Andrzej WAWRZUSISZYN

Technology in favour of European Union border

Abstract. In order to better manage the flow of travellers and better control of these flows, modern technological solutions are introduced at the external border of the European Union. The purpose of these activities is the so-called intelligent borders that will be crossed by some travellers automatically, without the interference of border guards. These are IT systems which main task is to strengthen the Community's security by monitoring migrants who cross the border in an unauthorized manner or extend their stay on its territory. Biometric data control, automated border check, comprehensive entry / exit recording systems, electronic travel permits, supervision of passenger air traffic, virtual gates and satellite monitoring will allow for quick verification of persons entering and leaving the territory of the Community. The author characterizes chosen technological solutions already in function and the ones implemented within the framework of the European concept of intelligent borders.
Keywords: *security, EU borders, management, technology, IT system, intelligent borders*

Technologia w służbie kontroli granic Unii Europejskiej

Streszczenie. W celu skuteczniejszego zarządzania przepływami podróżnych i lepszej kontroli tych przepływów na granicy zewnętrznej Unii Europejskiej wprowadzane są nowoczesne rozwiązania technologiczne. Celem tych działań są tzw. inteligentne granice, które będą przekraczane przez niektórych podróżnych automatycznie, bez ingerencji funkcjonariuszy służb granicznych. To systemy informatyczne, których zadaniem jest przede wszystkim wzmocnienie bezpieczeństwa Wspólnoty poprzez monitorowanie migrantów, którzy w nieuprawniony sposób przekraczają granice lub przedłużają swój pobyt na jej terytorium. Kontrola danych biometrycznych, zautomatyzowana odprawa graniczna, kompleksowe systemy rejestrowania wjazdu/wyjazdu, elektroniczne zezwolenie na podróż, nadzór nad pasażerskim ruchem lotniczym, wirtualne bramki oraz satelitarny monitoring pozwolą na szybką weryfikację osób wjeżdżających i wyjeżdżających z terytorium Wspólnoty. Autor charakteryzuje poszczególne rozwiązania technologiczne już funkcjonujące oraz wdrażane w ramach europejskiej koncepcji inteligentnych granic.
Słowa kluczowe: *bezpieczeństwo, granice unijne, zarządzanie, technologia, system informatyczny, inteligentne granice*

Introduction

The ideas of strengthening the security of the EU's external borders with information technology started at the beginning of the 21st century. The European Commission then stated that for this purpose solutions from in the field of high technology should be used. Modern technologies with ever better security and increasingly improved information management procedures as well as the use of biometric data have begun to gain more and

more approval as appropriate solutions within the EU area of freedom, security and justice and will contribute to the effective management of the constantly growing flow of travellers. On Commission initiative, preparatory work for the implementation of several systems using the latest achievements of various technologies was started. The purpose of the article is to present already existing and implemented IT systems that are to contribute to more effective management of the external borders of the European Union.

Information systems at the external borders of the European Union

As part of initiatives implementing the European Union policy to create an area of freedom, security and justice, three systems were built: the Schengen Information System (SIS), the Visa Information System (VIS) and the Fingerprint Identification System (EURODAC).

The first of these, the Schengen Information System (SIS), became a Community electronic database created on the basis of the provisions of the Convention of 19 June 1990 to the Schengen Agreement of June 14, 1985. According to art. 93 of the Convention, the aim of the system was to maintain public order and public security, including state security, in the territories of the contracting parties and the application of the provisions of the Convention relating to the movement of persons in these territories, using information provided through this system. The system collected data on observed, suspicious or prosecuted persons and objects (stolen vehicles, weapons, documents, etc.) and provided automated procedures for finding information about such persons and objects.

When crossing the external borders or during a standard police control using the system, officers could check whether a given person or object (e.g. car, document) are included in the database. Due to the fact that the scope of data processed in the system became insufficient, to establish the identity of persons or to identify items to be checked, an auxiliary body was introduced in the form of the SIRENE[1] office responsible for entering and processing supplementary[2] information in the system.

[1] The SIRENE Bureau (Supplementary Information Requests at the National Entries) the body appointed on the basis of art. 108 of the Convention Implementing the Schengen Agreement (KWS).

[2] Supplementary information is information that is not stored in the system but is related to alerts to the system and which are exchanged to allow Member States to consult or inform each other in the following circumstances: when making an alert, in order to be able to take appropriate action confirmation in the system, in case of inability to take the required action, in case of resolving data quality issues of the system, in case of resolving the issue of compliance and priority of entries, in the case

Due to the fact that the technical infrastructure of the system, which was designed in the 90s of the last century, was initially intended for servicing seven countries and was not prepared for new national installations, in 2004, work on the version of the second generation Schengen Information System was initiated (SIS II). Two years later, the European Parliament and the Council set up the second generation Schengen Information System (SIS II)[3].

The Regulation has broadened the purpose, scope and functions of the system. The Schengen Information System (SIS II) has become a modern large-scale system, using modern technologies and IT solutions enabling the processing of a larger number of data categories (text, biometrics), at the same time ensuring continuous, stable and uninterrupted access to the system by all participating Schengen Agreement countries. The asset of the system is the improvement of data quality and the ability to identify people. It is intended for use by border guards, customs officers, visa authorities and enforcement authorities in the Schengen area to ensure a high level of security. The system works 24 hours a day, 7 days a week.

The system is similarly constructed as its predecessor. It is divided into the central system (central SIS II), the national system (N. SIS II) in each Member State and the communication infrastructure between the central system and the national system. The system allows the transfer and exchange of data by an encrypted virtual network between the authorities responsible for the exchange of any supplementary information that SIRENE offices carry out. To unify the work of these offices, the SIRENE[4] manual was developed. It is a set of guidelines describing the general and specific procedures that the competent authorities must follow to exchange supplementary information on the following categories of entries:

a) entries for the purposes of refusing entry or stay (first pillar),
b) entries concerning persons wanted for arrest, surrender or extradition (this and other categories are included in the third pillar),
c) entries regarding missing persons,
d) entries regarding persons wanted for legal proceedings,

of solving issues related to access rights. Source: 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), OJ L 311/4 of 28.12.2006.

[3] Ibidem.

[4] Commission Decision 2008/333 / EC of 4 March 2008 on the adoption of the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II), OJ EU L 123, 8.05.2008.

e) entries for purposes of secret controls or specific checks,
f) entries regarding items to be seized or used as evidence.

The rules of organization and operation of the SIS II system do not differ much from the previous version. The construction, operation and maintenance of its own national system and communication with the central system are the responsibility of each Member State. In the case of a failure, a reserve central system was built, capable of providing all the functions of the main central system located in the vicinity of Salzburg.

The system database contains, provided by each Member State, certain information about persons that are necessary for making entries for the purpose of refusing entry and stay permits. They include mainly: surname and first name, family name, pseudonyms, specific physical features, place and date of birth, sex, photographs, fingerprints, citizenship, information on whether the person is armed, aggressive or whether he is an escapee and the reason for the entry and authority making an entry, as well as links to other entries made in the system (in the case of an operational need). The Member State that issued the alert has the obligation to ensure that the data is accurate, up-to-date and entered into the system in accordance with the law. All changes to the entered data are only authorized by the state which issued the entry. Users can only have access to the data they need to perform their tasks. The period of storage of entries in the system is three years. During this time, the Member State which issued the alert verifies the need to maintain it. After this period, entries are deleted automatically, unless there is a need to extend the period of storage of the given entry. The safety of the data processed in the system is the responsibility of each Member State.

The Schengen Information System (SIS II) allows third-country nationals to access data concerning them in terms of correction, inaccuracy or removal. If a citizen determines that his or her personal data have been misused or need to be corrected or deleted, he/she may apply for access to them in any Schengen country by contacting the relevant national data protection authority. The national authority is obliged to provide feedback as soon as possible, but no later than three months from the date of submitting the application. All operations performed in the system are subject to supervision by the Member State and the European Data Protection Supervisor.

The system (SIS II) was updated in 2015 to improve the exchange of information on people suspected of terrorism and to strengthen actions taken by Member States to cancel travel documents of persons who are

suspected of willingness to join terrorist groups outside the European Union. In order to further strengthen security at the external borders, it is planned to use databases containing stolen or lost travel documents (SLTD). The Commission allows Member States to use automated border control using the SIS and the SLTD database and monitors how Member States implement their obligations to provide data to the SLTD.

Another Union IT venture was the Visa Information System (VIS) with the purpose of identifying travellers for the purposes of visa data[5]. The decision to establish the system was at the same time the legal basis for including in the general budget of the European Union the necessary funds for the development of the Visa Information System (VIS). It was assumed then that the system would serve for the exchange of visa data between Member States, enabling authorized national authorities to enter and update visa data and electronic consultation of these data. However, in 2008, the European Parliament and the Council concluded that the previous assumptions should be modified. The relevant Regulation on the Visa Information System (VIS) introduces innovative conditions and procedures to facilitate the processing of applications and decisions regarding the issuance of short-stay visas and related decisions on cancellations, withdrawals or extensions thereof. The above regulation has specified the objectives of the previously defined system. The system is to serve primarily:

- better implementation of the common visa policy,
- improving consular cooperation and the consultation process between central visa authorities by facilitating the exchange of data on applications and related decisions between Member States in order to simplify the visa application procedure,
- preventing the visa trade and the fight against fraud,
- improvement of checks at border crossing points at external borders and in the territory of the Member States,
- assistance in identifying persons who may not fulfil the conditions for entry, stay or residence in the territory of the Member States or who no longer meet these conditions,
- contribute to the prevention of threats to the internal security of each Member State[6].

[5] Council Decision of 8 June 2004 on the establishment of the Visa Information System (VIS) (2004/512 / EC), OJ EU L 213/5 of 15.06.2004.

[6] Ibidem.

The system began operating in October 2011 in North Africa, when all Schengen states' consular offices were connected to the system in Algeria, Egypt, Libya, Mauritania, Morocco and Tunisia. Moreover, from October 31, 2011, all Schengen states used the system at crossings located at external borders.

The Visa Information System (VIS), like the SIS II system, consists of two main components: a central information system, a national system providing connection to the central national authorities of the relevant Member State and the communication infrastructure between the central system and national systems. The database of the system gathers data of the applicant and the visa holder (in addition to basic information, gender, race or ethnic origin, religion or belief, disability, age or sexual orientation), visa application, visa information (issued, extended, withdrawn, cancelled, refusals, etc.), photographs of the applicant, fingerprints, as well as information about the applications of persons traveling together (families, groups, etc.).

These data are processed in accordance with the highest security standards and may not be transferred or made available to third countries or international organizations. Access to the system database for entering, modifying or deleting data is limited. First and foremost, border services, bodies responsible for granting asylum and control of the legality of stay in the Schengen area are eligible. It is important that each person may apply to the state for correction of incorrect data about themselves and for the removal of data registered unlawfully. Furthermore, each person also has the right to institute proceedings or lodge complaints with the competent authorities or the competent courts of that Member State, who have denied the right of access or the right to correct or delete data relating to him or her. If a person has been the victim of an unlawful processing operation, he is entitled to receive compensation from the Member State that is the perpetrator of the damage suffered. The functioning of the Visa Information System (VIS) is supervised by the national authority and the European Data Protection Supervisor in the scope of lawfulness of personal data being processed. The national supervisory body ensures that at least every four years the audits of data processing operations in the system in accordance with international standards are carried out.

In order to unify the rules for the processing of asylum applications, the Member States of the European Union adopted the Dublin Convention

in 1990[7]. For its application, it became necessary to determine the identity of asylum seekers and persons detained in connection with the illegal crossing of the Community's external borders. In addition, it was necessary to allow each Member State to check whether a foreigner staying illegally on its territory had applied for asylum in another country. It was recognized then that fingerprints would significantly help in determining the identity of such persons, hence the Council of Europe decided to build a system for the comparison of fingerprints. In 2000, the relevant Regulation established a system for comparing fingerprints of asylum seekers (EURODAC)[8].

The EURODAC system allows EU Member States to identify asylum seekers and persons detained while trying to illegally cross the external EU border. By comparing dactyloscopic data, Member States can determine whether an asylum seeker or foreign national who has been found to be illegal in a Member State has not previously applied for asylum in another Member State or if the asylum seeker has not entered the territory of the Union illegally.

The system consists of a central unit within the Commission, equipped with a computerized central database for the comparison of fingerprints and an electronic data transfer system between the Member States of the Union and the database. In addition to fingerprints, the data sent by the Member States shall include: the Member State of origin, sex, place and date of submission of the asylum application or detention, reference number, date of fingerprints, date of transmission to the Central Unit. Data is collected from people aged 14 or over and then sent to the central unit via national access points[9].

The fingerprinting procedure must be in line with the practice in force in the Member State concerned and the security measures set out in the European Convention on Human Rights and in the United Nations Convention on the Rights of the Child.

---

[7] Convention designating the State responsible for examining applications for asylum filed in one of the Member States of the European Communities, done at Dublin on 15 June 1990, OJ 2005 No. 24 item 194. The Convention was replaced by the Dublin II Regulation in 2003, then Dublin III in 2013. This means that only one Member State is responsible for considering such a request. As a rule, this state is the first Member State whose border was crossed by a foreigner seeking protection. Under the Dublin III Regulation, foreigners are returned to the countries responsible for examining their refugee applications.

[8] Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of the EURODAC system for the comparison of fingerprints for the effective application of the Dublin Convention, OJ EU L 316, December 15, 2000.

[9] Ibidem.

In the case of asylum seekers, the data is stored for ten years. In turn, data on foreigners apprehended when trying to illegally cross the external border are kept for two years from the date of taking fingerprints. However, if a foreigner obtains the right of residence, leaves the territory of the Union or obtains the citizenship of any of the Member States, the data is deleted immediately. It is important that a person or a Member State that suffers damage as a result of an unlawful processing of data or an activity that is incompatible with the rules adopted is entitled to compensation from the Member State responsible for the damage caused. All activities related to the processing of data are monitored by national supervisory authorities, while the steps of the Commission are monitored by the European Data Protection Supervisor.

The concept of intelligent borders

Modernization of the European Union's external border management systems and ensuring that the Schengen area is better prepared to face future challenges has become the basis for adopting the idea of intelligent borders. Since 2008, on the initiative of the European Commission, preparatory work has been carried out for the implementation of several new systems using the achievements of various technologies that will guarantee effective management of travellers' flows. The term Intelligent Borders package appeared in media reports covering three IT systems:

1. The European Border Surveillance System (EUROSUR) to fight more effectively against cross-border organized crime, reduce the number of third-country nationals attempting to enter the European Union illegally and reduce the number of fatalities among illegal immigrants attempting to cross the Mediterranean Sea.
2. An Entry / Exit System (EES) registering in the electronic database the time and place of entry and the duration of short stays of travellers within the European Union Member States. In the future, it would replace the existing passport stamping system.
3. A traveller registration system (RTP) introducing the facilitation of travel to certain groups of third-country nationals, who are often in business or private movement as family members of persons who reside permanently or temporarily in the territory of the European Union. In practice, it is to provide them with simplified border control using automatic gates.

As a result of research on the entry / exit system (EES) and the traveller registration system (RTP), experts in 2016 combined them into one system called the Entry / Exit System (EES). In the same year, the European Commission proposed a new technological solution - a travel information system and travel permits (ETIAS) allowing to collect information on all travellers to the European Union and to allow advance monitoring of illegal migration and security controls. A complement to this system is the introduction by the Council of Europe of the obligation for air carriers to provide passenger name record (PNR data - identity and travel-related information) to the relevant national services. The regulations on the European register of passenger air data were also adopted in 2016.

The concept of creating a European Border Surveillance System (EUROSUR) assumed that its operation would consist in intensive border surveillance and exchange of information between border and police services of EU states, and the main tasks were to quickly identify threats at land and sea external borders of the European Union and increase capacity counteracting these threats. It was also acknowledged that the EUROSUR project will cover issues related to illegal migration, cross-border crime, crisis situations and others affecting border security. The system will help Member States to get a full picture of the situation at the external borders and will contribute to increasing the respond of their national services. EUROSUR will also provide a common technical framework to improve day-to-day cooperation and communication between the relevant services of the Member States and facilitate the use of state-of-the-art technology for border surveillance purposes. The main operational objective remains the exchange of information. The External Borders Fund became the financing source of the project. For the construction and operation of the system in the European Union budget until 2020, 244 million euros have been allocated.

In October 2013, the functioning of the system (EUROSUR) was established by the Regulation of the European Parliament and the Council[10]. Starting from 2 December 2013, the system was implemented in 18 EU Member States on the southern and eastern external borders and in Norway (a country associated with the Schengen group). The remaining 11 EU Member States and countries associated with the Schengen group joined the system from 1December 2014.

[10] Regulation (EU) No 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing a European Border Surveillance System (EUROSUR), U. UE L 295/11 of 6.11.2013.

The central coordination centres are the key element of the system for exchange of information and cooperation in the field of border protection. These centres operate continuously twenty-four hours a day, seven days a week. They provide primarily:

- timely exchange of information and cooperation between border services and other services responsible for security and public order and the Frontex Agency,
- create and maintain national images of the situation,
- support the planning and implementation of national activities in the field of border protection.
- Frontex Agency ensures:
- communication network and analytical tools to enable information exchange,
- creating and maintaining a European picture of the situation,
- technical assistance,
- interoperability of the communication network with any other ICT system as well,
- processing and storage of sensitive information.

The services participating in the EUROSUR system conduct comprehensive and intensive supervision over the borders most endangered of illegal migration – the Mediterranean coasts, forest areas, as well as the open sea and off the coast of North Africa. The system allows Member States to react more quickly not only in the case of individual events, but also in critical situations at the external borders. Particular emphasis was placed on ensuring compliance with fundamental rights and obligations under international law. Priority is given to children, unaccompanied minors or people in need of urgent medical assistance. The Member States and Frontex are obliged to respect the principle of non-refoulement[11] and human dignity in relation to persons in need of international protection. As the exchange of information within EUROSUR is limited to operational information, such as places of incidents and patrols, the possibility of exchanging personal data is very limited.

[11] One of the basic rights of foreigners at risk of persecution in the country of origin. It is based on international efforts to give all people equal opportunities to enjoy human rights, in particular the right to life, freedom from torture and cruelty, inhuman and degrading treatment or punishment, as well as personal freedom and security.

As the exchange of information within EUROSUR is limited to operational information, such as places of incidents and patrols, the possibility of exchanging personal data is very also limited.

Another important element of the security of the European external borders is the entry/exit system (EES), which was adopted in 2016 by a regulation of the European Commission and the Council[12]. The scope of the entry / exit system covers all third-country nationals entering the Schengen area for a short-term stay (maximum 90 days in each 180-day period), regardless of whether travellers are subject to a visa requirement or are exempt from this obligation or possibly citizens of third countries entering the Schengen area on the basis of a traveling visa[13].

The idea of the system is to record data on the entry and exit of third country nationals crossing the external borders of the European Union Member States, taking into account the date, time and place of entry and exit and the possible refusal of entry granted to third-country nationals. The system primarily:

- increase the effectiveness of border checks by calculating and monitoring the duration of authorized stay at the time of entry and exit of third-country nationals entitled to a short-term stay,
- improve the identification of persons who do not meet the conditions for entry or stay on the territory of the Member States,
- will identify people overstaying,
- will allow electronic checking of entry refusal,
- collects statistical data on entries and exits, refusal of entry and overstaying of third-country nationals for the purpose of shaping an effective migration policy of the European Union,
- contribute to the prevention of terrorist offenses by identifying and detaining terrorists and generating information on terrorist travel history.

[12] Regulation of the European Parliament and of the Council establishing an entry/exit system for recording data on entry and exit of third country nationals and entry refusal data with respect to third country nationals crossing the external borders of European Union Member States and specifying the conditions of access to the entry/exit system for prosecuting and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011.

[13] A traveling visa is an authorization issued by a Member State to allow a planned stay in the territory of at least two Member States for a period of more than 90 days in any 180-day period, provided that the applicant does not intend to stay for more than 90 days in any 180-day period on the territory of the same Member State. Source: Regulation of the European Parliament and of the Council establishing an entry/exit system..., op. cit.

The architecture of the entry/exit system will be created by two compatible systems: the central system and the national system. The national border infrastructure will be connected to the central system via a consistent national interface identical for all Member States, which will ensure the possibility of using existing national entry/exit systems. The complement will be the communication channel between the central entry/exit system and the central VIS system. Interoperability with the VIS will allow border guards to directly view data stored in both systems. As a result, visa data can be downloaded and imported to ensure the authenticity and validity of visas, as well as the ability to check the identity of the visa holder at external borders. In each Member State, border, visa and immigration services will be appointed, which will have access to the entry/exit system and the power to enter relevant annotations.

Thanks to the so-called automatic calculator the system will allow for quick and accurate calculation of the number of days of stay of foreigners from third countries, both covered by the visa requirement and those exempt from this obligation. When entering a country it will be possible it will be possible to check in the system the number of days remaining to be used by a foreigner, and when leaving and checking inside the Schengen area, whether the traveller has not exceeded the allowed period of stay. The system also allows border guards to check the length of the authorized stay more quickly and accurately, to withdraw from stamping passports, to provide accurate information to travellers about their period of stay[14].

Particular importance in the system is assigned to biometric identifiers. To launch the system (2020 is expected), the principle of collecting four fingerprints and the image of the face has been adopted. Such a solution will allow verification and identification, taking into account the anticipated capacity of the entry/exit system, and at the same time will allow to limit the amount of data to a reasonable level. The four fingerprints taken during registration will allow to check whether the third country national has already been registered in the system, while the image of the face will ensure the ability to check quickly and automatically at the next entry whether the person subjected to border control is a person registered in the entry / exit system. The amount of personal data collected in the entry / exit system is 26 data items. The right of access to personal data, correcting and removing it is clearly defined and subjected to appropriate guarantees.

[14] See: Ł. Użyczyn, *Inteligentne granice Unii Europejskiej*, „Biuletyn Migracyjny", 43/August, 2013.

The costs incurred in connection with the establishment and functioning of the entry/exit system are covered by the general budget of the European Union. The amount of 791 million euro was calculated with the assumption of a three-year extension period (2017-2019 inclusive), assuming at the same time that the system will start functioning in 2020. After the system is launched, future operational costs incurred by Member States will be covered by national programs implemented under the Internal Security Fund.

A new EU project to improve the safety of travellers at external borders is the automatic travel information system and travel permits (ETIAS)[15] announced by the President of the European Commission in 2016. It will become another large scale system in the area of migration policy. It is also one of the elements of the Union's security in response to terrorist attacks in Europe and an uncontrolled wave of migration. It will be operationally integrated with the already existing SIS, VIS, EURODAC systems and the emerging EES system. The system will apply to third-country nationals who use the visa-free regime[16]. The system will first of all gather information about all travellers to the European Union, enabling to carry out advance checks on illegal migration and security controls.

The ETIAS system will be friendly for travellers, but before entering the Schengen area they will need to obtain a travel permit. The issuing of the permit will take place by the usual procedure - filling out the application via the online form. The application is composed of 27 questions regarding the identity of the person concerned, his travel document, place of stay, contact details, criminal records and previous stays in the European Union. The authors of the project put the following tasks in front of the system[17]:

- checking information submitted by third country nationals. Verification will take place before the passenger has taken a trip to the European Union and will be able to assess whether the person poses a risk to public safety or health or if he/she is at risk of illegal migration,

[15] Similar systems operate in the USA, Canada and Australia. There eventually the border official decides whether or not to enter the country. The European Commission assumes that similar solutions will apply in the European Union.

[16] Council Regulation (EC) No. 539/2001 of March 15, 2001 listing third countries whose citizens must have visas when crossing the external borders, and those whose citizens are exempt from this requirement, OJ EU, L 81/1 from 21.03.2001.

[17] See: European Commission – Press release, Security Union: Commission proposes EU travel information system and travel permits, Brussels, 16 November 2016, access: 10.11.2017.

- automatic processing of the submitted application by other EU information systems (SIS, VIS, Europol and Interpol database, EES, EURODAC, ECRIS), comparison of such a request with a special list of ETIAS people watched and automatic checking of the application to determine if there are actual indications or reasonable grounds for issuing a travel permit or refusing it,
- issuing travel permits in the absence of a hit when searching databases.

It should be noted that the authorization obtained is not a visa. Permits will be issued for a period of 5 years, and their absence will become the basis for refusing entry into the Union. It is assumed that the ETIAS system will be an important step towards better and more intelligent IT systems in the field of cross-border security. The costs of establishing the system oscillate around 212 million euros, and its annual maintenance will reach 85 million euros.

An important step in order to combat illegal migration and strengthen border control more effectively was the introduction in 2004 of the obligation to provide data for travel to the European Union by air carriers[18]. Before accepting passengers on board, at the request of the Member State of destination, data equivalent to a given passport shall be transmitted in advance in order to alert border services to the passengers who could be a threat. Due to increasing terrorist threats and cross-border crime, the Council of Europe adopted in 2016 a directive regulating the mode in which air carriers provide PNR data to passengers (name and surname, date and route, seat number, luggage, contact details, payment method - credit card number and other) and processing of these data[19]. These operations allow law enforcement agencies to identify individuals who have not previously been suspected of having links to crime or terrorism before a detailed analysis of the data reveals that they already have similar relationships. Although some Member States use these data under their own legislation granting such powers to the police or other authorities, the PNR system at EU level harmonizes the legal provisions of the Member States and the protection of personal data. Air carriers shall transmit PNR data by electronic means within 48 hours before scheduled departure and immediately upon comple-

[18] Council Directive 2004/82 / EC of 29 April 2004 on the obligations of carriers to provide passenger data, OJ L EU L 261/24, 6.08.2004.

[19] 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, Journal of Laws EU L 119/132 of 4.05.2016.

tion of the check-in, i.e. after passengers have boarded an airplane preparing for departure, when passengers are no longer able to board or leave. The competent services use the transferred data by comparing PNR data with data contained in various databases of wanted persons and objects.

The results obtained are used, among others to assess passengers before arriving or departing according to specific risk criteria or to identify specific persons, to develop such risk criteria, as well as in specific investigations or legal proceedings. These actions are necessary to prevent, detect, investigate and proceed in cases concerning terrorism and serious crimes such as human smuggling, involvement in a criminal organization, cybercrime, child pornography, arms and ammunition smuggling, ammunition and explosives, etc. PNR data provided by carriers may be detained in the Member State's database for a period of five years.

Supportive IT systems

The complementation of the above presented systems, directly strengthening the cross-border security of the European Union, are two further IT projects fulfilling a supporting role. The first is the European Criminal Records Information System (ECRIS), facilitating the exchange of information on convicted third country nationals between Member States. Thanks to easier and faster access to criminal records, border services and law enforcement agencies become more effective in the fight against terrorism and cross-border organized crime. In turn, the second is the Copernicus Earth Observation Program provides information in the field of security, especially border control and maritime surveillance, but also supports the European Union's external action through the detection and monitoring of trans-regional threats, risk assessment and early warning and monitoring of border areas.

The Criminal Records Information System (ECRIS), established in 2009 by the decision of the European Council[20], is now fully operational. This is a decentralized IT system based on criminal records databases in each of the Member States of the Union, which started operating in 2012. The system created electronic interconnection between Member States enabling the rapid and uniform exchange of information on convictions, which were included in the criminal record systems of these countries, through stan-

[20] Council Decision 2009/316 / JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in accordance with Article 11 Framework Decision 2009/315 / JHA, Journal of the European Union, L 93/33 of 7.04.2009.

dardized electronic formats. The national judicial authorities may receive information on previous convictions handed down in other Member States. The system provides judges, prosecutors, border guards and law enforcement authorities with access, via the central authority designated in each Member State, to complete information on offenses committed by a Union citizen, regardless of the Member State in which the person was convicted in the past. The type of crime and the imposed sanction is transmitted in the form of codes, the meaning of which is identical for all Member States of the European Union.

The functioning of the system has shown unsatisfactory effectiveness over time. Therefore, the update has become a key priority of the European security agenda[21] being implemented by the European Commission. The Agenda proposed extending the ECRIS databases to third country nationals or stateless persons in order to better combat cross-border crime and terrorism. In January 2016, the Commission took legislative action to improve the exchange of information on third country nationals. The application presents the following undertakings and their justifications[22]:

1. Establishment of the central ECRIS-TCN system for third-country nationals. Thanks to a centralized database, it will be possible to quickly check whether a Member State has information on the conviction of a third country national. The improvements presented in the proposal will allow Member States to refer directly to the identified Member States through the ECRIS system for details of the conviction.
2. The system will help to determine the identity of a convicted third country citizen thanks to information stored in the database on: surnames, addresses, fingerprints and face images (if available). This will significantly strengthen the credibility of information on the identity of third-country nationals, which are often less reliable than information on European Union citizens because of the uncertainty regarding the identity documents presented.
3. The system will improve the exchange of information on convicted third country nationals between Member States. This will happen

[21] See: European Security Agenda as of 11/05/2015. In April 2015, the EC presented the European Security Agenda for 2015-2020, in which it defined the priorities of the EU strategy for the European area of internal security. The information indicates the basic documents and publications regarding the agenda, http://oide.sejm.gov.pl/oide/images/files/pigulki/agenda.pdf, access: November 20th, 2017.

[22] European Commission - Press release, Security Union: Commission introduces interoperability of information systems, Brussels, 29 June 2017, 22.11.2017.

thanks to easier and faster access to criminal records, and law enforcement agencies will become more effective in the fight against terrorism and organized crime.

4. The system will enable interoperability with other European Union databases. The centralized ECRIS system will be part of systems developed and managed by the eu-LISA agency, which will enable efficient exchange of information between various EU systems.

The above projects are systematically implemented. In turn, the largest project implemented by the European Union in cooperation with the European Space Agency (ESA)[23] and the European Environment Agency (EEA)[24] is the Copernicus program. It is an important contribution to building the Global Earth Observation System of Systems (GEOSS) created within the Group for Earth Observation (GEO). It is a civilian program and under civilian control directed at users, based on existing national and European capabilities.

The initiative was taken at the end of the 90s of the last century with the intention of developing methods for monitoring the state of the environment from the satellite, air and ground perspective. It was recognized then that satellite observations of the earth are one of the best examples of the practical use of space and satellite techniques. Satellite observation is a method of remote gathering of information, which in some applications replaces, and in many others complements aeronautical and ground observations and measurements. It consists in remotely collecting information through passive observation or through lighting of the area of interest and measurement of reflected radiation[25]. Therefore, the following general objectives are outlined in the Copernicus program:

[23] The European Space Agency (ESA) was set up under the Convention signed in Paris on May 30, 1975. Is an intergovernmental organization. Its task is to implement a common European program for research and use of space. The agency also supports the development of a modern and competitive industry in the Member States. The ESA consists of 22 Member States, including Poland (from November 2012). The ESA headquarters are located in Paris, but the agency operates in several locations in which ESA branches are located.
Source: http://www.esa.int/pol/ESA_in_your_country/Poland/Poznaj_ESA, access: 20.11.2017.

[24] The European Environment Agency (EEA) is one of the EU agencies. Its task is to provide reliable and objective information on environmental protection. It is the main source of information for entities involved in the development, adoption, implementation and evaluation of environmental policy and for the public. The Regulation establishing the EEA dates from 1990 and entered into force in 1993 as soon as the decision on the location of its headquarters in Copenhagen was taken. The Agency currently has 33 Member States and six cooperating States.
Source: https://www.eea.europa.eu/pl/about-us/who/who-we-are, access: 20.11.2017.

[25] See: B. Mikołajek-Zielińska, European program of global monitoring of the environment and security of Copernicus. Analysis of Poland's participation in the program and the use of its effects by Polish institutions, Department of Strategy, Ministry of Science and Higher Education,

- monitoring the Earth to support environmental protection and actions in the field of civil protection and civil security,
- maximizing socio-economic benefits related to sustainable economic and social growth,
- supporting the European space sector in the development and implementation of innovative Earth observation systems.

The Copernicus program consists of three components:

- service component – providing users with unified data and information,
- the space component – ensuring observations from space,
- ground component – providing data obtained from terrestrial, marine or airborne sensors.

The task of the Copernicus Program is to provide users with reliable and precise information in six main thematic areas: monitoring the terrestrial environment, monitoring the marine environment, monitoring the state of the atmosphere, crisis situations, security and climate change. From the point of view of ensuring cross-border security, the most important information comes from the area of security, and its scope includes:

- maritime surveillance: maritime borders, illegal immigrants, smuggling and illegal trade, piracy, sensitive loads, etc.,
- supervision of infrastructure: land borders, critical infrastructure, e.g. pipelines,
- support for peace activities: monitoring of population, resources, e.g. water,
- recognition and early warning,
- support for operations in crisis management.

The data collected in the form of thematic maps, databases, reports etc. and collected and processed by means of satellites and terrestrial measurements will allow for more effective management of the environment and improve the security of citizens. The provided information services are made available to users free of charge and without any obstacles. The main users in the area of security are: Frontex Agency, European Commission, European Union Military Staff, peaceful European and UN missions, International Atomic Energy Agency, law enforcement agencies, anti-terror agencies, maritime police organizations and drug smuggling detection, Member States navies,

http://docplayer.pl/4024457-European-program-global-monitoring-ofenvironmental-and-security-copernicus.html, access: 19.11.2017.

industry oil and gas, ship owners[26], etc. The pool of financial resources for the implementation of activities in the years 2014-2020 is approximately EUR 4.4 billion.

Summary

Presented solutions consisting of on the project of smart borders are to ensure effective management of the external borders of the European Union thanks to the use of state-of-the-art technologies. The systems are extremely complicated technically, entail huge financial costs and do not guarantee trouble-free operation. Their full launch will undoubtedly lead to increased surveillance and collection of personal data at borders. There is some risk, the issue often taken by critics of the concept of intelligent borders, that the benefits of these proposals are not at all obvious, and the social and economic costs – very large. The nearest reality will verify all opinions and expectations. Undoubtedly, the management of the external borders of the European Union should take advantage of various possibilities, from traditional ones to the latest technological solutions. These actions should be guided by the objective of increasing the Community's internal security.

Bibliography

Użyczyn Ł., *Inteligentne granice Unii Europejskiej*, „Biuletyn Migracyjny", 43/sierpień, 2013.

Websites:

http://docplayer.pl/4024457-Europejski-program-globalnego-monitoringu-srodowiska-i-bezpieczenstwa-copernicus.html, Mikołajek-Zielińska B., *Europejski program globalnego monitoringu środowiska i bezpieczeństwa Copernicus. Analiza udziału Polski w programie i wykorzystanie jego efektów przez polskie instytucje*, Departament Strategii Ministerstwa Nauki i Szkolnictwa Wyższego.

http://www.esa.int/pol/ESA_in_your_country/Poland/Poznaj_ESA, Poznaj ESA.

https://www.eea.europa.eu/pl/about-us/who/who-we-are, Europejska Agencja Środowiska, co robimy.

http://oide.sejm.gov.pl/oide/images/files/pigulki/agenda.pdf, Europejska Agenda Bezpieczeństwa, Materiały OIDE.

[26] Ibidem.