THE DIGITAL FORENSIC METHOD USED IN INTEROPERABILITY FRAMEWORK FOR INFORMATION SYSTEMS USED ON EU LEVEL IN THE AREA OF MIGRATION AND BORDER MANAGEMENT

Snežana Stojičić[1]
Ministry of the Interior of the Republic of Serbia
Nataša Petrović[2]
Ministry of the Interior of the Republic of Serbia
Milesa Srećković, PhD[3]
School of Electrical Engineering, University of Belgrade, Serbia
Radovan Radovanović, PhD[4]
University of Criminal Investigation and Police Studies, Belgrade, Serbia
Zoran Milanović[5]
University of Criminal Investigation and Police Studies, Belgrade, Serbia

Abstract: Over the past years, great effort was directed to make the various information systems interoperable, as the lack of interoperability was recognized as a major obstacle to progress on the general digitalization processes. Implementation of interoperability framework is challenged especially regarding large IT systems on EU level using and developing in the area of border management. In this paper, the main components and current status of development will be presented, including those searching portal, common biometric system, common identity data repository, and multiple identity detector. Following this approach, the use of a shared biometric matching service, as a digital forensic method, has a goal to allow users to perform more efficiently search and cross-match biometric data. Furthermore, a common identity repository will

1 snezana.stojicic@mup.gov.rs
2 natasa.petrovic@mup.gov.rs
3 esreckov@etf.bg.ac.rs
4 radovan.radovanovic@kpu.edu.rs
5 zoran.milanovic@kpu.edu.rs

enable easy access to biographical information, so a person can be more reliably identified, and with a multiple identity detector, it will be possible to detect multiple identities.

Keywords: digital forensic, interoperability, large scale IS, identity

INTRODUCTION

We are witnessing accelerated digitalization in all spheres of life, which includes the increasing use of biometric data for the purpose of reliable person's identification. Therefore, the progress of forensic methods is conditioned, especially in the application of biometric identification of persons, including aspects of verifying the authenticity of identification documents based on biometric data. Carrying out the procedure of identification of persons in a fast and efficient way is a challenge for state bodies and institutions, companies, telecommunication operators, educational institutions and many others.

Also, one of the challenges today is the heterogeneous environment in the domain of large-scale IT systems, which are used in the EU, leading to the need to give high priority to establishing an appropriate level of interoperability between these IT systems.

One of the trends emerging in recent years is the increasing use of ubiquitous data collection systems, including biometric data through video surveillance systems, artificial intelligence (AI) systems, and decision support algorithms. The use of solutions based on information technologies and principles of electronic business in all areas of life is expanding, such as providing electronic services of vital public services, health, services related to police work, work of legal entities, migration monitoring, education, finance, trade and other areas. The risk of using new technologies also increases, especially in times of political tensions, elections, protests, demonstrations, armed conflicts or other types of crises, such as pandemics (Głowacka, Youngs, Pintea et al, 2021).

Having in mind the area of human rights, it is evident that raising awareness at the level of the international community about how technologies affect societies in almost every part of everyday life. It is well known that the general principles of human rights apply to the Internet and other digital technologies, i.e. they must meet the criterion of legality, pursue a legitimate goal, and be necessary and proportionate to achieve this goal. That means, the use of digital technologies that might violate human rights must always be the exception, not the rule, have to be determined by law, have to be applied only in special circumstances and include the least restrictive necessary means.

Digital technologies and technological development have an increasingly important role, they can be viewed both from the aspect of enabling and ensuring the fulfillment and full respect of human rights as well as from the aspect of possible abuses and violations of various aspects of human rights (Głowacka, Youngs, Pintea, et al, 2021). Especially is important to provide exchanging right information on time in case of emergency and security issues.

THE INTEROPERABILITY CONCEPT

The issue of interoperability has been mostly discussed in relation to digital public services (New European Interoperability Framework: Promoting seamless services and data flows for European public administrations, European Commission, 2017) but has also been raised in relation to many other policy fields. For the interoperability of e-Government services foundation was provided via the European

Interoperability Framework (EIF). The EIF was initially published in 2004 and has been subsequently updated in 2010 and 2017, the latter update following calls in the EU's Digital Single Market Strategy (A Digital Single Market Strategy for Europe, European Commission, 2015).

Although the subject matter is different, much of the EIF is relevant to the implementation of an interoperability model for Justice and Home Affairs (JHA) information systems. In particular, the extensive work conducted by the EU in this field has resulted in the development and refinement of guiding principles for, as well as a definition of, a model for interoperability (*https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604947/IPOL_STU(2018)604947_EN.pdf*).

The European Data Protection Supervisor says in his Opinion: *Interoperability is not primarily a technical choice; it is in particular a political choice to be made. Against the backdrop of the clear trend to mix distinct EU law and policy objectives (i.e. border checks, asylum and immigration, police cooperation and now also judicial cooperation in criminal matters) as well as granting law enforcement routine access to non-law enforcement databases, the decision of the EU legislator to make large-scale IT systems interoperable would not only permanently and profoundly affect their structure and their way of operating, but would also change the way legal principles have been interpreted in this area so far and would as such mark a "point of no return" (https://www.statewatch.org/observatories/eu-interoperability-of-justice-and-home-affairs-databases-a-point-of-no-return/).*

The concept of interoperability in area of JHA context using the definition determined in the EIF (European Interoperability Framework for Pan-European eGovernment Services, European Communities, 2004). Specifically, it defined the concept as "the ability of IT systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge" (Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, European Commission, 2005). There is no further discussing the applicability of this definition to the JHA context. Also, it is stated there that interoperability is a technical concept and not a legal or political concept, but interoperability of EU information systems in the area of Justice and Home Affairs has been identified as a priority at the highest political level (Interoperability: State of play, European Commission, 2018). Expected outcome by interoperability establishment, is that the EU information systems will supplement each other and will facilitate the correct identification of persons, thereby contributing to fighting identity fraud and increasing the efficiency of identity checks of third-country nationals in the Schengen area.

The main question is how interoperable databases will boost Europe's security, as databases used to control borders and fight crime are not talking with each other. Against what was decided to develop new tools so that authorities can better access and share information across the EU, European search portal: simultaneous search in all relevant EU databases, Multiple identity detector: creates an alert when it detects a risk of identity fraud, Biometric matching service: cross-checks biometric data in relevant databases and Common identity repository: streamlines access to data on non-EU citizens.

Expected improvement of information flows will help to better detect security threats, combat identity fraud, improve border checks as well as prevent information gaps.

In May 2019, the European Parliament and the Council adopted regulations 2019/817 (Regulation on establishing a framework for interoperability between EU information systems in the field of borders and visa, European Commission, 2019) and 2019/818 (Regulation on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration, European Commission, 2019). The purpose of the regulations is to ensure that border

guards and law enforcement officers have systematic and efficient access to the information they need to perform their duties, thus further closing security gaps (https://www.eulisa.europa.eu/Newsroom/News/Pages/Political-Agreement-for-Interoperability-between-EU-Information-Systems.aspx).

The interoperability concept applied to the EU information systems, police and border officers, among others, aimed to make access information much faster. Easier information sharing will considerably improve security, allow for more efficient checks at external borders, improve detection of multiple identities and help prevent and combat illegal migration.

THE MAIN INTEROPERABILITY COMPONENTS

In addition to checking the travel document, taking fingerprints and entering personal data within the border control procedure, it should be possible to check whether the person has applied for asylum earlier, whether they are in the criminal record, they are actively involved in by searching, how many times previously in the EU (with and without a visa).

The four main interoperability components need to be established: a European search portal to allow authorities to search multiple information systems simultaneously, using both biographical and biometric data; a shared biometric matching service, which would enable searching and comparing fingerprints and facial images from several system; a common identity repository, which would contain biographical and biometric data of third-country nationals available in several EU information systems; and a multiple identity detector, which checks whether the biographical identity data contained in the search exists in other systems covered, to enable the detection of multiple identities linked to the same set of biometric data (*https://www.consilium.europa.eu/en/press/press-releases/2019/05/14/interoperability-between-eu-information-systems-council-adopts-regulations/*).

The European Search Portal (ESP) would enable the simultaneous query of multiple JHA information systems using (both biographical and biometric) identity data (Central-SIS, Eurodac, VIS, the future EES, and the proposed ETIAS and ECRIS-TCN systems, as well as the relevant Interpol systems and Europol data) Figure 1.

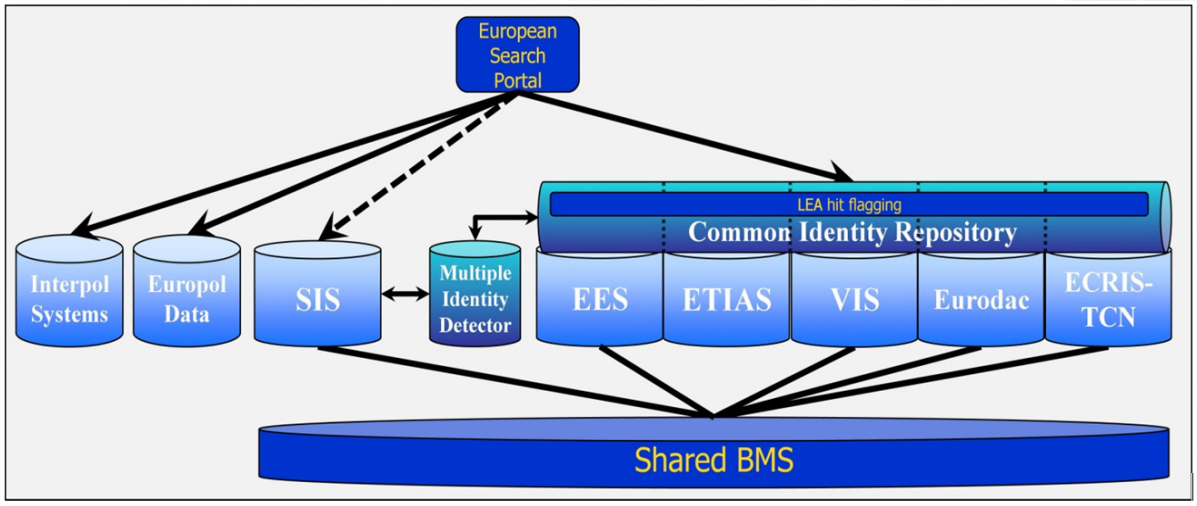

Figure 1. *The necessary technical components to achieve interoperability*[6]

The shared Biometric Matching Service (sBMS) is dedicated to enable the querying and comparison of biometric data (both fingerprint and facial images) across EU information systems by generating and storing mathematical representations of the biometric data (SIS, Eurodac, VIS, the future EES and the proposed ECRIS-TCN).

The shared BMS storing biometric templates obtained from the biometric data will contribute through the storage and use of mathematical representations of biometric data to support the ESP, the CIR and the MID. The biometric data (fingerprint and facial images) are exclusively retained by the underlying systems. The shared BMS would create and retain a mathematical representation of the biometric samples (a template) without the actual data, which remains thus stored in one location, only once. However, the biometric templates shall be stored in the shared BMS in logically separated form according to the EU information system from which the data originate (Regulation on establishing a framework for interoperability between EU information systems in the field of borders and visa, European Commission, 2019) meaning that the shared BMS constitutes a new database of the templates and therefore does not fully conform to an appropriate definition of interoperability (Gutheil, Liger, Eager et al, 2018).

The shared BMS added value is in identifying multiple identities across the information systems. Representing a key enabler to help detect connections between data sets and different identities assumed by the same person in different central systems. From that point of view, it also brings value without the other interoperability components. The search BMS would still be able to determine multiple identities across all systems except for ETIAS.

The Central Identity Repository (CIR) creating an individual file for each person that is registered in the EES, VIS, ETIAS, Eurodac or ECRIS-TCN and would be a shared component for storing the biographical and biometric identity data of third-country nationals. It is established for the purpose of facilitating and assisting in the correct identification of persons registered in the EES, VIS, ETIAS, Eurodac and ECRIS-TCN (Gutheil, Liger, Eager et al, 2018) and shall store the data with reference to the actual record in the EU IS to which the data belong, logically separated according to the information system from which the data have originate.

However, the establishment of the CIR is the most challenging aspect of interoperability – as conceived by the Commission – and raises privacy and data protection concerns in numerous respects (Gutheil, Liger, Eager et al, 2018). As such, the CIR introduces the most significant changes compared to the current implementation and represents the most significant challenge from the aspect of the protection of personal data and the right to privacy in this context.

A multiple-identity detector (MID) would check whether queried identity data exists in more than one system and allow a mechanism for investigating and verifying the linked identity data (data held in the CIR as well as SIS).

A multiple-identity detector (MID) creating and storing identity confirmation files containing links between data in the EU information systems included in the CIR and SIS and allowing detection of multiple identities, with the dual purpose of facilitating identity checks and combating identity fraud. It is established for the purpose of supporting the functioning of the CIR and the objectives of the EES, VIS, ETIAS, Eurodac, SIS and ECRIS-TCN. However, it does not fully constitute an interoperability solution in line with an appropriate definition of interoperability. This is because it creates new data in the form of links and identity confirmation files.

THE ADDITIONAL ELEMENTS TO SUPPORT INTEROPERABILITY COMPONENTS

The universal message format (UMF) defines standards for certain content elements of cross-border information exchange between information systems, authorities or organizations in the field of Justice and Home Affairs. The UMF planned to be used in the development of the EES, ETIAS, the ESP, the CIR, the MID. The UMF standard introduces a common and unified technical language to describe and link data elements, in particular the elements relating to persons and (travel) documents. Using UMF when developing new information systems guarantees easier integration and interoperability with other systems.

Establishment of a central repository for reporting and statistics (CRRS) is necessary to enable the creation and sharing (anonymous) statistical data analytical reporting for policy, operational and data quality purposes. The current practice of gathering statistical data only on the individual information systems is detrimental to data security and performance and it does not enable the correlating of data across systems.

The CRRS would provide a dedicated, separate repository for anonymous statistics extracted from SIS, VIS, Eurodac, the future EES, the proposed ETIAS, the proposed ECRIS-TCN system, the common identity repository, the multiple-identity detector and the shared biometric matching service.

The concepts of automated data quality control mechanisms and common quality indicators, needed to ensure the highest level of data quality when feeding and using the systems. Without that, consequences may occur not just for not being able to identify wanted persons, but also by affecting the fundamental rights of innocent people (*https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:793:FIN*).

EXISTING AND FUTURE IS UNDER INTEROPERABILITY ARCHITECTURE

The Visa Information System (VIS) is one of the information systems in the center of the Schengen area, which connects the consulates of the member states in non-EU countries and all external border crossings. It provides support for the process of issuing a short-stay visa for a visit or transit through the Schengen area, as well as their verification. It includes a biometric data management system (BMS) that allows third-country nationals traveling to the EU to identify and verify based on biometric data. It also facilitates checks in the territory of the Member States, in the identification of persons who do not meet the conditions for entry or stay in the territory of the Member State. In addition, it supports the asylum application process and thus contributes to preventing threats to internal security. Usage of VIS for one-year period is shown on Figure 2, 3.

The VIS is an integral part of the developing interoperable IT architecture in the field of justice and home affairs (JHA). The VIS itself is evolving in support and implementation of a stronger, more efficient and safer common visa policy. The development of the VIS is aimed at enabling detailed verification of data on visa applicants, through better exchange of information and full interoperability with other databases used in the EU. The upgrade also includes the introduction of face image search capabilities and the storage of additional information. As part of interoperability, it is of particular importance to achieve interconnection between VIS and EES, with elements of data exchange and synchronization, with the aim of limiting duplication of personal data, and in line with the "privacy by design" approach.

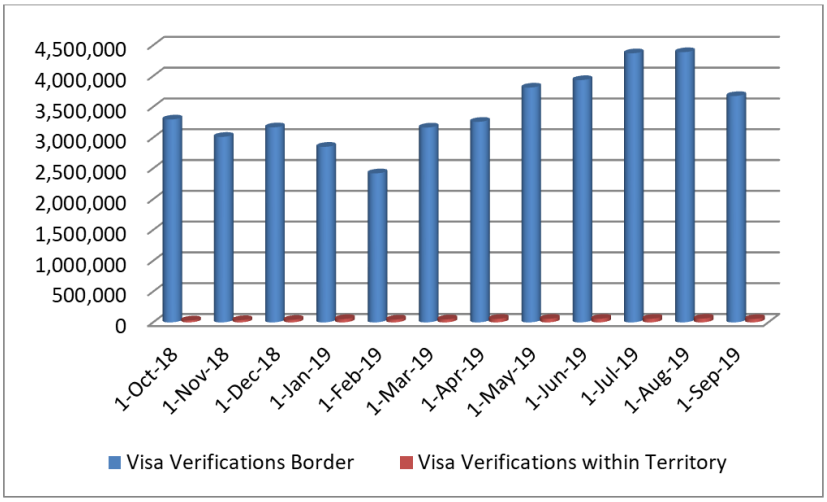

Figure 2. V*isa verification distribution (oct 2018-sept 2019)*[7]

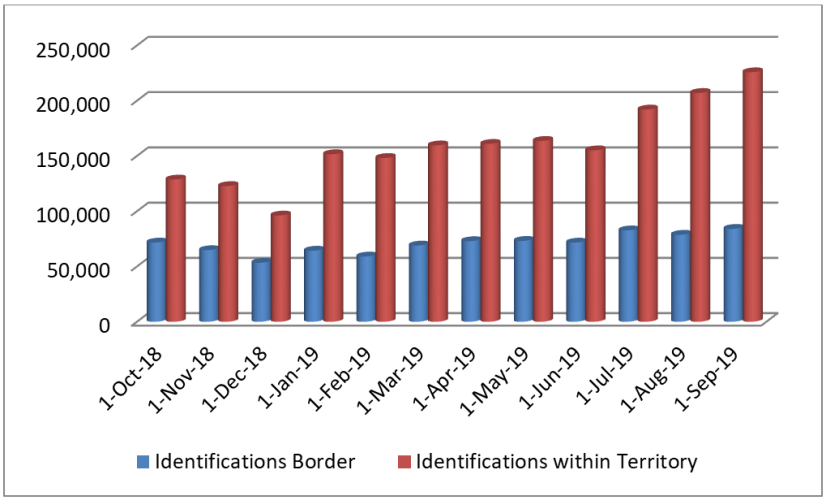

Figure 3. *Visa identification distribution (oct 2018-sept2019)*[7]

The central system VIS (CS-VIS) has two components, a VIS central database (located in

Strasbourg, France, with a back-up site in Sankt Johann im Pongau, Austria) with alphanumerical searching capabilities, and an Automated Fingerprint Identification System (AFIS) that compares new fingerprints against those in the database and returns a hit/no-hit response, along with matches. The national interfaces (NI-VIS) are located at all external border crossing points of each Schengen state and at consulates in non-EU countries.

The primary data used for verification and identification are 10 fingerprints and a scanned/digital photograph, both of which are required to be registered for persons wishing to apply for a visa into the Schengen area. While other alphanumeric data are necessary for the visa application process, the VIS makes use of biometric data for identification and verification purposes.

Biometric information for new applicants for a Schengen visa at an EU consulate remains valid in the system for five years after the expiration of the visa.

Upon the arrival of third-country nationals to the Schengen area competent border authorities can perform two types of searches, both carried out using the separate Biometric Matching System (BMS): a check that the fingerprints scanned at the border crossing point correspond to the fingerprints associated with those attached to the visa to establish the validity of a claimed identity (1-1) and an identification search at the border crossing post that compares the fingerprints of any person who may not, or may no longer, fulfil the conditions for the entry to, stay or residence on the territory of the Member States with the contents of the entire database (1-n). Usage of VIS by user group is shown on Figure 4. Performance was very good in terms of the average processing time reported: in 2019 it was less than 0.8 seconds on average for alphanumeric searches (SLA is 30 seconds) and less than 2 seconds on average for fingerprint verification (SLA is 3 seconds)[9].

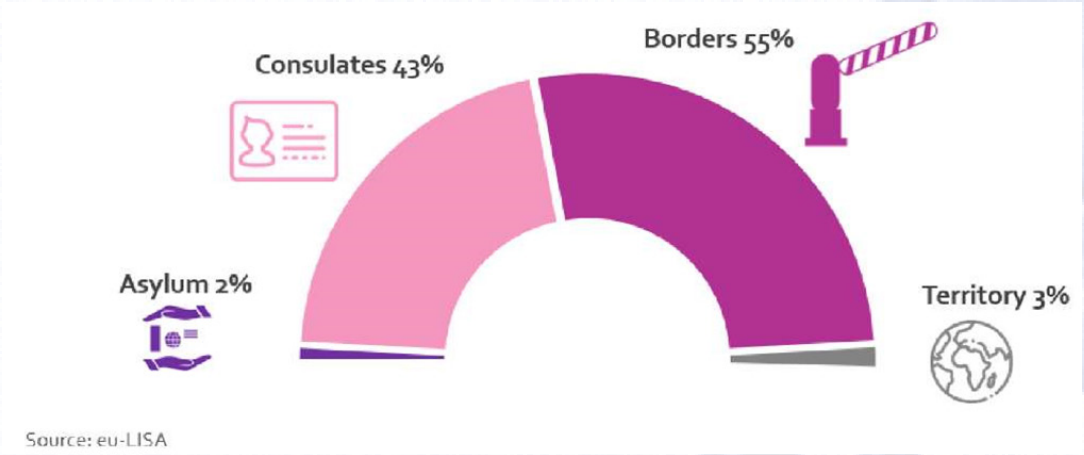

Figure 4. *Breakdown VIS usage per user group (2019)*[8]

In terms of its evolutions, the VIS central system has been hugely affected by the development of the EES.

The Entry/Exit System (EES) will electronically register the time and place of entry, exit and refusal of third-country nationals admitted for a short stay to the territory of Schengen Member States and will automatically calculate the duration of their authorized stay.

In November 2017, the Regulation establishing an EES and amending the Schengen border code in relation to the EES was adopted (Regulation of the European Parliament and of the Council on establishing an Entry/Exit System (EES), European Commission, 2017). This system is developed with the aim of ensuring systematic and reliable identification of over stayers, aiming to strengthening of internal security and the fight against terrorism by permitting law enforcement authorities access to travel history records. The EES will abolish passport stamping and instead a record of all cross-border movements of third-country nationals will be created via the collection of alphanumeric and biometric (fingerprints and facial recognition (Commission Implementing Decision (EU) 2019/329, European Commission, 2019) data to strengthen the fight against irregular migration and ease the border crossing time for the large majority of 'bona fide' third-country travelers. The specifications relating to the quality, resolution and use of fingerprints for biometric verification and identification in the EES are set out in the Annex of Commission Implementing Decision (EU) 2019/329.

The EES Regulation is envisaged to be interoperable with the VIS via secure communication channel. The border authorities using the EES to consult the VIS. Retrieving the visa-related data users will be

8 Report on the technical functioning of the Visa Information System (VIS), European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, 2020

able to create and update entry/exit records or refusal of entry records; to enable the border authorities to verify the validity of the visa and the identity of the visa holder by directly searching the VIS with fingerprints at the borders where EES is operated; and to enable the border authorities to verify the identity of visa-exempt third–country nationals against the VIS by using fingerprints. There is a two-way communication, meaning that through this interoperability also allows the border and other authorities using the VIS to directly consult the EES from the VIS for the purposes of examining visa applications and of taking decisions relating to those applications, and of enabling visa authorities to update the visa-related data in the EES in the event that a visa is annulled, revoked or extended.

EES data may be used as an identity verification tool in cases where the third country national has lost/destroyed its documents or where designated authorities are investigating a crime through the use of fingerprints or facial images and wish to establish an identity**.** The Furthermore, EES data is intended to facilitate the provision of evidence by tracking the travel routes of a person suspected of having committed a crime or who is the victim of crime (Commission Implementing Decision (EU) 2019/327, European Commission, 2019).

The Eurodac (European Asylum Dactyloscopy Database) has been the EU asylum fingerprint database since 2003. (Council Regulation (EC) No. 343/2003, European Commission, 2003). Its primary purpose, set out in the Eurodac Regulation (Regulation (EU) No 603/2013, European Commission, 2013), is to assist application of the Dublin III Regulation (Regulation (EU) No 604/2013, European Commission, 2013) that lays down rules for determining which Member State is responsible for examining an asylum application. The main reason why Eurodac was created was to determine whether an asylum applicant had previously applied for asylum in another Member State, thus preventing 'asylum-shopping'.

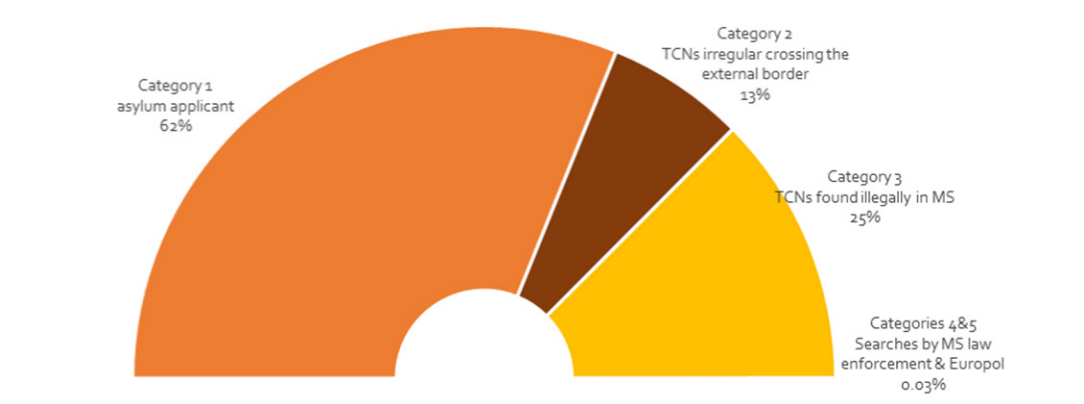

Figure 5. *Data breakdown per the main category transmitted to Eurodac in 2020*[9]

The EURODAC contains only fingerprints in a central database (along with data and place of registration) and no other personal information. Each Member State is required to perform acquisition of fingerprint for all applicants for international protection and those apprehended whilst attempting to cross a border irregularly over the age of 14 and to transmit the data to Eurodac within 72 hours of the irregular crossing (Regulation (EU) No 603/2013, European Commission, 2013). Thus, the Eurodac holds fingerprints on two categories of persons: individuals who have applied for international protection; and individuals from irregular border entries.

According the regulation fingerprint data is required to be erased from Eurodac once those present in the database acquire EU citizenship. The 2000 Eurodac legislation (Council Regulation (EC)

9 https://www.eulisa.europa.eu/Publications/Reports/Eurodac%20-%202020%20Statistics%20-%20Report.pdf

No 2725/2000, European Commission, 2000) did not provide for law enforcement authorities to request fingerprint comparisons; however, the scope of Eurodac was expanded with Regulation (EU) No 603/2013 providing new functionalities for granting access to national law enforcement bodies and Europol. Competent national law enforcement bodies and Europol are only permitted to consult Eurodac data for the purposes of preventing, detecting or investigating terrorist offences and other serious crimes (Framework Decision 2002/47540, Framework Decision 2002/58441 European Commission, 2002). Further improvement of the regulation is ongoing process.

The Schengen Information system is under operation for 25 years up to 2020. The second-generation Schengen Information System (SIS II) has been in operation since 2013, and supports external border control and law enforcement cooperation in the Schengen states. It enables competent authorities to enter and consult alerts on certain categories of wanted or missing persons and objects. Furthermore, the instructions are provided on what to do in case of 'hit', when the person or object has been found. As a prime compensatory measure for the abolition of internal border control, the purpose of the SIS II is 'to ensure a high level of security within the EU's area of freedom, safety and justice, including the maintenance of public security and public policy and the safeguarding of security in the territories of the Member States, and to apply the provisions of the Treaty relating to the movement of persons in their territories, using information communicated via this system' (Regulation (EC) No 1987/2006, European Commission, 2006).

The scope of SIS II is defined by legal instruments, Regulation 1987/2006 which provides for border guards and visa issuing and immigration authorities to insert and consult alerts on third-country nationals for the purpose of refusing their entry into or stay in the Schengen area (Regulation (EC) No 1987/2006, European Commission, 2006), Council Decision 2007/533 enables competent authorities to register and check alerts on persons or objects related to criminal offences, as well as on missing persons (Council Decision 2007/533/JHA, European Commission, 2007).

Alerts are inserted on to the system by competent authorities (which is dependent upon the nature of the alert issued) of Member States on third-country nationals to be refused entry or stay; persons wanted for arrest or surrender purposes, persons sought to assist with a judicial procedure; missing persons; persons and objects for discreet checks or specific checks; and objects sought for the purpose of seizure or use as evidence in criminal proceedings.

The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), is in charge of the operational management of the central system and the communication infrastructure. According the high-performance demand EU-Lisa use agile project management methodology for system development and 24/7 operational monitoring support. As it is under continuous improvement in the recent years this included: the deployment of the SIS II Automated Fingerprint Identification System (AFIS) realized in March 2018 with the obligation for the Member state to enabling SIS-AFIS searches by December 28, 2020; the adoption of the recast Regulations in December 2018, the implementation of the SIS recast is ongoing, for the first time the disconnection of a Member State was planned and tested (The disconnection of the United Kingdom was implemented at the beginning of 2021).

In 2020, searches in SIS II AFIS were performed by Austria, Belgium, Bulgaria, the Czech Republic, Denmark, Germany, Hungary, Iceland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, the Netherlands, Portugal, Romania and Slovenia (*https://www.eulisa.europa.eu/Publications/Reports/SIS%20II%20-%202020%20Statistics%20-%20report.pdf*).

On December 31, 2020, there were 93,419,371 alerts stored in the SIS. The alerts on Persons represented 1% of the total alerts stored in SIS II. The largest categories were Issued document and Security, with 76% (over 71 million alerts) and 7% (over 6.5 million alerts), respectively. Figure 4 provides a visual breakdown of alerts per category.

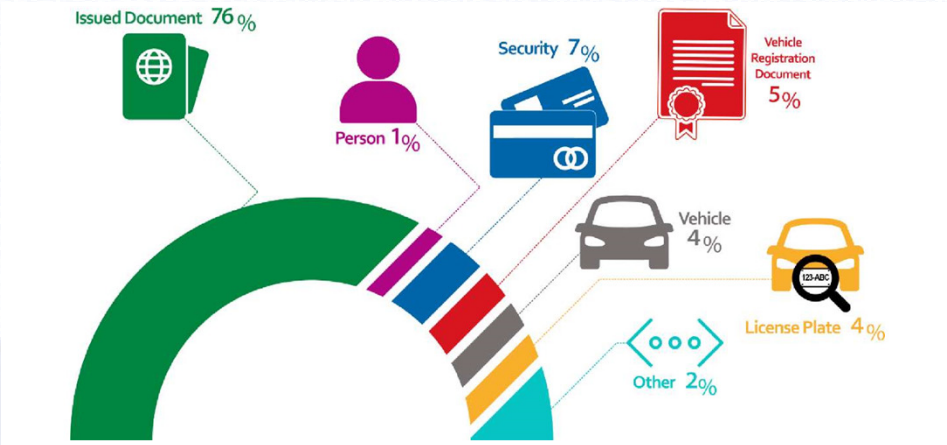

Figure 6. *Breakdown of alerts per category stored in SIS II as of Dec 31, 2020*[10]

The European Criminal Records Information System (ECRIS) was established and has been operational since April 2012. This decentralized system allows for the electronic exchange of criminal records between Member States. It allows criminal record authorities to obtain complete information on previous convictions of EU citizens from the Member State of which they are a national. ECRIS-TCN (Regulation (EU) 2019/816, European Commission, 2019), once established, will be a centralized system that allows Member State authorities to identify which other Member States have criminal records of third-country nationals or stateless persons being checked, so that they can then use the existing ECRIS system to solving problems related to the required information on convictions only in the identified Member States.

Improving ECRIS in terms of TCN is part of the European Security Agenda. The initiative is also a part of a new approach set by the European Commission towards border and security data management. Moreover, all centralized EU information systems for security, border management and migration should become interoperable with full respect for fundamental rights. The ECRIS-TCN System is scheduled to be ready in conjunction with the roll-out of the components required to implement interoperability.

The European Travel Information and Authorization System (ETIAS) is a system that allows pre-travel approval for visa-exempt travelers. Its key function is to verify that a third-country national qualifies for entry before traveling to the Schengen area. Information and access are provided through an internet application, before arriving at the border, which significantly increases the risk assessment of irregular migration, as well as the verification of public health risks before travel. The application for entry is processed according to the EU and relevant Interpol databases, and a special ETIAS watch list, in accordance with clearly defined rules.

The ETIAS will make it possible to identify persons who may pose a security risk before they reach the external Schengen border; and make available information to national law enforcement authorities and Europol, for the purpose of preventing, detecting or investigating terrorist offenses or other serious criminal offenses.

10 https://www.eulisa.europa.eu/Publications/Reports/SIS%20II%20-%202020%20Statistics%20-%20report.pdf

AUTOMATED EXCHANGE OF INFORMATION ON DNA, DACTYLOSCOPIC AND VEHICLE REGISTRATION DATA

There is identified need for improvement in relation to the challenges faced by Member States in the automated exchange of information on DNA, fingerprints and vehicle registration data (VRD), covered by the Prum Framework. According Council Decision 2008/615 automated exchange covers data search and comparison, hit notification or no hit and reference to data. The VRD exchange is fully automated, via EUCARIS applications. The analyzes conducted by Statewatch organization (Study on the Feasibility of Improving Information Exchange under the Prüm Decisions, European Commission, 2020) identified topics for improvement, including scope expansion Prum decisions, adoption of a common data format for data categories, and improving process efficiency and additional functions for exchanged data categories under Prum.

The issues to be considered relate to extending the scope of the Prum Framework to include searches to find missing persons or identify the dead in favor of those Member States, which are not permitted under applicable national law; analysis of current data exchange standards for biometric data sharing; and finding common standards based on best practices for future data exchange under Prum with perspective to future interoperability, Figure 7, and data portability across the EU, as well as further details for each main data type looking current access to exchange fingerprint images, DNA profiles and vehicle registration data within Prum, proposes solutions and recommendations for data improvement exchange and assess the impacts of such changes.

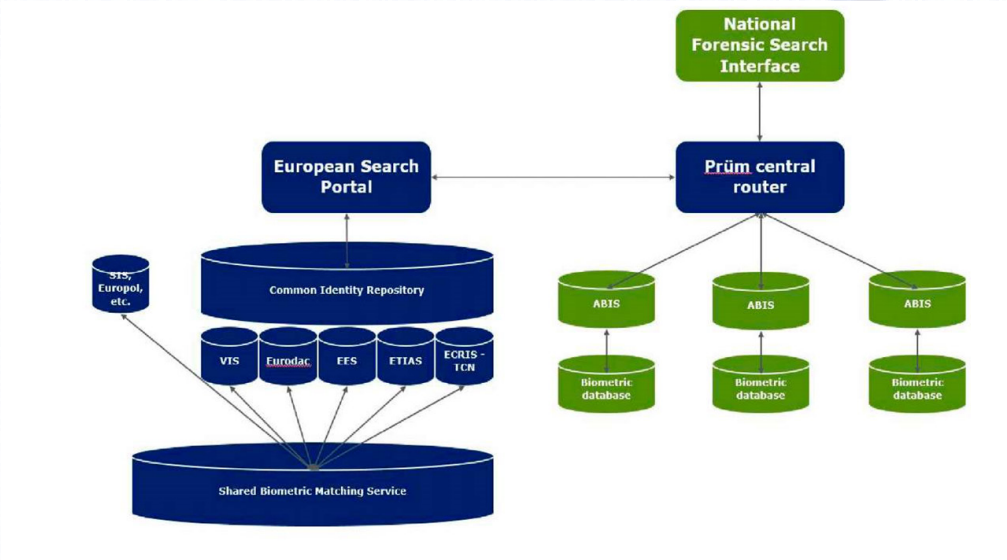

Figure 7. *Diagram of the IT architecture*[11]

The fingerprint efficiency improvements, related to the Automated Fingerprint Identification Systems (AFIS), which have been in use for over 30 years and have provided forensic law enforcement with an indispensable tool for identifying criminal suspects using both ten-print and latent fingerprint images. Fingerprint images for data exchange and adoption of AFIS platforms have been included in Prum for over 10 years and it is widely accepted that the sharing of data between Member States, for forensic fingerprint recognition, has been highly successful (Study on the Feasibility of Improving Information Exchange under the Prüm Decisions, European Commission, 2020).

11 https://www.statewatch.org/media/1386/eu-com-prum-expansion-technical-study-final-report-5-20.pdf

There is consequence if will be adopted a standardized image quality metric such as NFIQ2 across Prum and will impact the majority of Member States. The majority indicated they did not currently have a standard quality metric in place and those who did were based on NFIQ and would therefore need to be updated (Study on the Feasibility of Improving Information Exchange under the Prüm Decisions, European Commission, 2020).

To implement automated reporting of hit, it would be needed to update existing applications and systems to allow the sending of additional NIST container message. Provide automate sending the following up data based following confirmation of a hit or no-hit by a forensic user as well as handle the receipt of incoming data and storage within a database for future reporting and store within a level of national database.

To support priority-based requests will needed to implement systems that can schedule requests on their infrastructure based on the priority level assigned by requesting state.

Furthermore, the need to change their quota enforcement polices to restrict based on priority as well as provision of support to the transmission of vendor feature data was identified to include vendor specific templates in addition to raw images. Also, in particular the needs can be identified to conduct other changes in ICT infrastructure for provision of smooth operation.

Nevertheless, there still remain issues related to other biometric data that might cause need for national system adjustment.

Introducing an entirely new biometric data type introduces a range of requirements to adopt the technical and user skills of using a new type of technology. It might require significant investment in training of existing users would be required to cover the use of facial biometric systems, capability limitations etc. needs to seek to adopt new Standard Operating Procedures (SOP's) for the capture of facial images and provide necessary training to end users, enhance existing ICT infrastructure including increasing bandwidth (higher traffic and larger data sets) will result in quotas needing to be agreed.

The use of a fairly common type of data, such as facial images, in the limited scope of forensic criminal investigation within the Prum Framework would clearly distinguish this use came from other uses of facial recognition, such as real-time facial recognition for mass identification or identity verification in, e.g., border crossing situations. In particular processing facial images in this context would require the same deep and accurate scientific expertise through law enforcement forensic specialist, as is now the case with fingerprint and DNA analysis. Therefore, the concern that facial images would be lighter and likely to generate more "false positive results" than matching DNA and fingerprint data. Overall and based on the aforementioned, the transmission of facial images can be supported although there are some challenges.

In terms of search and adjudication process, no major changes are expected, as the two-step approach will be maintained. However, forensic experts would make use of the central ABIS, instead of using national systems. This would imply many forensic experts that should be trained and get familiar with the new ABIS technologies.

In terms of data, problems are expected to arise while trying to connect the central ABIS to every national database. Since biometric data have been collected and stored in different quality, the use of the ABIS with every database might be difficult. Any solution will be needed to accommodate for gallery images of varying quality and outline common quality metrics for communication (i.e. ESS for DNA, ICAO for faces, and NFIQ2 for fingerprint). Enforced restrictions based on quality might generate some issue due to potential loss of data (unusable lower quality data). From that point of view, it is

important that either the biometric image data stored at national level shall be converted in a readable format by the ABIS or the ABIS should be able to treat all the biometric data whatever the data format or quality. However, poor quality will result in poor matching results.

From the abovementioned we might conclude that what is in front of us are great challenges in order to achieve adequate level of interoperability.

SUMMARY

Due to the fact that coming with an ever-increasing range of uses and ever-evolving need accurate and reliable personal identification, the field of biometrics is evolving rapidly so this paper has been prepared to present recent developments and trends in the use of biometrics, particularly in large-scale IT systems being used for border control or law enforcement cooperation worldwide as well as identified needs for following it from the aspect of forensic science.

Nevertheless, two sides of the problem need to be considered: on the one hand, it will improve cooperation and efficiency between migration agencies, police forces and the judiciary. To others without adequate protection, it could become a dangerous remedy against fundamental rights, as centralization of databases could increase the risk of misuse of the system for purposes beyond its original intent.

Improve the current exchange of data: Although most forensic experts agree that the automated data exchange is currently working almost well, a few points for improvements have to been raised. The legal scope is considered to be not equivalent for all participant, the exchange standards have to be updated as existing might be considered as outdated and additional information could be made available to law enforcement officers (Study on the Feasibility of Improving Information Exchange under the Prüm Decisions, European Commission, 2020).

In the coming period, the "identity data" of citizens outside the EU biographical and biometric will be taken from five individual large databases and stored in a new system named as Common Identity Repositories (CIR). In accordance with its purpose, this will facilitate police identity checks, by providing a common set of biometric and biographical data on the vast majority of non-EU citizens present in the Schengen area. The increasing the ability to verify identity will indirectly affect and produce other open issues that need to be addressed.

The use of biometric data for identity verification is constantly increasing over the years. The national authorities responsible for verifying "whether the conditions for entry, stay or stay in the territory of the Member States are met" may search the VIS using the visa number and / or the fingerprints of the individual. Checks may be made to verify the identity of the person or to try to identify the person.

The possibilities of using CIR for identity verification are far wider. More specifically, when a person does not have a personal document, when there are "doubts" regarding the identity data provided by the person, to confirm the authenticity of the personal document or the identity of the document holder, or when the person has restrictions or refuses to cooperate.

If the identity check officer is authorized to access both CIR and VIS, and CIR and ETIAS, or both CIR and EES, the search will allow access to a larger set of individual identity data in the case of "hit".

Acknowledgement: Our sincere thanks to the Ministry of the Interior, the School of Electrical Engineering, the University of Belgrade and the University of Criminal Investigation and Police Studies, Belgrade for their contribution and providing persistent support.

REFERENCES

1. Biometrics in Large-Scale IT (2015). Recent trends, current performance capabilities, recommendations for the near future, European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA), 2015, https://www.eulisa.europa.eu/Publications/Reports/Biometrics%20in%20Large-Scale%20IT.pdf#search=The%20use%20of%20the%20Visa%20Information%20System%20for%20verification%20and%20identification%20within%20the%20Schengen%20area
2. Bunyan, T. (2018). Analysis The "point of no return" Interoperability morphs into the creation of a Big Brother centralized EU state database including all existing and future Justice and Home Affairs databases, Sitewatch, https://www.statewatch.org/media/documents/analyses/eu-interop-morphs-into-central-database.pdf
3. Casagran, B.C. (2021). Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU, Human Rights Law Review, 2021, 21, 433–457, doi: 10.1093/hrlr/ngaa057
4. Commission Implementing Decision (EU) 2019/327 of 25 February 2019 laying down measures for accessing the data in the Entry/Exit System (EES), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019D0327&qid=1571902694169
5. Commission Implementing Decision (EU) 2019/329 of 25 February 2019 laying down the specifications for the quality, resolution and use of fingerprints and facial image for biometric verification and identification in the Entry/Exit System (EES) C/2019/1280, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019D0329&qid=1571902694169
6. Commission Implementing Regulation (EU) 2021/1224 of 27 July 2021 concerning the detailed rules on the conditions for the operation of the web service and data protection and security rules applicable to the web service as well as measures for the development and technical implementation of the web service provided for by Regulation (EU) 2017/2226 of the European Parliament and of the Council and repealing Commission Implementing Decision C(2019)1230, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R1224&qid=1571902694169
7. Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32007D0533
8. Eurodac – 2020 statistics, European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), 2021, https://www.eulisa.europa.eu/Publications/Reports/Eurodac%20-%202020%20Statistics%20-%20Report.pdf
9. European Commission (2005) Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs. COM (2005) 597 final (24.11.2005), p. 3. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0597:FIN:EN:PDF

10. European Commission (2015) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Single Market Strategy for Europe {SWD(2015) 100 final}, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192
11. European Commission (2017) New European Interoperability Framework: Promoting seamless services and data flows for European public administrations, https://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_1&format=PDF
12. Głowacka, D., Youngs, R., Pintea, A. & Wołosik, E. (2021). Digital technologies as a means of repression and social control, Policy Department for External Relations, Directorate General for External Policies of the Union, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653636/EXPO_STU(2021)653636_EN.pdf
13. Gutheil, M., Liger, L., Eager, J., Oviosu, Y. & Bogdanovic, D. (2018). Interoperability of Justice and Home Affairs Information Systems, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, the Policy Department for Citizens' Rights and Constitutional Affairs, https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604947/IPOL_STU(2018)604947_EN.pdf
14. Interoperability: state of play, (2018). 7931/1/18 REV 1, Council of the European Union, https://www.statewatch.org/media/documents/news/2018/nov/eu-council-Interoperability-State-Of-Play-14193-18.pdf
15. Jones, C. (2020). Automated Suspicion the EU's new travel surveillance initiatives, Statewatch.org, https://www.statewatch.org/media/1235/sw-automated-suspicion-full.pdf
16. Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second-Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates, https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32006R1986
17. Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32006R1987
18. Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R2226
19. Report on the technical functioning of the Visa Information System (VIS) (2020). European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, eu-LISA
20. Report on the technical functioning of the Visa Information System (VIS), European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, 2020, https://www.eulisa.europa.eu/Publications/Reports/2019%20VIS%20Report.pdf
21. SIS II – 2020 statistics, (2021). eu-Lisa, https://www.eulisa.europa.eu/Publications/Reports/SIS%20II%20-%202020%20Statistics%20-%20report.pdf
22. Study on the Feasibility of Improving Information Exchange under the Prüm Decisions, Written by Deloitte Consulting & Advisory CVBA (2020). European Commission, Directorate / General

for Migration and Home Affairs, https://www.statewatch.org/media/1386/eu-com-prum-expansion-technical-study-final-report-5-20.pdf

23. Study on the Feasibility of Improving Information Exchange under the Prüm Decisions, Study, Deloitte Consulting & Advisory CVBA, European Commission, 2020, https://www.statewatch.org/media/1386/eu-com-prum-expansion-technical-study-final-report-5-20.pdf
24. Vavoula, Niovi, The 'Puzzle' of EU Large-Scale Information Systems for Third-Country Nationals: Surveillance of Movement and Its Challenges for Privacy and Personal Data Protection (October 9, 2019). Forthcoming, European Law Review, Available at SSRN: https://ssrn.com/abstract=3466766
25. Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralized system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726 PE/88/2018/REV/1, EUR-Lex - 32019R0816 - EN - EUR-Lex (europa.eu)