FACTA UNIVERSITATIS
Series: **Law and Politics** Vol. 16, N° 3, 2018, pp. 195-211
https://doi.org/10.22190/FULP1803195T

Original Scientific Paper

THE INTEROPERABILITY OF EUROPEAN INFORMATION SYSTEMS FOR BORDER AND MIGRATION MANAGEMENT AND FOR ENSURING SECURITY

UDC 341.222:061.1EU
351.756:314.74

Krzysztof Tomaszycki

Faculty of Law, University of Bialystok, Poland

Abstract. *In recent years, the European Union has been exposed to an increase in illegal migration. With migration, the threat of terrorist acts increased, which contributed to reducing the sense of internal security of citizens. The EU citizens expect more effective external border controls and more efficient migration management. Such challenges are addressed by the interoperability of European information systems for border management and migration, as well as ensuring security of the EU. A key element of interoperability is the adaptation of current systems and the development of new ones, especially in the technical aspect. In addition to legal, organizational and logistic activities, it is a key element of the entire system of activities of European institutions and agencies.*

Key words: *interoperability, migration, border management, sense of security, EU information systems.*

INTRODUCTION

When considering the issues of interoperability of European databases, their functioning and role in creating a sense of security resulting from social migrations to and within the European Union (EU) should be considered. These migrations are attributed to various negative phenomena in social perception. The threats associated with migration include, among others: (1) formation of criminal groups, (2) increase in crime, (3) human smuggling, drug trafficking, smuggling of weapons and tangible goods, (4) human and organ trafficking, (5) terrorist attacks, (6) spread of infectious diseases, (7) radicalization of social life, (8) fundamentalism, (9) jihad, (10) disturbance of the labor market, (11) creating enclaves within the country of destination[1]. Regulatory authorities of the power elite play a

Received December 12th, 2018 / Accepted December 21st, 2018
Corresponding author Krzysztof Tomaszycki, PhD (in Sociology), Faculty of Law, University of Bialystok, Republic of Poland, ID SCOPUS ORCID: 0000-0002-2979-0275; e-mail: ktomaszycki@wp.pl
[1] K. Tomaszycki, *Proces migracji - realne czy wirtualne zagrożenie?,* [w:] S. Gwoździewicz, K. Tomaszycki, *Prawne i społeczne aspekty cyberbezpieczeństwa,* Międzynarodowy Instytut Innowacji «Nauka – Edukacja – Rozwój» w Warszawie, Warszawa 2017, s. 196.

leading role in creating a sense of security not only at the level of individual member states of the European Union (EU MS) but also at the level of EU structures. In order to indicate not only the speech act[2] of the ruling elite, but also the actual actions at the European level, we need to look at the decisions on methods and means of control of third-country citizens arriving in the EU and protection of its external borders.

In this respect, an important element is the use of modern technologies - European databases, including biometric systems operating at national and international level. Databases and communication and information systems collecting data on persons crossing the EU external borders may use this information in their operation and monitor migration flows at the EU's external borders through functional mechanisms. Due to their nature, they have been called large-scale systems, and their role in raising the sense of security in the European area of freedom, security and justice is a leading one. Existing EU-wide systems operate autonomously, and the data collected in them often duplicate. Strengthening of cooperation between the EU member states in the field of controlling the migration of people from outside the Union and providing information that may foil terrorist attacks, reduce the terrorist threat or prevent cross-border organized crime requires taking measures in the field of integration and interoperation of already existing systems (Fig. 1.) and development and implementation of new information and communication solutions.

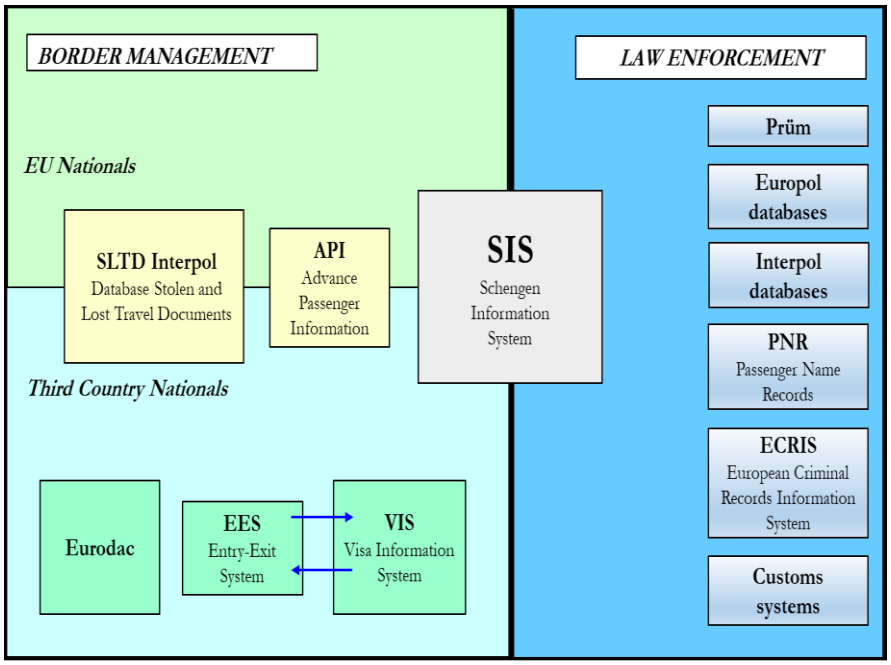

Fig.1 Schematic overview of the main information systems for border management and law enforcement
Source: own work, based on: Commission Communication to the European Parliament and the Council. *More efficient and more intelligent information systems for border management and security*, (COM (2016) 205 final of 06.04.2016).

[2] Speech *act - any of the acts that may be performed by a speaker in making an utterance, considered in terms of the content of the message, the intention of the speaker, and the effect on the listener*.

SYSTEMS AND DATABASES CURRENTLY OPERATING IN THE FIELD OF BORDER MANAGEMENT AND LAW ENFORCEMENT

Systems and databases existing in the European Union operate within the scope of: (1) border management and border traffic control in relation to European Union citizens and third-country nationals, and (2) law enforcement. Below I present a brief description of individual systems and databases.

Schengen Information System (SIS)[3]

It is the largest and most widely used information exchange platform on migration and law enforcement. It is a large-scale centralized information system used by 25 EU Member States[4] and 4 Schengen-associated countries[5]. Access to information input and processing is carried out by competent authorities responsible for maintaining public safety and order: the police, border control authorities and immigration authorities. It has information on third-country nationals who are forbidden to enter the Schengen area or to stay in the Schengen area, as well as information on EU citizens and third-country nationals who are sought or missing (including children) and information about sought items (firearms, vehicles, identity documents, industrial equipment, etc.). A characteristic feature of SIS is that, in case of obtaining specific information, instructions on a specific action to be taken on the spot (arrest or seizure of things) are obtained in relation to persons or things. The data controller of the data processed in the Schengen Information System in Poland (national database N-SIS) is the Chief Commander of the Police[6]. From April 9, 2013, Poland uses the second generation Schengen Information System - SIS II[7], which has a larger catalog of data categories compared to SIS, including biometric data. SIS II allows the creation of alerts in order to refuse entry or stay of third-country nationals. Since 2013, the responsibility for the operational management of SIS II rests with the European eu-LISA agency, which deals with the management of large-scale IT systems in the area of freedom, security and justice.

In terms of border management, the following systems and databases exist:

Data on stolen or lost travel documents (SLTD)

A database created in 2002 regarding passports, identity documents and visas that have been reported to Interpol by issuing authorities as stolen or lost. Details on stolen and lost travel documents are transferred directly to the STLD database by the National Bureau of INTERPOL and law enforcement authorities via the secure global police communication

[3] Legal basis: 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) (EU DU L 381/4 of 28.12.2006), Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 on the access of the services responsible in the Member States for the issuance of vehicle registration certificates to the second generation Schengen Information System (SIS II); Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (DU UE L 205/63 from 07.08.2007).

[4] All EU Member States except Ireland, Cyprus and Croatia.

[5] Switzerland, Liechtenstein, Norway, Iceland.

[6] Act of 24 August 2007 on the *participation of the Republic of Poland in the Schengen Information System and the Visa Information* System (Law Gazette of 2018 r. item 134, 138).

[7] https://mswia.gov.pl/pl/aktualnosci/10771,System-Informacyjny-Schengen-II.html, [access: 11/07/2018].

system INTERPOL I-24/7. Authorized officers at airports and border crossings can check a travel document and receive feedback within a few seconds, which is an opportunity to take an appropriate action. A total of 174 countries enter alerts in STLD and over 68 million pieces of information on stolen or lost travel documents have been entered. To help identify and stop criminals from using lost or stolen travel documents long before reaching an airport or a border, the INTERPOL developed *I-Checkit*. Thanks to this initiative, selected airlines may send information on the travel document in order to verify it in the SLTD database the moment the client starts booking an airline ticket. Presenting the effectiveness of this database, we can use the statistics of verifications for the period from January to September 2016, where 1,243000,000 searches were made, thereby yielding over 115,000 positive indications[8].

Advance Passenger Information (API)[9]

The API system is intended to gather information on the identity of a person before they take a flight to the EU and to identify irregular migrants at the time of their arrival. API data include information contained in the travel document of the traveler, such as full name, date of birth, nationality, number and type of travel document and information on the border inspection post where the person crossed the border (place of departure and entry), and also transport information. API data is collected during check-in.

Eurodac (European Dactyloscopy)[10]

The European Automated Fingerprint Recognition System contains biographical and biometric data. It has been operating since 2000 in the field of processing fingerprints of third-country nationals: asylum seekers, illegally crossing the external borders of the Schengen area or staying on the premises of an EU MS without any valid residence documents. Currently, its main purpose is to make it possible to determine which EU country, in accordance with the Dublin Regulation,[11] is responsible for examining the application for asylum. The Eurodac system consists of: (1) a central unit (fingerprint

[8] https://www.interpol.int/en/INTERPOL-expertise/Border-management/SLTD-Database,[access: 11/07/2018]

[9] Legal basis: Council Directive 2004/82 / EC of 29 April 2004 *on the obligation of carriers to provide passenger data* (Law Gazette EU L261/ 24 of August 6, 2004).

[10] Legal basis: Council Regulation (EC) No 2725/2000 of 11 December 2000, *concerning the establishment of Eurodac for the comparison of fingerprints for effective application of the Dublin Convention* (Law Gazette EC-L 316/1 of 15/12/2000), The European Parliament and of the Council (EU) No. 603/2013 of 26 June 2013 *on the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Regulation (EU) no 604/2013 establishing the 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 the presence of a comparison with the Eurodac data by Member States' law enforcement authorities and Europol for law enforcement, and amending Regulation (EC) no 1077/2011 establishing a European Agency for Operational Management of Large Scale Information Systems in the Area of Freedom, Security and Justice*, (Law Gazette UE L 180/1 of 29/06/2013).

[11] Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 *on establishing 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* (Dublin III), (Law Gazette UE L 180/31 of 2013) - amending the Council Regulation (EC) No. 343/2003 of 18 February 2003 *establishing 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* (Dublin II), (Law Gazette EU L 50/1 of 2003).

recognition system), (2) a central database in which data specified in the Eurodac Regulation is processed for the purpose of comparing fingerprints, and (3) measures for transferring data between EU MS and the central database. Registering fingerprints of asylum seekers or migrants with an irregular status in a centralized system makes it possible to detect and monitor their secondary movements within the EU until an application for international protection is made or until a decision is issued ordering the person to return to the country from which they came to the EU. Since 2013, responsibility for the operational management of Eurodac rests with eu-LISA, the EU agency dealing with the management of large-scale IT systems in the area of freedom, security and justice.

Entry/exit system (EES)[12]

The EES is a communication and information system registering identity of third-country nationals (biographical (alphanumeric) and biometric data (fingerprints and face image)) together with detailed data of travel documents. The main functional objective of the system will be to combine these data with electronic entries on entry and exit and information on the reason for refusal of entry along with data of the body that issued it. All third-country nationals who cross the border (entry and exit) arriving in the Schengen area as part of a short-term stay (maximum 90 days in a 180-day period) will be subject to registration, both for travelers subject to visa obligation and for travelers exempted from the visa obligation, or as a part of a stay on the basis of a new traveling visa (up to one year). The objective of the EES system is to: (1) improve the management of external borders, (2) reduce illegal migration by preventing unlawful prolonging of stay, and (3) support the fight against terrorism and serious crime, which as a result will contribute to increasing the level of internal security. The central registration will enable detection of persons who prolong their stay excessively and identification of persons without documents staying in the Schengen area.

Visa Information System (VIS)[13]

The Visa Information System is a centralized short-term visa information exchange system between Member States was created in 2004. It is used to process data and make decisions regarding applications for short-term visas allowing individuals to stay in the Schengen area or transit through it. All consulates of Schengen countries (around 2,000) and all border crossings at the external borders of these countries (around 1,800) are connected to the VIS. Every third-country visa applicant must provide detailed biographical information and biometric data (face photo in digital format and 10 fingerprints). At border

[12] Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 *establishing an Entry / Exit System (EES) to record data on entry and exit of third country nationals crossing the external borders of the Member States and entry refusal data with regard to such citizens and defining 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,* (Law Gazette EU L 327/20, 2017).

[13] Council Decision 2004/512 / EC of 8 June 2004 *establishing the Visa Information System (VIS) (Law* Gazette UE L 213/5 2004), Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July *2008 on the Visa Information System (VIS) and exchange of data between Member States on short-stay visas (VIS Regulation) (Law Gazette EU L 218/60 from 2008)* , Regulation of the European Parliament and of the Council (EC) No 810/2009 of 13 July 2009 *establishing a Community Code on Visas* (Law Gazette UE L 243/1, 2009) and Commission Decision 2010/49 /EC of 30 November 2009 *determining the first regions in which the Visa Information System (VIS) will be launched* (Law Gazette UE L 23/62 Z 2010).

crossing points or in the EU MS, the VIS is used to verify the identity of the visa holder by comparing his fingerprints with fingerprints registered in the system. This action guarantees verification of the person concerned based on biometric data at the border crossing point or inside the EU MS. The data collected in VIS also allow the identification of a person who applied for a visa in the last 5 years and who may not have identification documents with them. Since 2012, the operational management of VIS has been carried out by the EU agency eu-LISA.

Within the scope of compliance with legislation, the following systems and databases operate in the European Union:

Exchange of information under the Prüm Decision[14]

It aims to strengthen cross-border cooperation in combating terrorism, cross-border crime and illegal migration. Exchange of several types of data: automatic transmission of DNA profiles, fingerprint data, some data related to national vehicle registration and data related to events with a large cross-border dimension (e.g. sports events, European Council meetings) is based on a multilateral agreement between the EU MS. Law enforcement officers in one EU MS who need information to perform their duties may obtain it from another MS in the declared purpose for criminal proceedings. The data is stored in anonymous profiles and only after finding a "match" between the profiles you can request personal data, taking into account the limitations imposed by the national legislation in the field of data protection. DNA and fingerprint data exchange is based on a "match / no match" approach, which means that DNA profiles or fingerprints found at the crime scene in one EU MS can be automatically compared to profiles stored in databases of other EU countries. In a situation where the search finds a "match" in the database of another EU MS, the so-called "second step" follows and detailed information about that match is exchanged via bilateral exchange mechanisms. The Prum Treaty has not yet been fully implemented and is not consistently applied. Not all articles have been implemented by all Member States. In addition, not all Member States are interconnected for the purpose of automated data exchange regarding the three types of data mentioned above.

Europol Information System (EIS)[15]

It is the center of information on crimes in the EU and supports the exchange of information between national police authorities. The EIS is a centralized ICT system containing a database of suspected and convicted persons, criminal structures, crimes and measures to commit them on territory of the EU MS. EU Member States are able to collect, store, process and search crime (cross-border, organized and serious crime) and terrorist activities data. According to law, data are entered and downloaded to the EIS by national units, liaison officers, director, deputy directors and authorized Europol employees. Data exchange takes place through the Europol Information System - SIENA. This system

[14] Council Decision 2008/615/JHA of 23 June 2008 *on the intensification of cross-border cooperation, in particular in combating terrorism and cross-border crime* (Law Gazette L 210, 2008).

[15] Legal basis: Article 6 of the Convention drawn up on the basis of art. K.3 of the Treaty on European Union, on the establishment of the European Police Office (Europol Convention) (Law Gazette EC C 316/2 of 1995), Convention drawn up on the basis of Article K.3 of the Treaty on European Union on the establishment of a European Police Office (Europol Convention), drawn up in Brussels on July 26, 1995. In the name of Republic of Poland, the President of the Republic of Poland (Law Gazette 2005 No 29, pos. 243).

guarantees a fast, secure and user-friendly exchange of information between the EU MS and Europol or with third parties that have concluded cooperation agreements with the Europol. The Europol shall maintain cooperation in the field of information exchange in accordance with the role assigned with: (1) the Eurojust[16]; (2) the European Anti-Fraud Office (OLAF)[17]; (3) the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX)[18]; (4) the European Police College (CEPOL)[19]; (5) the European Central Bank; and (6) the European Monitoring Center for Drugs and Drug Addiction[20]. In the scope of performing its activities, the Europol may also cooperate with third countries, international organizations or the International Criminal Police Organization (Interpol).

Interpol Information System (IIS)[21]

The International Criminal Police Organization (Interpol) is an organization that improves global police cooperation by providing technical and operational support. Interpol maintains databases accessible to members via the National Central Bureaus (NCB) in real time via the Interpol I-24/7 network. Data collected in the Interpol databases concern: fingerprints, DNA profiles of perpetrators and victims of child molestation, stolen and lost travel documents, forged documents, stolen administrative documents, registration data of motor vehicles, motor boats and vessels, works of art, data on weapons (ballistics data, data on lost and illegally possessed weapons), data on radiological and nuclear materials, and data on sea piracy.

In addition to databases, the Interpol also supports the system of notices, the so-called wanted notices used to identify and locate persons or objects. Wanted notices are an international request for cooperation or a warning about sharing critical information. There are six categories that are published by the Secretariat-General. The six categories of wanted notices are: (1) Red – search in order to arrest wanted persons and extradite them; (2) Yellow – search for missing persons or in order to identify individuals who cannot provide their identity; (3) Blue – obtaining additional information about people or about illegal activity concerning crime; (4) Black – obtaining information about unidentified corpses; (5) Green – warnings and intelligence information about persons who have

[16] Eurojust was established by Council Decision 2002/187 / JHA of 28 February 2002 *establishing Eurojust in order to reinforce the fight against serious crime* (Law Gazette L 63 of 2002), as amended by Council Decision 2009/426/JHA of 16 December *2008 on the strengthening of Eurojust and amending Decision 2002/187 / JHA establishing Eurojust in order to reinforce the fight against serious crime* (Law Gazette EU L 138/14 of 2009).

[17] Commission Decision 1999/352/EC of 28 April 1999 establishing the *European Anti-Fraud Office (OLAF)* (Law Gazette EC L 136/20, 1999).

[18] Council Regulation (EC) No 2007/2004 of 26 October 2004 *establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union* (Law Gazette EU L 349 2004), as amended by Regulation (EC) No 863/2007 of the European Parliament and Council of 11 July 2007 (Law Gazette UE L 199/30 of 2007), Regulation (EU) No 1168/2011 of the European Parliament and of the Council of 25 October 2011 (Law Gazette UE L 304/1, 2011) The amendment, introduced by Regulation (EU) No 656/2014, *establishes rules for the protection of the EU's external sea borders in the context of operational cooperation coordinated by Frontex*.

[19] Regulation (EU) 2015/2219 of the European Parliament and of the Council of 25 November 2015 *on the European Police College (CEPOL) and replacing and repealing Council Decision 2005/681 JHA* (Law Gazette EU L 319/1, 2015).

[20] Regulation (EC) No 1920/2006 of the European Parliament and of the Council of 12 December 2006 *concerning the European Monitoring Center for Drugs and Drug Addiction* (Law Gazette EU L376/1, 2006).

[21] Interpol - International Criminal Police Organization founded in 1923

committed a crime and are likely to repeat these crimes in other countries; (6) Orange – warnings about people or events that due to their nature pose a serious and immediate threat to public safety.

Passenger Name Record (PNR)[22]

The PNR is a database containing a data set for each passenger's travel which contains the information necessary for allowing the processing and verification of bookings by air carriers operating the reservation and flight with regard to each flight booked by any person or on their behalf, regardless of whether the set is located in reservation systems, passenger check-in systems or equivalent systems performing the same functions. Each carrier would be required to provide relevant authorities with data on persons entering or leaving the European Union, and Member States would have to set up national passenger data systems based on common EU rules. The transferring passenger flight data system is being successively implemented in individual EU MS. The effectiveness of this system depends on the exchange of information (contained within it) between individual countries. Although PNR data were originally introduced for airlines, they can also be used for hotel reservations, car rentals, airport transfers and train travel. Following the terrorist attacks in Brussels in March 2016, Belgian authorities adopted a law transposing the European directive into the Belgian legislative frameworks, which indicates the need to introduce PNR data on train passengers.

European Criminal Records Information System-Third CountryNational (ECRIS-TCN)[23]

The ECRIS-TCN is an information exchange system regarding previous convictions passed against a specific person by criminal courts in the EU MS. These data concern EU citizens as well as third-country nationals and stateless persons. The central authorities designated in each EU MS are contact points in the ECRIS network; they perform tasks such as: providing information from criminal records, storing them, requesting them and sharing them. The system was launched in 2012 and operates in a decentralized architecture, which means that data is stored in national databases, and the exchange takes place between these systems. Currently, 25 EU MS exchanges data on convictions, while Malta, Portugal and Slovenia currently do not participate in the exchange of data using the ECRIS.

[22] Directive of the European Parliament and of the Council (EU) 2016/681 *of 27 April 2016 on the use of Passenger Name Record (PNR) data to prevent and detect terrorist offenses and serious crime, investigate and prosecute them* (Law Gazette EU L 119/132 of 04/05/2016).

[23] Council Framework Decision 2009/315/JHA of 26 February 2009 *on the organisation of the exchange of information extracted from criminal records between the Member States and the content of this information* (Law Gazette L 93/23 from 07.04.2009), Council decision 2009/316/JHA of 6 April *2009, on the establishment of the European criminal records information system* (Law Gazette L 93/33 from 07.04.2009), regulation of the European Parliament and of the Council *establishing a centralized system for the identification of Member States information on convictions passed against third-country nationals and stateless persons on the need to complement and support the European criminal records information system (ECRIS-TCN) and amending Regulation (EU) no 1077/2011,* (2017) 344 of 29.06.2017 r.

Code Information Systems (CIS)[24]

They play an important role in interdisciplinary cooperation at the EU's external borders. EU MS customs authorities hold various IT systems and databases containing data on the movement of goods between EU MS and third countries and the identification of economic operators. Thanks to these systems, customs authorities have information about possible threats that can be used to ensure the sense of internal security. The development of CTI technologies is accompanied by harmonization and unification of customs procedures in the EU MS. An important element of operation of these systems is the ability to cooperate with other CTI systems in order to manage EU borders and undertake customs operations. Customs IT systems have their own controlled, limited and secured infrastructure (common communication network), proper functioning of which is guaranteed by law. In order to minimise the risk to the Union, its citizens and its trading partners, the harmonised application of customs controls by the Member States should be based upon a common risk management framework and an electronic system for its implementation.

MANAGEMENT OF EXTERNAL BORDERS OF THE EUROPEAN UNION

Management of the EU's external borders concerns efficient deployment of people and goods to its area with an appropriate level of security risks. Mass migration of people from third countries to the European Union has shown that existing security measures at EU's external borders are not sufficient. As a result of acts of terror and increased illegal migration, some of the EU MS (Austria, Belgium, Denmark and Sweden) have since September 2015 restored control at the internal borders of the Schengen area. Adoption of this measure results from Article 23 of the Schengen Borders Code[25], and was a necessity due to issues of internal security and law enforcement. Mass illegal migration pushed EU institutions and agencies to take action aimed at more effective external border protection. The result of these activities was the creation of the European Border and Coast Guard[26]. *The objective of the Union's policy in the area of management of the EU's external borders is to develop and implement a European integrated border management system that goes beyond the national level to the EU level, which is an unavoidable consequence of the free movement of people within the EU and a fundamental element in the area of freedom,*

[24] Customs information systems cover all systems created under the Community Customs Code (Council Regulation (EEC) No 2913/92 of 12 October 1992 *establishing the Community Customs Code* (Law Gazette EC L 302/1 of 1992)) and the Union Customs Code (Regulation European Parliament and Council (EU) No 952/2013 of 9 October 2013 *establishing the EU Customs Code* (Law Gazette EU L 269/1 from 2013)) and the decision on elimination of paper documents in the customs and trade sectors (Decision No. 70 / 2008 / EC) and the Customs Information System (CIS) established under the 1995 CIS Convention. They are intended to help combat customs crime by facilitating cooperation between European customs authorities.

[25] Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 *on the EU Code on the rules governing the movement of persons across borders* (EU Border Code) (Law Gazette EU L 77/1, 2016), as amended by the Regulation of the European Parliament and Council (EU) 2017/458 of 15 March 2017 with *regards to the intensification of border checks at external borders using appropriate databases* (Law Gazette EU L74 / 1 from 2017).

[26] Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 *on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No. 863/2007 of the European Parliament and Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC* (Law Gazette EU L 251/1, 2016).

security and justice. European integrated management of external borders is a key element to improving migration management. The aim of such an approach is to effectively manage border traffic at external borders and to address challenges related to migration and accompanying threats, thereby contributing to combating serious cross-border organized crime and contributing to ensuring a high level of internal security in the EU MS. At the same time, efforts should be made to ensure that the actions taken are carried out with full respect for fundamental rights and in a manner that guarantees the free movement of people in the EU.[27] The appointment of another EU agency does not guarantee protection from acts of terror caused by assassins crossing the borders of the Union; however, it may be necessary to improve the effective management of border-crossing by people and goods.

An important element of all measures aimed at improving the management of external borders is the collection of data, their proper analysis and use at the EU level. The development of the presented CTI systems and introduction of new ones is based on the assumption that the EU MS will use the data collected and/or generated in these systems for more efficient border management. In addition, these data must be verified against data collected in national systems. An important factor is also the assumption that EU MS enter appropriate data into EU systems (e.g. SIS II), so that they are relevant and, therefore, that automatic matching with data already collected in other European border management systems can be carried out. The effectiveness of all initiatives in the area of management of the EU's external borders depends on the assessment of migration risk and from inter-agency cooperation and information exchange between border management agencies, customs authorities and other EU MS bodies, as well as at EU, national and bilateral level. The development of concepts increasing the security of external borders must be directed at the possibility of comprehensive downloading and processing of not only biographical data but also biometric data (fingerprints, facial image). As Włodzimierz Fehler points out, important elements affecting the elimination of multidimensional threats to the internal security of the EU are activities aimed, inter alia, at: wide application of preventive measures, including those based on intelligence data, use of a comprehensive information exchange model, operational cooperation, cooperation between criminal justice authorities and integrated border management[28]. In this context, improving the management of external borders should be based on the introduction of new technologies combined with a comprehensive exchange of information on migratory flows at external borders and within the EU, in individual Member States. In line with the expectations of EU citizens, checks on persons at external borders and controls within the Schengen area should be effective, allow effective management of migration and borders, and contribute to internal security. These challenges have drawn special attention to the urgent need to combine and comprehensively reinforce EU's information tools for border and migration management as well as internal security. ICT systems currently functioning at EU level may provide border guards and law enforcement officers and immigration officials with relevant information about persons. For this support to be effective, information provided via EU information systems must be complete, accurate and reliable. However, there are many imperfections and structural flaws in the EU's information management structure. The border and security

[27] Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016. Art. 2

[28] W. Fehler, *Poprawa bezpieczeństwa UE przez zarządzanie granicami*, [in:] W. Fehler, K. P. Marczuk (red.), *Polityka Unii Europejskiej w zakresie bezpieczeństwa wewnętrznego. Uwarunkowania, realizacja, wyzwania w drugiej dekadzie XXI wieku*, Wydawnictwo Difin, Warszawa 2015, p. 192.

data management structure is fragmented, as information is stored separately in unrelated systems, despite collecting and processing the same data categories. In its actions, the EU aims to create a data exchange system based on interoperability, so that the appropriate border guards, migration and law enforcement authorities and the judiciary authorities have access in a given time and place to data allowing effective management of external borders, migration and strengthening internal security.

INTEROPERABILITY OF EU IT SYSTEMS IN THE FIELD OF SECURITY, BORDER MANAGEMENT AND MIGRATION

In order to move on to the issue of interoperability of EU information systems in the fields of security, border management and migration, the term 'interoperability' should first be clarified. Interoperability is the ability of various systems and organizations to engage in an effective cooperation based on: (1) technical standards, (2) legal regulations, and (3) organizational measures. In terms of EU activities, the term 'interoperability' means the ability of information systems to exchange data and enable information exchange to increase the efficiency and effectiveness of pan-European information exchange tools, providing technical processes, standards and tools that enable better interoperability of EU information systems in security, external border management and migration. This means that authorized users (police and border guards, migrant officers and employees responsible for internal security) have faster, easier and more systematic access to the information they need to do their job. In the field of border management and migration, interoperability will consist in the targeted use of existing data in various ICT systems, their aggregation and connections between systems based not only on biographical data but also on biometric data. The example of a Berlin bomber (December 19, 2016), who carried out a terrorist attack by using a stolen truck (killing 12 people on the scene and the driver of the stolen truck), indicates that despite the police and special services' prior interest in him, he was able to freely move around the EU using many documents issued for different identities. "He was listed as a person with as many as 14 different identities," said Dieter Schuermann, Head of the State Criminal Police Service in North Rhine-Westphalia.[29] This example shows that lack of biometric data made it impossible to effectively control the movement of this assassin and, thus, to counteract his terrorist activity. Despite many ICT systems, there are loopholes that allow third-country nationals to move across the EU without any control or supervision. Effective border management and law enforcement requires legislative and organizational work to ensure the use of existing ICT systems, create new ones and ensure convergence between the systems and the existing communication infrastructure between individual EU MS. This will ensure synergy of data usage and its quality in terms of biography and biometrics.

[29] http://l24.lt/pl/swiat/item/166992-zamachowiec-z-berlina-mial-14-tozsamosci, [online access: 10/08/2018].

Removal of the information gap in the field of combining biographical and biometric data in the most widely used system - SIS - comes to the fore. These activities were supported by the establishment of the High Level Expert Group on Information Systems and Interoperability[30]. The final report published in May 2017 sets out a series of recommendations that remove information loopholes and reinforce actions to develop EU systems and their interoperability. The basis for the activities will be the full centralization of EU ICT systems. Respect for fundamental rights has become an overriding priority of these activities. An expression of the efforts made in terms of interoperability was a proposal amending the Regulation of the European Parliament and the Council on establishing a framework for interoperability between EU information systems sent in June 2018 by the European Commission[31]. The proposal includes the following objectives:

1. ensuring that end users have fast, efficient, systematic and controlled access to the information they need to perform their official tasks;
2. providing a solution to detect different identities associated with the same biometric data (improving identification of bona fide travelers and combating identity fraud);
3. facilitating the control of the identity of third country nationals on the MS territory by authorized services; and
4. facilitating and improving law enforcement access to information systems not related to the prosecution of crimes at EU level, if necessary, for the purpose of preventing, investigating or prosecuting serious crimes and terrorism.

Achieving these objectives will be possible by centralizing existing pan-European systems (SIS (including SIS II), Eurodac, and VIS) and creating new centralized pan-European systems (Entry/Exit System (EES), European Travel Information System and travel permits (ETIAS), and a European system for transferring information on third-country nationals from criminal records (ECRIS-TCN system)). This concept focuses on the processing of personal data from the so-called third countries (except SIS). The indispensable element that determines the effectiveness of this concept is the elaboration of technical intentions on the basis of which it will be possible to achieve full interoperability of EU ICT systems. Technical assumptions for interoperability are presented in Fig. 2.

[30] Commission Decision of 17 June 2016 *setting up the High Level Expert Group on Information Systems and Interoperability* - (Law Gazette UE C 257/3 of 15/07/2016).

[31] Proposal from the European Commission amending the *REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing an interoperability framework between EU information systems (police and judicial cooperation, asylum and migration) and amending [Regulation (EU) 2018/XX [Eurodac Regulation], Regulation (EU) 2018/ XX [SIS Regulation regarding the prosecution], Regulation (EU) 2018/XX [ECRIS-TCN Regulation] and Regulation (EU) 2018/XX [the eu-LISA Regulation*] -COM (2018) 480 final from 13/06/2018 rf.

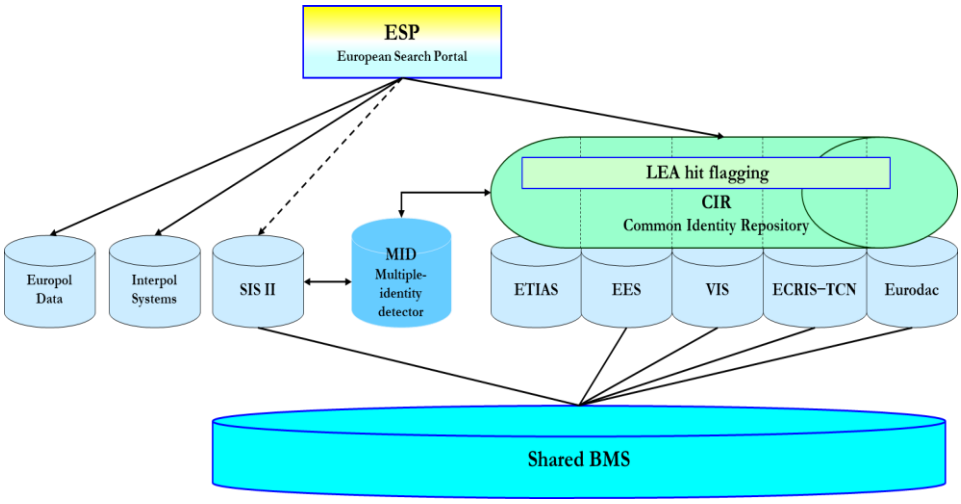

Fig. 2 Technical assumptions of interoperability

Source: own study; based on: Commission proposal to the European Parliament and the Council: *REGULATION OF THE EUROPEAN PARLIAMENT AND THE COUNCIL establishing the interoperability framework between EU information systems (in the area of borders and visa policy) and amending Council Decision 2004/512 / EC, Regulation (EC) No. 767/2008, Council Decision 2008/633 / JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226*, (COM (2017) 793 final of 12.12.2017)

TECHNICAL ELEMENTS OF INTEROPERABILITY

European Search Portal (ESP)

It is an essential element for viewing different systems: central Schengen information system (C.SIS and SIS II), Eurodac, VIS, future EES, proposed ETIAS and ECRIS-TCN systems, as well as relevant Interpol and Europol databases. Identity search operations will be based on both biographical and biometric data. This will provide services responsible for border protection and migration management with fast, efficient, effective, systematic and controlled access to all information necessary to perform their tasks. This provides the ability to address one query and, as a result, to check on many systems and get answers from many systems in real time without unnecessary delay. The ESP would be an "intermediary" in searching for the necessary data in various systems. This portal does not collect any data (new or existing) and does not process new data. It uses data (biographical and biometric) that are already collected in other systems.

Shared biometrics matching service (Shared BMS)

It is an essential element enabling consultation and comparison of biometric data (fingerprints and face images) from various central systems (especially SIS, Eurodac, VIS, future EES and the proposed ECRIS-TCN system), in addition to the ETIAS system, which will not contain biometric data, will not be therefore associated with a common website for the association of biometric data. Today, every central system uses its biometric search engine, while a common biometric matching service would provide a common platform for simultaneous viewing and comparison of these data. Biometric data (fingerprints and face

images) are stored only in basic systems. In the proposed solution, the BMS would be an essential element im detecting links between different sets of data and different identities assumed by the same person and registered in different central systems.

Common Identity Repository (CIR)

It is a common component for the collection of biographical and biometric data on the identity of third-country nationals registered in the Eurodac, VIS, future EES and in the proposed ETIAS and ECRIS-TCN systems. Each of these five central systems registers or will register biographical data of specific people for specific reasons. The relevant identity data would be stored in a common identity repository, but they would still "belong" to the relevant core systems in which they were registered. The common identity repository will not contain data collected in the SIS. The main objective of CIR is to facilitate the biographical identification of third-country nationals. The result of a carried out check will be presented in the function "result / no result". Out of the five systems that would be covered by the common identity repository, the future EES and the proposed ETIAS and ECRIS-TCN are new systems that still need to be developed. Currently, Eurodac does not include biographical data, so new legal provisions have to be developed in order to use it.

Multiple Identity Detector (MID)

It is an element used to check that consulted identity data is present in more than one of the systems connected to it. The module includes identity data collection systems in the common identity repository (CIR) (Eurodac, VIS, future EES and proposed ETIAS and ECRIS-TCN systems) and SIS. It would provide for detecting the multiplication of identity associated with the same set of biometric data, which would serve the dual purpose of correctly identifying people traveling in good faith and combating identity fraud. This solution is an innovation in regard to effectively resolving the problem of using false identities, which is a serious security breach. The module would only show biographical entries concerning identities to which there are links in different central systems. Such links would be detected using a common biometric matching site based on biometric data, and would require confirmation or rejection by the authority that registered this data in the information system that led to the creation of the link. The connections will be presented in four categories:

- yellow connection - the possibility of differing biographical identities belonging to the same person;
- white connection - confirmation that different biographical identities belong to the same person traveling in good faith;
- green connection - confirmation that different people traveling in good faith have the same biographical identity;
- red connection - the suspicion that the same person unlawfully uses different biographical identities.

CONCLUSION

In recent years, threats to internal security in individual EU MS have taken different forms and have been very visible. Spectacular examples of an increase in the level of threats were acts of terror, which made not only the public opinion of the European Union Member States but also the involved EU institutions and bodies pay more attention to security issues. While the general public expresses its concern over the increase of threats resulting from mass migration, including illegal migration, EU institutions and bodies have made efforts to counteract these threats. The challenges associated with migration have highlighted the urgent need for more effective use of ICT tools possessed by EU. These activities are aimed at making more effective use of existing information systems, addressing loopholes and using data collected in these systems intelligently to protect the EU's external borders in a better way, managing borders and migrations more effectively, and enhancing internal security. The proposed interoperability solutions must comply with respect for fundamental rights and protection of personal data.

Currently used central EU ICT systems have many loopholes and are not technically coupled with each other. This results in introduction of the same data into different systems by various entities responsible for public security and border surveillance. Ensuring public security requires the ability to check real-time (biographical and biometric) data on persons that cross the EU borders and move around its territory. The interoperability of ICT systems proposed by the European Commission is a response to the challenges of illegal migration and threats arising from it. Consultations in individual EU MS enabled development of assumptions that will meet these challenges. Interoperability of EU information systems is essential for internal security, common high standards of border management, prevention of cross-border crime and acts of terror, and providing security authorities with systematic, efficient, fast and controlled access to necessary information.

REFERENCES

Act of 24 August 2007 on the *participation of the Republic of Poland in the Schengen Information System and the Visa Information* System (Law Gazette of 2018 r. item 134, 138).

Commission Decision 1999/352 / EC of 28 April 1999 *establishing the European Anti-Fraud Office (OLAF) (Law Gazette EC L 136/20, 1999).*

Commission Decision of 17 June 2016 *setting up the High Level Expert Group on Information Systems and Interoperability* - (Law Gazette UE C 257/3 of 15/07/2016).

Council Decision 2002/187 / JHA of 28 February 2002 *establishing Eurojust in order to reinforce the fight against serious crime* (Law Gazette L 63 of 2002), as amended by Council Decision 2009/426 / JHA of 16 December *2008* on the strengthening of Eurojust and amending Decision 2002/187 / JHA establishing Eurojust in order to reinforce the fight against serious crime (Law Gazette EU L 138/14 of 2009).

Council Decision 2004/512 / EC of 8 June 2004 *establishing the Visa Information System (VIS)* (Law *Gazette UE L 213/5 2004), Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 on the Visa Information System (VIS) and exchange of data between Member States on short-stay visas (VIS Regulation) (Law Gazette* EU L 218/60 from 2008) , *Regulation of the European Parliament and of the Council (EC) No 810/2009 of 13 July 2009 establishing a Community Code on Visas* (Law Gazette UE L 243/1, 2009) and Commission Decision 2010/49 /EC of 30 November 2009 *determining the first regions in which the Visa Information System (VIS) will be launched* (Law Gazette UE L 23/62 Z 2010).

Council Decision 2008/615/JHA of 23 June 2008 *on the intensification of cross-border cooperation, in particular in combating terrorism and cross-border crime* (Law Gazette L 210, 2008).

Council Regulation (EC) No 2007/2004 of 26 October 2004 *establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union* (Law Gazette EU L 349 2004), as amended by Regulation (EC) No 863/2007 of the European

Parliament and Council of 11 July 2007 (Law Gazette UE L 199/30 of 2007), Regulation (EU) No 1168/2011 of the European Parliament and of the Council of 25 October 2011 (Law Gazette UE L 304/1, 2011); the amendment, introduced by Regulation (EU) No 656/2014, *establishes rules for protection of the EU's external sea borders in the context of operational cooperation coordinated by Frontex*.

Directive of the European Parliament and of the Council (EU) 2016/681 *of 27 April 2016* on the use of Passenger Name Record (PNR) data to prevent and detect terrorist offenses and serious crime, investigate and prosecute them (Law Gazette EU L 119/132 of 04/05/2016).

Council Directive 2004/82 / EC of 29 April 2004 *on the obligation of carriers to provide passenger data* (Law Gazette EU L261 / 24 of August 6, 2004).

Council Regulation (EC) No 2725/2000 of 11 December 2000, *concerning the establishment of Eurodac for the comparison of fingerprints for effective application of the Dublin Convention* (Law Gazette EC-L 316/1 of 15/12/2000), The European Parliament and Council Regulation (EU) No. 603/2013 of 26 June 2013 *on the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Regulation (EU) no 604/2013 establishing the 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 the presence of a comparison with the Eurodac data by Member States' law enforcement authorities and Europol for law enforcement, and amending Regulation (EC) no 1077/2011 establishing European Agency for the operational management of large-scale IT systems in the area of freedom*, security and justice, *(Law Gazette UE L 180/1 of 29/06/2013).*

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) (EU Law Gazette L 381/4 of 28.12.2006), Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 on the access of the services in the Member States responsible for the issuance of vehicle registration certificates to the second generation Schengen Information System (SIS II); Council Decision 2007/533 / JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (Law Gazette UE L 205/63 from 07.08.2007).

Proposal from the European Commission amending the *REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing an interoperability framework between EU information systems (police and judicial cooperation, asylum and migration) and amending [Regulation (EU) 2018 / XX [Eurodac Regulation], Regulation (EU) 2018 / XX [SIS Regulation regarding the prosecution], Regulation (EU) 2018 / XX [ECRIS-TCN Regulation] and Regulation (EU) 2018 / XX [the eu-LISA Regulation*] -COM (2018) 480 final from 13/06/2018 rf

Regulation (EC) No 1920/2006 of the European Parliament and of the Council of 12 December 2006 *concerning the European Monitoring Center for Drugs and Drug Addiction* (Law Gazette EU L376 / 1, 2006).

Regulation (EU) 2015/2219 of the European Parliament and of the Council of 25 November 2015 *on the European Police College (CEPOL) and replacing and repealing Council Decision 2005/681 JHA* (Law Gazette EU L 319/1, 2015).

Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 *on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No. 863/2007 of the European Parliament and Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267 / EC* (Law Gazette EU L 251/1, 2016).

Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 *on the EU Code on the rules governing the movement of persons across borders* (EU Border Code) (Law Gazette EU L 77/1, 2016), as amended by the Regulation of the European Parliament and Council (EU) 2017/458 of 15 March 2017 with *regards to the intensification of border checks at external borders using appropriate databases* (Law Gazette EU L74 / 1 from 2017).

Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 *establishing an Entry / Exit System (EES) to record data on entry and exit of third country nationals crossing the external borders of the Member States and entry refusal data with regard to such citizens and defining 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*, (Law Gazette EU L 327/20, 2017).

Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 *on establishing 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* (Dublin III), (Law Gazette UE L 180/31 of 2013) - amending the Council Regulation (EC) No. 343/2003 of 18 February 2003 *establishing* 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 (Dublin II), (Law Gazette EU L 50/1 of 2003).

The Convention drawn up on the basis of art. K.3 of the Treaty on European Union, *on the establishment of the European Police Office (Europol Convention)* (Law Gazette EC C 316/2 of 1995), *Convention drawn up on the basis of Article K.3 of the Treaty on European Unionon the establishment of a European Police Office (Europol Convention), drawn up in Brussels on July 26, 1995. In the name of Republic of Poland, the President of the Republic of Poland* (Law Gazette 2005 No 29, pos. 243).

Union Customs Code (Council Regulation (EEC) No 2913/92 of 12 October 1992 *establishing the* Union Customs Code *(Law Gazette EC L 302/1 of 1992)) and the EU Customs Code (Regulation European Parliament and Council (EU) No 952/2013 of 9 October 2013 establishing the EU Customs Code* (Law Gazette EU L 269/1 from 2013)) and the decision on elimination of paper documents in the customs and trade sectors (Decision No. 70/2008/EC) and the Customs Information System (CIS) established under the 1995 CIS Convention. They are intended to help combat customs crime by facilitating cooperation between European customs authorities.

Fehler, W. (2015). *Poprawa bezpieczeństwa UE przez zarządzanie granicami*, [in:] Fehler W., Marczuk K.P., (ed.), *Polityka Unii Europejskiej w zakresie bezpieczeństwa wewnętrznego. Uwarunkowania, realizacja, wyzwania w drugiej dekadzie XXI wieku*, Wydawnictwo Difin, Warsaw 2015.

Tomaszycki, K. (2017), *Proces migracji - realne czy wirtualne zagrożenie?,* [in:] Gwoździewicz S., Tomaszycki K., *Prawne i społeczne aspekty cyberbezpieczeństwa*, Międzynarodowy Instytut Innowacji «Nauka – Edukacja – Rozwój» w Warszawie, Warsaw 2017.

https://www.interpol.int/en/INTERPOL-expertise/Border-management/SLTD-Database. [online access: 11/07/2018].

http://l24.lt/pl/swiat/item/166992-zamachowiec-z-berlina-mial-14-tozsamosci [access: 11/07/2018]

https://mswia.gov.pl/pl/aktualnosci/10771,System-Informacyjny-Schengen-II.html [online access 11/07/2018].

INTEROPERABILNOST EVROPSKIH INFORMACIONIH SISTEMA U UPRAVLJANJU GRANICAMA I MIGRACIJAMA, I OBEZBEĐIVANJE SIGURNOSTI

Evropska unija se poslednjih godina suočava sa porastom ilegalnih migracija. Porast migracija doveo je do povećane opasnosti od terorističkih akata, što je doprinelo smanjenju osećaja sigurnosti građana Evropske unije. Građani EU očekuju efikasniju kontrolu spoljašnjih granica kao i efikasnije upravljanje migracijama. Odgovor na ove bezbednosne izazove može se naći u interoperabilnosti evropskih informacionih sistema koji se koriste za upravljanje granicama i migracijama, kao i za obezbeđivanje sigurnosti Evropske unije. Ključni element interoperabilnosti je adaptacija postojećih sistema i razvoj novih, posebno u tehničkom smislu. Pored pravnih, organizacionih i logističkih aktivnosti, to je ključni element čitavog sistema aktivnosti evropskih institucija i agencija.

Ključne reči: *interoperabilnost, migracije, upravljanje granicama, osećaj bezbednosti, informacioni sistemi EU.*