Interoperability of EU information systems – a tool to fight terrorism and serious cross-border crime (Part II)

retired lieutenant colonel dr Edyta Kot[1]

[1] Former affiliation: Central Forensic Laboratory of the Police

Abstract

A key element of the counter-terrorism strategy is to protect citizens from terrorist attacks and to level the consequences of such attacks. This is possible by improving border security, transportation and cross-border infrastructure. No less important part of the strategy is the prosecution of terrorists, especially those with an international dimension. EU member states in favour of thwarting terrorists have the tools to share information, intelligence, threat analysis and strengthen operational law enforcement cooperation. The European Union has also developed legal and organisational instruments to assist in the fight against terrorism and organized cross-border crime[2].

Keywords: Eurodac, Entry/Exit, ECRIS-TCN, interoperability, large-scale systems

Border security can be improved by introducing biometrics into the large-scale systems already described in the first part of the publication, namely the Visa Information System (VIS), the Schengen Information System (SIS), as well as the Eurodac, Entry/Exit and ECRIS-TCN systems, which are described in this part of the publication.

Over the past few years, situations of illegal border crossings have become increasingly common in the European Union. Checks on people at the EU's external borders should be made more effective, in order to enable, among other things, effective management of migrant traffic. With this in mind, there is a need to combine and comprehensively strengthen the EU's IT tools for managing external borders and preventing and combating illegal migration. The article addresses the issue of ensuring interoperability of all centralized information systems operating in the EU's area of freedom, security and justice.

Eurodac system (European Dactiloscopie)

In an effort to standardize national asylum policies and provide adequate protection for refugees, European Union member states signed a convention in Dublin on June 15, 1990,that determined the state responsible for processing an asylum application filed in a Union member state. The agreement, called the Dublin Convention, came into force in twelve countries on September 1 1997, in Austria and Sweden on October 1, 1997, and in Finland on January 1, 1998[3]. With this in mind, Council Regulation (EC) No. 2725/2000 of December 11, 2000 established the Eurodac system for the comparison of fingerprints for the effective application of the Convention[4]. The Dublin Convention mainly regulated the criteria for determining the state responsible for processing an asylum application, defined the means of exchanging information and the rules for transferring an application to another state. In addition, it aimed to ensure that the application of any person seeking

[2] EU *Counter-Terrorism* Strategy, http://register.consilium.europa.eu/doc/srv?l=PL&f= ST% 2014469%202005%20REV%204.

[3] https://encyklopedia.interia.pl/slownik-ue/news-konwencja-dublinska,nId,2112521

[4] Council Regulation (EC) No. 2725/2000 of December 11, 2000 *concerning the establishment of the "Eurodac" system for the comparison of fingerprints for the effective application of the Dublin Convention,* (OJ L 316, 15.12.2000), https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:32000R2725.

asylum in the European Union would be processed by one of the member states[5]. The Dublin Convention was replaced by Council Regulation (EC) No. 343/2003 of February 18, 2003. *establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national*[6]*,* also known as Dublin II. The current legal act concerning the common asylum policy of the Member States is Regulation (EC) No 604/2013 of the European Parliament and of the Council of 26 June 2013 *on the establishment of criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person*[7]*.*

In order to facilitate the application of the Dublin Convention, an ICT system for comparing fingerprint data called Eurodac has been developed. It allows EU member states to identify asylum seekers (under current EU law, the term "asylum" has been replaced by "international protection"), as well as persons illegally crossing the external borders of the European Union, and makes it possible to determine whether a foreigner illegally residing on the territory of one of the EU member states has not previously applied in another country for refugee status[8]. The Eurodac system makes it possible to determine the member state responsible for processing an application for international protection submitted by a third-country national or stateless person. In addition, the provisions of the current Regulation (EU) No. 603/2013 of the European Parliament and of the Council on the *establishment of Eurodac for the comparison of fingerprints for the effective application of Regulation (EU) No. 604/2013 on the establishment of criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requesting comparisons with Eurodac data by law enforcement authorities of the Member States and Europol for law enforcement purposes, and amending Regulation (EU) No. 1077/2011 establishing a European Agency for* the operational management of large-scale information systems in the area of freedom, security and justice. *Operational Management of Large-Scale Information Systems in the Area of Freedom, Security and Justice*[9] allow comparison of fingerprint data for law enforcement purposes. According to this regulation, the term "law enforcement" means the prevention, detection or prosecution of terrorist crimes or other serious crimes[10]. This means that the Eurodac system, which has served until now, improving asylum policy, has gained a new functionality of searching the database for fingerprint information of potential terrorists or criminals [D. Jaroszewska-Choraś, 2016]. Inextricably linked to this term are the terms "terrorist crime" meaning offenses defined in national law that correspond or are equivalent to the offenses referred to in Directive 2017/541 of the European Parliament and of the Council[11], and "serious crimes" meaning forms of crime that correspond or are equivalent to those referred to in Framework Decision 2002/584/JHA, if they are punishable under national law by deprivation of liberty or a protective measure involving deprivation of liberty for a maximum period of at least three years[12].

The architecture of the Eurodac system consists of a computerized central fingerprint database, called the "central system", which includes a central unit. The second important component of the system, is the communications infrastructure between the central system and the member states, providing an encrypted virtual network to transmit Eurodac data. This network isTESTA-ng[13].

The central system records, among other things, fingerprint data, the Member State of origin, the place

[5] https://encyklopedia.interia.pl/slownik-ue/news-system--dublinski, nId,2112880

[6] Council Regulation (EC) No. 343/2003 of February 18, 2003 *establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national,* [OJ. L50 of 25.2.2003].

[7] Regulation (EC) No. 604/2013 of the European Parliament and of the Council of 26 June 2013 *on the establishment of criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person,* [OJ L 180/31, 29.06.2013].

[8] https://odoserwis.pl/p/306/europejski-zautomatyzowany-system-rozpoznawania- prints-fingerprints-eurodac.

[9] Regulation (EU) No 603/2013 of the European Parliament and of the Council of June 26, 2013. on the *establishment of the Eurodac system...*, [OJ EU L 180, 29.06.2013].

[10] Ibid.

[11] Directive (EU) 2017/541 of the European Parliament and of the Council of March 15, 2017 *on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA* [Official Journal of the EU L 88 of 31.03.2017].

[12] Council Framework Decision 2002/584/JHA of June 13, 2002 *on the European arrest warrant and the surrender procedures between Member States, their detection or prosecution,* [Official Journal of the EU *L 190 of 18.07.2002].*

[13] Regulation (EU) No 603/2013 of the European Parliament and of the Council of June 26, 2013. on the*establishment of the Eurodac system...*, [EU OJ L 180/1, 29.06.2013].

and date of the application for international protection, the date of the application (the date entered by the Member State that transferred the applicant), gender, the reference number used by the Member State of origin, the date the fingerprints were taken, the date the data were sent to the central system, the operator's identification number, the date the person arrived after the successful transfer, the date of the decision to process the application, the date the person left the territory of the Member States or the date the person was removed from the territory of the Member States[14].

The Eurodac system has been in operation since January 15, 2003. Poland joined its activities on May 1, 2004, with its accession to the European Union. The first upgrade of the Eurodac interface (module) was carried out in 2015 and was caused by the entry into force on July 20, 2015 of Regulation (EU) No. 603/2013 of the European Parliament and of the Council of June 26, 2013[15] and the need to adapt the system to the requirements arising from the implementation of new functionalities.

According to the aforementioned regulation, all Member States are obliged to immediately download and transmit fingerprint data of any applicant for international protection and any third-country national or stateless person apprehended in connection with the illegal crossing of a Member State's external border. This data, in the form of fingerprint prints (fingerprint data), is collected and recorded in the Eurodac system from individuals at least 14 years of age[16]. Immediacy in this case means that each member state is obliged to take fingerprints from the above-mentioned persons and send them, along with reference data, to Eurodac within 72 hours of the foreigner's application for international protection. In the case of serious technical problems, Member States may extend the 72-hour transmission deadline by a maximum of another 48 hours. Such the same time applies when, due to the condition of the fingertips, fingerprints of sufficient quality cannot be taken.

Three categories of people are registered in Eurodac, namely[17]:

- applicants for international protection (category 1),
- third-country nationals or stateless persons apprehended in connection with the illegal crossing of the external border (category 2),
- third-country nationals or stateless persons residing illegally in a member state (category 3).

Data relating to persons shall be deleted from the central system, before the expiration of the retention period, if the Member State of origin receives information that a foreigner has acquired citizenship of any of the Member States of the European Union.

A new functionality of Eurodac is the ability to conduct comparisons of fingerprint data with data stored in the Eurodac central system for law enforcement purposes, these are so-called comparisons of category 4 data and category 5 data – data processed by Europol.

In 2015. The European Parliament and the EU Council established the Eurodac Regulation, which forced the adaptation of Polish law to the requirements of the aforementioned regulation. The group includes:

a) Agreement dated March 11, 2015 between the Chief of Police, the Chief of Border Guard, the Head of the Internal Security Agency, the Head of the Central Anti-Corruption Bureau and the Central Forensic Laboratory of the Police *regarding the implementation of Regulation (EU) No. 603/2013 of the European Parliament and of the Council of 26.06.2013 with regard to the comparison of fingerprint data with data stored in the Eurodac central system for law enforcement purposes*,
b) Agreement of June 1, 2015 between the Chief of Police, the Chief of Border Guard, the Head of the Office for Foreigners, the Refugee Board and the Central Forensic Laboratory of the Police *regarding mutual cooperation and coordination of activities in the implementation of the provisions of Regulation (EU) No. 603/2013 of the European Parliament and of the Council with regard to administrative proceedings conducted in cases of foreigners*,
c) Order of the Chief of Police No. 23 dated 16.07.2015 *on the procedure for sending requests for comparison of fingerprint data with Eurodac* data (Official Gazette of 20.07.2015, item 56).

Entry/Exit System (EES)

In February 2013. The European Commission proposed aRegulation of the European Parliament and of the Council amending Regulation (EC) No. 562/2006 in connection with the application of the Entry/Exit System (EES) and the Registered Traveller Program (RTP)[18].

[14] Ibid.

[15] OJ. EU L 180/1 of 29.06.2013.

[16] Regulation (EU) No 603/2013 of the European Parliament and of the Council of June 26, 2013. on the *establishment of the Eurodac system*..., [OJ EU L 180/1, 29.06.2013].

[17] Ibid.

[18] Regulation (EC) No. 562/2006 of the European Parliament and of the Council of March 15, 2006 *establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code),* [OJ EU L 105, 13.04.2006].

The requested changes were necessary for the establishment of theEntry/Exit System (Entry/Exit System – EES) and the Registered Traveler Program (RTP), forming the "Smart Borders" (Smart Borders) package. In 2015, the eu – Lisa agency withdrew the RTP project due to the high complexity of implementing the system in all member states and the high cost of technical implementation of the projected system.

In order to prevent, detect and investigate terrorist or other serious crimes, the European Commission has established an entry/exit system. The system was adopted with a view to more effective management of the external borders and to verify compliance with regulations on the permitted period of stay in the territory of member states. The Entry/Exit system electronically records the time and place of entry and exit of third-country nationals with a short-term residence permit on the territory of European Union member states. In addition, the system calculates the period of permitted stay of a third-country national on the territory of the Union and should replace the procedure of mandatory stamping of passports of third-country nationals. The legal basis for the establishment of the EES is Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 *establishing an entry/exit system (EES) for the recording of data on the entry and exit of third-country nationals crossing the external borders of the Member States and data on the refusal of entry in respect of such nationals, 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*

According to the EES regulation, the term "dactyloscopic data" means "data on the prints of the four fingers of the right hand: index, middle, heart and little hand, if any,and otherwise of the left hand".[19].

The Entry/Exit system consists of[20]:

- central system,
- a uniform national interface in each member state to connect the central system to the national border infrastructure in member states,
- a secure communication channel between the central EES system and the central VIS system,
- a secure, encrypted communications infrastructure between the EES central system and uniform national interfaces, and a a network service that provides third-country nationals with an "OK/NOT OK" response,
- a data repository, established at the central level, containing data solely for the purpose of producing reports and statistics, without individual identification.

The key body of the system in question is eu – LISA. The agency is responsible for establishing a secure communication channel between the EES central system and the VIS central system to enable interoperability between these systems. Interoperability allows border services using the EES to view the VIS from within the EES.

Border services or immigration authorities are authorized to conduct searches using fingerprint data or combined fingerprint data with a facial image for the sole purpose of identifying a third-country national. If a search by the aforementioned data reveals that the data on a third-country national is not registered in the EES, the data in the VIS is accessed for identification. In the event that the use of fingerprints of the third-country national in question is not possible, or if the search using fingerprint data or fingerprint data combined with a facial image fails, then the check is carried out using all or selected alphanumeric data, namely: surname, forename or forenames, date of birth, nationality or nationalities, gender, type and number of travel document and three-letter code of the country issuing the travel document, expiration date of the travel document[21].

Under the EES system, any third-country national crossing the external borders of the European Union will be subject to registration of entry and exit data[J. Niklas, 2012]. The entry/exit system will modernize the management of external borders by increasing the quality and efficiency of their control. The construction of the new system is being carried out by eu – LISA and individual member states, and should culminate in the commissioning of the finished system by 2022.[22]

ECRIS-TCN

The ECRIS system was launched in April 2012 and is used to exchange information on convictions handed down in the EU. Each member state stores and exchanges information on its citizens. The operation of ECRIS is governed by Council Framework Decision 2009/315/JHA of February 26, 2009 onthe *organisation and content of the exchange of information extracted from the criminal record between Member States*[23]. Article 11 of this decision sets out the format and rules for

[19] Ibid.

[20] Ibid.

[21] OJ. L 327 of 09.12.2017.

[22] https://www.schengenvisainfo.com/entry-exit-system-ees

[23] Official Journal of the EU L 93 of 07.04.2009.

organizing the exchange of information on convictions between the central authorities of the Member States. The above article has been incorporated into Council Decision 2009/316/JHA of April 6, 2009 *on the establishment of the European Criminal Records Information System (ECRIS),* which implements Decision 2009/315/JHA[24].

ECRIS is an information system with a decentralized structure. It is based on criminal records databases maintained in each member state. The ECRIS system consists of the following components[25]:

a) software that allows the exchange of information between criminal records databases of member states,
b) a common communications infrastructure based on an encrypted network.

Since 2012, there has been a sharp increase in the amount of information exchanged between member states. From 300,000 in 2012, 863,000 in 2013, 1,257,000 in 2014, 1,812,000 in 2015, 1,978,000 in 2016, 2,574,000 in 2017, 2,964,000 in 2018 to 4,179,000 in 2019, an average of 348,000 exchanged per month[26].

Europe is currently struggling with a migration problem. Foreigners who come to Europe from outside the European Union, often commit crimes and are convicted in the country. Under the current rules, information on convictions of third-country nationals residing in the EU is not collected in the Member State of nationality, but is stored in the various Member States where individual convictions were handed down. The only effective way to obtain full information about a third-country national's previous criminal record is to send out a request for information on his criminal record to of all member states.

In 2017. The European Commission submitted a proposal for a regulation to establish a centralized ECRIS – TCN system, which, like other large-scale systems, will be managed by the EU Agency for Large-Scale Information Systems (eu – LISA). The system in question is currently under construction and is expected to be operational in 2022. The legal basis for the establishment of the ECRIS – TCN system is the Ro Regulation of th-eEuropean Parliament and of the Council (EU) 2019/816 of April 17, 2019 *establishing a centralized system for the identification of Member States holding information on convictions of third-country nationals and stateless persons (ECRIS-TCN) for the purpose of supplementing the European Criminal Records Information System and amending Regulation (EU) 2018/1726*[27]. According to this Regulation, ECRIS-TCN should contain information on the identity of third-country nationals convicted by criminal courts within the EU. The scope of information collected in the system should include alphanumeric data, fingerprint data and facial images, if the legislation of the Member State of conviction allows it[28].

The ECRIS-TCN system consists of[29]:

a) central system, in which information on the identity of convicted third-country nationals is collected and processed,
b) national central access point located in each member state,
c) interface to connect competent authorities to the central system through central access points and communication infrastructure,
d) communication infrastructure between the central system and national central access points.

The central system in technical terms is managed by eu-LISA. In terms of content, the central system is operated by the central authority of the Member State that issued the conviction against the third-country national[30]. This authority makes entries in the central system to the extent described below[31]:

a) alphanumeric data, i.e.: surname (family name), forenames (given names), date and place of birth (city and state), nationalities, gender, previous names, conviction code. In addition, additional optional information can be entered into the register, i.e. parents' names, identification number or type and number of identity document and name of issuing authority, nicknames, nicknames.

[24] Official Journal of the EU L 93 of 07.04.2009.

[25] Official Journal of the EU L 93 of 07.04.2009.

[26] Report from the Commission to the European Parliament and the Council *concerning the exchange through the European Criminal Records Information System (ECRIS) of information extracted from criminal records between the Member States*,https://ec.europa.eu/info/sites/info/files/1_en_act.pdf.

[27] OJ EU L135, 22.05.2019.

[28] Ibid.

[29] Regulation of the European Parliament and of the Council (EU) 2019/816 of April 17, 2019 *establishing a centralized system to identify Member States holding information on convictions of third-country nationals and stateless persons (ECRIS-TCN) for the purpose of completing the European Criminal Records Information System and amending Regulation (EU) 2018/1726*, [OJ. EU L 135 of 22.05.2019].

[30] Regulation of the European Parliament and of the Council (EU) 2019/816 of April 17, 2019 *establishing a centralized system to identify Member States holding information on convictions of third-country nationals and stateless persons (ECRIS-TCN) for the purpose of completing the European Criminal Records Information System and amending Regulation (EU) 2018/1726*, [OJ. EU L135 of 22.05.2019].

[31] Ibid.

b) fingerprint data, i.e.: fingerprint data collected in accordance with national law in the framework of criminal proceedings, at least fingerprint data collected in the case of a third-country national with a prison sentence of at least 6 months or convicted of an offense that is punishable under the law of a Member State by a maximum term of imprisonment of at least 12 months.

Fingerprint data entered into the system must comply with technical specifications in terms of quality, resolution and file storage format. The fingerprint data reference number of the convicted person must include the code of the convicting member state. In addition, the entries posted in the system may include facial images of a convicted third-country national if the convicting country's legislation permits the collection and processing of facial images of convicted persons[32].

According to Justice, Consumers and Gender Equality Commissioner Věra Jourova, "The new system will enable law enforcement agencies to more quickly and easily identify third-country nationals who have previously been convicted in the EU through a simple search in ECRIS. This will contribute to improved police and judicial cooperation for a more effective fight against crime and terrorism across the EU and will ultimately make Europe a safer place for all citizens".[33].

The main advantage of the ECRIS – TCN system will be the ease of access by authorized authorities. The database will be available on the Internet by searching on a "result/no result" basis. In the event of a hit, the member states from which the criminal record information of a person of interest to the authority can be obtained will be indicated. In addition, the system will include dactyloscopic data (fingerprints) and possibly a facial image, in addition to alphanumeric identity information. The ECRIS-TCN system will be used for criminal investigations and, among other things, for background checks on individuals who are expected to work with children or who apply for firearms licenses[34].

Interoperability of EU information systems

In terms of organisation, the functioning EU information systems used by member states to fight crime, control borders and manage the flow of migrants are not interconnected. This results in repeatedly sending requests to the various systems and waiting for responses, which often come back with long delays. Such a solution may lead to information gaps[35]. In order to enable EU information systems to complement each other, to facilitate the identification of individuals and unidentified human remains, and to enable the fight against identity fraud, member states have begun implementing interoperability of EU information systems.

The interoperability framework covered large-scale information systems, namely. SIS, VIS, ECRIS-TCN, Entry/Exit, Eurodac, ETIAS. In 2019, the European Council adopted two regulations establishing the scope of interoperability between EU information systems in the field of justice and home affairs. The group includes:

a) Regulation (EU) No. 2019/817 of the European Parliament and of the Council of 20 May 2019 *on establishing an interoperability framework for EU information systems in the area of borders and visa policy and amending Regulations (EC) No. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726, (EU) 2018/1861 and Council Decisions 2004/512/EC and 2008/633/JHA*[36];

b) Regulation (EU) No 2019/818 of the European Parliament and of the Council of 20 May 2019 *on establishing an interoperability framework for EU information systems in the areas of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816*[37].

Improving the flow of information between member states in the area of interoperability will be possible through the creation and implementation of new tools, namely[38]:

- european search portal,
- a common biometric comparison system,
- a common repository of identification data,
- multiple identity detector.

Reliable identification of individuals is done by comparing biometric data, such as fingerprint mappings, facial images or DNA profiles.

In functioning systems, fingerprint and palm print data are most commonly used to identify individuals. Currently, these systems are dispersed, i.e. each functions separately and is used for different services. Work is underway at the EU level to establish a common system for comparing biometric data, including fingerprint

[32] Ibid.

[33] https://ec.europa.eu/poland/news/190409_security_pl

[34] Ibid.

[35] https://www.consilium.europa.eu/pl/press/press-releases/2019/05/14/interoperability-between-eu-information-systems-council-adopts-regulations/

[36] Official Journal of the EU L 2019. 135.27 of 22.05.2019.

[37] Official Journal of the EU L 2019. 135.85 of 22.05.2019.

[38] Official Journal of the EU L 2019. 135.27 of 22.05.2019, para. 9.

data, to identify individuals who are currently registered in different databases. Law enforcement and justice authorities have no knowledge of which system processes the fingerprint data of persons of interest to them. This causes delays and undermines the effectiveness of ongoing investigations. The idea behind interoperability is to improve the activities of authorities responsible for preventing and detecting crimes, including terrorist crimes, by accessing information stored in any of the EU information systems.

The above systems will be accessed through the already mentioned European search portal, which will consist of[39]:

a) central infrastructure including a search portal that allows simultaneous consultation of EES, VIS, ETIAS, Eurodac, SIS, ECRIS – TCN and Europol and Interpol data,
b) a secure communication channel between the European search portal and the member states and EU agencies authorized to use the European search portal,
c) secure communications infrastructure between the European search portal and the aforementioned systems and databases, as well as between the European search portal and the central infrastructure of the common identification data repository and the multiple identities detector.

The European search portal will be responsible for delivering query results quickly and transparently. The above will be possible through simultaneous data retrieval in different systems using alphanumeric or biometric data. The user will not perform individual searches and receive separate results from all systems. The new data processing functionality will involve storing data in a common repository, which is a common component of the EES, VIS, ETIAS, Eurodac, ECRIS – TCN systems. To support the operation of the common data repository in carrying out reliable verification of the identity of individuals whose data is collected in different systems. Data processing through the European search portal and common biometric comparison system is limited to detecting multiple identities. By design, the above will occur when new data is added to one of the systems that are part of the common data repository or to the SIS. In addition, a common biometric matching system will support the multiple identities detector and meet the objectives of the EES, VIS, Eurodac, SIS, ECRIS – TCN systems.

Law enforcement agencies, such as the Police, will be able to send queries to the common data repository in the following cases:

a) "when the police authority is unable to identify a person due to the lack of a travel document or other reliable document proving the person's identity
b) when there are doubts about the identity data provided by a person,
c) when there are doubts about the authenticity of a travel document or other reliable document presented by a person,
d) when there is doubt about the identity of the holder of a travel document or other reliable document,
e) when a person is unable or refuses to cooperate. Making such inquiries is not permitted with respect to minors under the age of 12, unless it is done for the benefit of the child". [40].

According to Article 22 of the Regulation, designated authorities of Member States and Europol will be able to carry out checks on EU information systems for the purpose of preventing and detecting terrorist or other serious crimes, as well as for investigating them. Especially in a situation where it is suspected that the data of the perpetrator or victim of a terrorist or other serious crime is stored in EES, VIS or ETIAS.

There is now a huge amount of information being processed, and the answer to the question "will data from different sources be merged or not?" remains a matter of legal and organisational constraints. Technological developments are fostering efforts to ensure the interoperability of information systems. This will enable designated authorities to access specific information quickly and in a controlled manner. The continuing threat of terrorism in Europe and around the world, as well as the growing phenomenon of migration in Europe, pose serious challenges for the Schengen area [A. Gajda, 2019]. The implementation and maintenance of smoothly functioning instruments for the exchange of information between authorized authorities is essential to ensure an adequate level of internal security in the Schengen member states [A. Gajda, 2019].

Article 56 of the regulation sets out the obligations of member states to conduct information exchange, including fingerprint data. As part of interoperability, each EU member state will be required to connect

[39] Regulation (EU) No. 2019/817 of the European Parliament and of the Council of 20 May 2019 *on establishing a framework for interoperability of EU information systems in the area of borders...*, Article 6, [Official Journal of the EU L 2019. 135.27 of 22 May 2019].

[40] Regulation (EU) No. 2019/817 of the European Parliament and of the Council of 20 May 2019 *on establishing a framework for interoperability of EU information systems in the field of borders...*, Article 20, [Official Journal of the EU L 2019. 135.27, 22 May 2019].

to a European search portal and a common data repository, as well as to integrate functioning national systems and infrastructure with the aforementioned interoperability elements and the multiple identities detector. In addition, member states will be responsible for implementing legislative measures under which designated authorities will be authorized to query the common data repository. The legislative measures adopted will define the objectives of identification for the purposes of Article 2(1)(b) and (c) "preventing and combating illegal immigration", "ensuring a high level of security within the area of freedom, security and justice of the European Union, including the maintenance of public safety and public policy and guaranteeing security in the territories of the Member States".[41]. In addition to technical and legislative issues, the issue of the organisation of the information exchange process is extremely important, with a particular focus on conducting manual verification of search results, both on the basis of alphanumeric data and biometric data. The body responsible for verifying the differing identities is the SIRENE Bureau.

Currently, the fully functioning systems that process fingerprint data are SIS, Eurodac and VIS. The process of collecting and processing this data is carried out in accordance with applicable national laws. Many member states, including Poland, are working to prepare for the implementation of interoperability of large-scale EU information systems. At the EU level, this work is overseen by eu-LISA. The European Parliament and the Council of the EU are making changes to the operation of the European Union's large-scale systems through regulations. The Polish administration faces a major challenge in adapting national institutions and information systems to changes in the functioning of large-scale EU systems.

It is currently focused on operating the SIS, VIS, Eurodac systems in operation. A key role in the implementation of the cooperation of Polish institutions with SIS and VIS is played by the National Information System, in particular the Central Technical Body located in the KGP[42].

The body responsible for the N.SIS II national system is the COT KSI, whose tasks include[43]:

a) creation, launch, technical operation and maintenance of the KSI;
b) ensure the smooth operation and security of the Schengen Information System within the N SIS II national system.

The SIRENE Bureau, mentioned earlier, also operates within the Police structure (Article 7(2) of *Council Decision 2007/533/JHA* and Article 35 of the *Law on Participation of the Republic of Poland in SIS and VIS)*. The Bureau's primary tasks include the exchange of supplementary information, which is necessary for the entry of alerts and to enable appropriate action to be taken in the event of a hit in SIS II. This is in accordance with the guidelines in the SIRENEHandbook[44]. The SIRENE office is the only 365/7/24 point of contact operating in each of the Schengen countries.

Each member country also has a National Interpol Bureau (NBI), which is tasked with maintaining contacts and acting as an intermediary between the country's law enforcement agencies and the National Interpol Bureaus of other member countries and the Interpol General Secretariat. The police organisational unit that performs the tasks of the Polish National Bureau is the Chief of Police, and in practice it is the Office of International Police Cooperation. Currently, through the SPP*(Police Search System*) tool, police officers have access to Interpol's databases for wanted and missing persons. Interpol data is also accessed at the front line of border control in an IT system operated by Border Guard officers.

The new EU regulations introduce changes that will alter the organisation of the existing model for the operation of large-scale systems in Poland. The new organisational framework will address two areas, namely:

1. in the case of the systems currently in operation (SIS II, VIS and Eurodac), the changes will concern the modernisation of the systems in production so that there are no problems with operational cooperation with the systems of Polish institutions,
2. in the case of the EES, ETIAS and ECRIS-TCN systems, new functionalities will be implemented, to which Polish institutions will be attached.

The implementation of the new EES, ETIAS, ECRIS-TCN systems, the expansion of the functionality of SIS, VIS and Eurodac, as well as the results of

[41] Regulation (EU) No. 2019/817 of the European Parliament and of the Council of 20 May 2019 *on establishing a framework for the interoperability of EU information systems in the field of borders...,* Article 2 (1), [Official Journal of the EU L 2019. 135.27 of 22 May 2019.

[42] Act on the participation of the Republic of Poland in SIS and VIS, art. 2 item 11, [Dz. U. 2007 no. 165 item 1170].

[43] Ibid, Articles 26–34.

[44] Commission Implementing Decision (EU) 2017/1528 of August 31, 2017 replacing the Annex to Commission Implementing Decision 2013/115/EU *adopting the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II),* [Official Journal of the EU L 231/6, 07.09.2017].

the "Interoperability" project, will require the creation of new rules for the organisation of the process in Poland. With the above in mind, the new organisational framework for the cooperation of Polish institutions with large-scale EU systems assumes the division of tasks of the Central Technical Body, namely:

1. for the tasks of the COT in the area of cooperation with SIS, VIS and Eurodac, should be the responsibility of the Chief of Police;
2. for the tasks of the COT in the area of cooperation with ECRIS – TCN, should be the responsibility of the head of the designated unit in the Ministry of Justice;
3. the tasks of the COT related to the functioning of the EES system in Poland (on the external borders of the EU), and the cooperation of Polish institutions with the ETIAS system should be the responsibility of the Commander-in-Chief of the Border Guard.

Such a dispersed model can generate technical problems related to the integration of individual systems, as well as legislative problems related to the amendment of existing legislation, the development of new legislation, and the conclusion of cooperation agreements within different institutions, such as the Police and Border Guard.

Conclusions

Implementing interoperability will involve large-scale efforts on both organisational and legislative issues. Organisationally, interoperability will affect the operations of the Police Department, especially the Police Central Forensic Laboratory. A novelty arising from the requirements of implementing interoperability of information systems is the verification of positive search results for SIS, or ECRIS – TCN, which will be performed by experts or fingerprint specialists from CLKP. The fulfillment of tasks related to the handling of international inquiries resulting from the implementation of system interoperability prompts the centralisation of systems that process biometric data, including fingerprint data. Currently, the existing systems do not work together. Therefore, a European search portal, a common biometric matching service, a common identity repository and an identity multiplication detection module were proposed as interoperability tools.

REFERENCES

1. Gajda, A. (2019). Interoperacyjność unijnych systemów informacyjnych w zakresie bezpieczeństwa, ochrony granic i zarządzania migracjami (Interoperability of EU information systems for security, border protection and migration management). *Kwartalnik Kolegium Ekonomiczno-Społecznego "Studia i Prace", 1*(37).
2. Jaroszewska – Choraś, D. (2016). *Biometria. Aspekty prawne* (*Biometrics. Legal Aspects)*. Wydawnictwo Uniwersytetu Gdańskiego.
3. Niklas, J. (2012). *Inteligentne granice Unii Europejskiej (Smart Borders – European Union)*. https://panoptykon.org/wiadomosc/ inteligentne -granice-unii-europejskiej, 2012.
4. Report from the Commission to the European Parliament and the Council concerning the exchange through the European Criminal Records Information System (ECRIS) of information extracted from criminal records between the Member States, https://ec.europa.eu/info/sites/info/files/1_en_act.pdf.
5. EU Counter-Terrorism Strategy, http://register.consilium.europa.eu/doc/srv?l=PL&f= ST%2014469%202005%20REV%204.

Legal acts

1. Council Framework Decision 2002/584/JHA of June 13, 2002 on the European arrest warrant and the surrender procedures between Member States, their detection or prosecution, Official Journal of the EU L 190 of 18.07.2002.
2. Commission Implementing Decision (EU) 2017/1528 of August 31, 2017 replacing the Annex to Commission Implementing Decision 2013/115/EU on the adoption of the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II), OJ L 231/6, 07.09.2017.
3. Directive (EU) 2017/541 of the European Parliament and of the Council of March 15, 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, Official Journal of the EU L 88 of 31.03.2017.
4. Council Regulation (EC) No. 2725/2000 of December 11, 2000 concerning the establishment of the "Eurodac" system for comparing fingerprints for the effective application of the Dublin Convention, OJ. L 316, 15.12.2000, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:32000R2725.
5. Council Regulation (EC) No. 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national, OJ. L 50 of 25.2.2003.
6. Regulation (EC) No. 562/2006 of the European Parliament and of the Council of March 15, 2006

establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code), OJ. EU L 105 of 13.04.2006.

7. Regulation (EC) No. 604/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person, OJ. L 180/31 of 29.06.2013.
8. Regulation (EU) No. 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of Eurodac for the comparison of fingerprints for the effective application of Regulation (EU) No. 604/2013 on the establishment of criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in a Member State by a national third country or stateless person and on requesting comparisons with Eurodac data by law enforcement authorities of Member States and Europol for law enforcement purposes, and amending Regulation (EU) No. 1077/2011 establishing a European Agency for the operational management of large-scale information systems in the area of freedom, security and justice, OJ EU L 180, 29.06.2013.
9. Regulation (EU) 2017/2226 of the European Parliament and of the Council of November 30, 2017 establishing an entry/exit system (EES) for recording data on the entry and exit of third-country nationals crossing the external borders of the Member States and data on refusal of entry in respect of such nationals, and laying down 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, OJ. EU L 327 of 09.12.2017.
10. Regulation of the European Parliament and of the Council (EU) 2019/816 of April 17, 2019 establishing a centralized system to identify Member States holding information on convictions of third-country nationals and stateless persons (ECRIS-TCN) for the purpose of supplementing the European Criminal Records Information System and amending Regulation (EU) 2018/1726, OJ. EU L 135 of 22.05.2019.
11. Regulation (EU) No. 2019/817 of the European Parliament and of the Council of May 20, 2019 on establishing an interoperability framework for EU information systems in the area of borders and visa policy and amending Regulations (EC)No. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726, (EU) 2018/1861 and Council Decisions 2004/512/EC and 2008/633/JHA, Official Journal of the EU L 135/27 of May 22, 2019.
12. Law on Participation of the Republic of Poland in SIS and VIS, art. 2 item 11, Dz. U. 2007 no. 165 item 1170.

Websites

1. https://encyklopedia.interia.pl/slownik-ue/news-konwencja-dublinska,nId,2112521.
2. https://encyklopedia.interia.pl/slownik-ue/news-system-dublinski,nId,2112880.
3. https://odoserwis.pl/p/306/europejski-zautomatyzowany-system-rozpoznawania- odciskow-palcow- eurodac.
4. https://www.schengenvisainfo.com/entry-exit-system-ees/.
5. https://ec.europa.eu/poland/news/190409_security_pl.
6. https://www.consilium.europa.eu/pl/press/press-releases/2019/05/14/interoperability-between-eu-information-systems-council-adopts-regulations/.