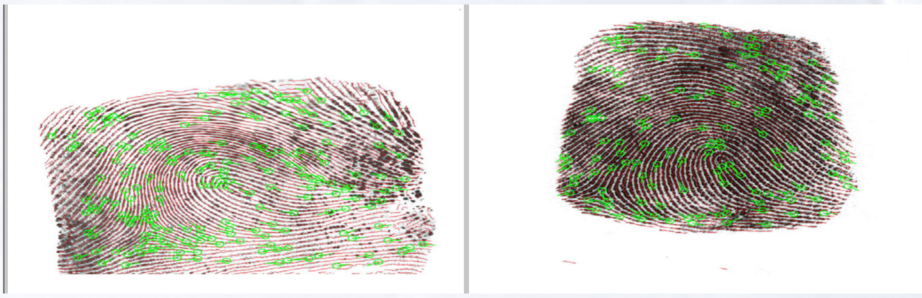

Figure 5 Search 1: 1 - comparison and verification

Search 1: N indicates the identification of an unknown person. The identification compares the biometric data of an unknown person with the biometric data stored in the databases. This type of search is used in the Prum and the EURODAC systems through electronic biometrical data exchanges.

Searching with an identification number consists of retrieving data ("Fetch") for a specific person who is located in the database under that number. In data exchanges, this search is used when the person is identified by fingerprints and it is needed to exchange personal data with the requesting party.

POSSIBILITY AND NEED TO CONNECT AFIS AND FIIS SYSTEMS WITH EUROPEAN DATA EXCHANGE SYSTEMS

Given that there is a constant need for rapid exchange of information between the EU member states and non-EU countries, as well as with non-EU countries that need to exchange data with each other, the Convention on Police Cooperation in Southeast Europe on automatic exchange of DNA data, dactyloscopic data and data on registered vehicles (hereinafter: KPS SEE) was made with the aim of strengthening cross-border cooperation, in particular in the fight against terrorism, cross-border crime and illegal migration and in an effort to implement KPS SEE, sending and comparing DNA profiles, dactyloscopic data and data on registered vehicles where all signatory states have successfully passed evaluations in the field of personal data protection and accordingly met the preconditions for the exchange of personal data, while taking into account common European principles and standards of data protection. For this purpose, it is necessary to adapt the national AFIS systems for interstate data exchange, to be, as it was called "Prum ready". The Republic of Serbia is also a signatory to this Convention (Law on Ratification of the Agreement between the Parties to the Convention on Police Cooperation in Southeast Europe on Automatic Exchange - Agreement, Official Gazette RS, - International Agreements, No. 15/2018).

To this end, all parties signed this agreement shall ensure the availability of reference data from the databases of the national AFIS systems established with the possibility to automatic exchange biometrical data for the purpose of identification of crime offenders, missing persons and corpses (Agreement, Official Gazette RS, International Agreements, No. 15/2018).

Relevant data for automatic exchange includes only dactyloscopic data and a reference number - a number used to link the data in the database with the data being sent. This data do not contain personal data on the basis of which the identity of the person can be directly determined (Data protection, Immigration Enforcement and Fundamental Rights, 2019). Reference data that cannot be used for person's identity verification linked to any person has to be send as dactyloscopic data for unknown person whom identity needed to be determined.

The rules for data exchange system which have to be defined and followed by all parties are:

1. Searches may be carried out only in individual cases and in accordance with the national law of the requesting State. Confirmation of the coincidence of dactyloscopic data with the dactyloscopic data of the country whose database was searched is performed by the national contact point of the state requesting the data, by automatically submitting the reference data necessary for an unambiguous hit. If there is a discrepancy between dactyloscopic data, the submission of additional available personal data and other information in addition to the basic personal data in relation to the reference data shall be governed by the national law of the country in whose database the dactyloscopic data are requested. Appropriate measures shall be taken to ensure the confidentiality and integrity of data transmitted to other Parties, including their encryption. States Parties shall take the necessary measures to guarantee the integrity of dactyloscopic data made available or transmitted to other Parties for comparison and to ensure that such measures comply with international standards.

2. The requested State may process the data of an identified person only for the purpose for which the data were transmitted. Processing for other purposes is permitted only with the prior approval of the requesting State and only in accordance with the national law of the requesting State. The submitted data is deleted immediately after comparing the data or sending automatic responses to searches unless further processing is required.

3. Electronic exchange of DNA data, dactyloscopic data and data on registered vehicles between the signatory states of the Convention is done through secure private communication networks with encryption. Technical details of the communication network and contact details and the availability of technical contact points are given in the user manual.

4. States Parties shall take all necessary measures to ensure that automatic search or comparison of DNA data, dactyloscopic data or data on registered vehicles is available 24 hours a day, seven days a week. In the event of a technical failure, the national contact points shall immediately inform each other and agree on temporary alternative arrangements for the exchange of information in accordance with the applicable legal provisions. Automatic data exchange is re-established as quickly as possible.

5. Digitization of dactyloscopic data and their sending is done in accordance with the adopted data format.

6. Each Party, both the one requesting the data and submitting the search request to the data submitter, shall ensure that the dactyloscopic data it sends are of sufficiently good quality for comparison using the AFIS system.

7. Each Party shall ensure that its search requests do not exceed the search capacities specified by the requested Party. The Parties shall submit statements establishing maximum daily search capacities for dactyloscopic data of identified persons and dactyloscopic data of persons whose identity has not yet been established.

8. The requested Party shall, without delay, check the quality of the dactyloscopic data sent by a fully automated procedure. In the event that the data are unsuitable for automated comparison, the requested Party shall promptly notify the requesting Party.

9. The requested Party shall carry out searches in the order in which the requests are received. Requests are processed within 24 hours by a fully automated procedure. The requesting Party may, if required by its national law, request that its requests be expedited and that the requested Party conduct such inquiries without delay. If the deadlines cannot be met due to force majeure, the comparison shall be made without delay as soon as the obstacles have been removed.

CONCLUSION

Towards the development of readiness for the application of the principles of electronic business for the exchange of biometric data kept in automated systems, the existing systems have to be enhanced. This enhancement should provide a complete solution for data acquisition (alphanumeric and biometric data), processing, integration with existing databases, and exchange through a telecommunications interconnection platform for secure information exchange. Modern systems offer effective person identification based on biometric data in a reliable and secure way. The systems have to be designed and developed to enable through simpler and more reliable manner easier work, as well as compliance with international norms and standards. On the other hand, those systems dedicated to support biometric identification of criminals might significantly contribute to the fight against terrorism and organized crime, with automatic exchange of data with other countries and other systems of the same or similar purpose. Furthermore, an efficient and effective person's identification is the foundation of the digitalisation of administrative procedures and in the end national security.

REFERENCES

1. 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, http://data.europa.eu/eli/dec/2008/615/oj
2. Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, http://data.europa.eu/eli/dec/2008/616/oj
3. Zakon o potvrđivanju sporazuma između strana potpisnica konvencije o policijskoj saradnji u jugoistočnoj Evropi o automatskoj razmeni DNK podataka, daktiloskopskih podataka i podataka o registrovanim vozilima, sa sporazumom o sprovođenju sporazuma između strana potpisnica konvencije o policijskoj saradnji u jugoistočnoj Evropi o automatskoj razmeni DNK podataka, daktiloskopskih podataka i podataka o registrovanim vozilima, Službeni glasnik RS - Međunarodni ugovori, broj 15/2018., http://www.parlament.gov.rs/upload/archive/files/lat/pdf/zakoni/2018/3419-18-lat.pdf
4. Biometric data and data protection regulations, (2020). Thales, Accessed 15th May 2020, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data
5. Latent Print AFIS Interoperability Working Group, (2020). Accessed 6th March 2020, https://www.nist.gov/programs-projects/latent-print-afis-interoperability-working-group
6. Biometric Standards for Law Enforcement, https://www.nist.gov/industry-impacts/biometric-standards-law-enforcement, Accessed 20th May 2020.
7. Nilsson, P. (2019). Face off: the perils of sharing your biometric data, Special Report Cyber Security, Financial Times, Accessed 14th May 2020. https://www.ft.com/content/90d4c8a2-02ba-11e9-bf0f-53b8511afd73
8. Policy Framework for the Regional Biometric Data Exchange Solution, (2015). The Bali Process, on People Smuggling, Trafficking in Persons and Related Transnational Crime, the Governments of Australia and Indonesia and comprising over 45 member countries and organizations.https://www.baliprocess.net/UserFiles/baliprocess/File/Policy%20Framework%20for%20the%20RBDES.pdf
9. Guidance Biometric data-sharing, (2016). UK Visas and Emigration, https://www.gov.uk/government/publications/biometric-data-sharing-fingerprint-matching-process-and-diagram
10. Biometric data-sharing process (Five Country Conference (FCC) data-sharing process) (2016). Home Office UK https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/557896/biometric-data-sharing-v7.0.pdf
11. Campbell, Z. & Jones, C., (2020). Leaked reports show EU police are planning a pan-European network of facial recognition databases, The proposal to link the EU’s facial recognition databases would likely connect them to the U.S. as well, in a massive consolidation of biometric data, https://theintercept.com/2020/02/21/eu-facial-recognition-database/
12. Campbell, Z., Chandler L. C. & Jones, C. (2020). Brussels considers pan-EU police searches of ID photos, Polotico, https://www.politico.eu/article/eu-police-facial-recognition-surveillance-report/
13. Jasserand, C. (2016). Legal Nature of Biometric Data: From ‘Generic’ Personal Data to Sensitive Data’, University of Groningen, Research Gate, https://www.researchgate.net/publication/308890225_Legal_Nature_of_Biometric_Data_From_’Generic’_Personal_Data_to_Sensitive_Data’

14. Data Protection, Immigration Enforcement and Fundamental Rights: What the EU's Regulations on Interoperability Mean for People with Irregular Status, (2019). PICUM, the Centre for European Policy Studies (CEPS) and European Migration Law, https://picum.org/wp-content/uploads/2019/11/Data-Protection-Immigration-Enforcement-and-Fundamental-Rights-Full-Report-EN.pdf

15. NIST Study Measures Performance Accuracy of Contactless Fingerprinting Tech, National Institute of Standards and Technology, U.S. Department of Commerce, https://www.nist.gov/news-events/news/2020/05/nist-study-measures-performance-accuracy-contactless-fingerprinting-tech, Published 19th May 2020

16. Libert, J., Grantham, J., Bandini, B., Ko, K., Orandi, S., &Watson, C. (2020). Interoperability Assessment 2019: Contactless-to-Contact Fingerprint Capture, National Institute of Standards and Technology, U.S. Department of Commerce, https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8307.pdf

17. Libert, J., Grantham,J., Bandini B., Wood, S., Garris, M.,Ko, K., Byers, F. at al. (2018). Guidance for Evaluating Contactless Fingerprint Acquisition Devices, National Institute of Standards and Technology U.S. Department of Commerce, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-305.pdf

18. Butler, M. J., Iyer, H., Press, R., Taylor, K. M., Vallone M. P. &Willis, S. (2018). NIST Scientific Foundation Reviews, National Institute of Standards and Technology U.S. Department of Commerce, https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8225-draft.pdf

19. Herr, F., & Podio, F. L. (2015). Common Biometric Exchange Formats Framework Standardization, The National Institute of Standards and Technology (NIST)**,** U.S. Department of Commerce, Accessed on 25th March 2020. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=914210

20. Biometrics and the Schengen Information System – Fostering identification capabilities, EU Science Hub, Accessed on 10th May 2020. https://ec.europa.eu/jrc/en/news/biometrics-and-schengen-information-system-fostering-identification-capabilities

21. ID System Statement of Work for MOI AFIS and FIIS, (2003). Ministry of Interior