Zawadzka, S., 2022. *Biometric technology in European Union border management after 2015*, Przegląd Geopolityczny, 39, s. 93-113.

Sylwia ZAWADZKA
Wroclaw University

BIOMETRIC TECHNOLOGY IN EUROPEAN UNION BORDER MANAGEMENT AFTER 2015

Abstract:

The aim of this paper is to examine the evolution of biometric control of the movement of people in the EU after the migration crisis and the impact of new large-scale IT systems on improving EU security. In conditions of increased mobility and challenges related to illegal migration and organized crime, it is necessary to improve migration security in the Schengen area. The answer to these challenges is the implementation of the EU package of "smart borders", which is associated with the use of innovative technologies of control and information processing. The article presents a comparative analysis of two systems: Entry and Exit System (EES) and European Travel Information and Authorization System (ETIAS). Based on the Regulations establishing the new systems, the most important issues concerning their origins, objectives and principles of operation were analyzed. The main element of the research process was to identify and evaluate the determinants which indicate the usefulness of the systems in improving security in the Schengen area, as well as to assess the process of biometric authentication and its impact on the early detection of cross-border threats.

Keywords: biometrics, EES, ETIAS, migration crisis, Schengen area, smart borders.

Growing migratory pressures and the need to control the movement of people

In an environment of increased mobility and the challenges of illegal migration and organized crime, it is imperative to improve migration security in the EU. The ‘smart borders’ package implemented by the EU institutions is related to the use of innovative technologies for control and information processing. Therefore, it is part of the institutional and legal framework of intelligent border administration. The new large-scale systems, complementing the Schengen *acquis* in this area, are primarily to detect any irregularities related to the stay of foreigners on the territory of the Member States through the use of data (including biometric data) collected in various databases.

Already after the terrorist attacks in the USA in 2001, the European Union took steps to include provisions on biometrics in EU legislation, which after the 2015 migration crisis became one of the determinants of effective border management and countering threats such as illegal border crossing or terrorism. The phenomenon of biometrics means the use of specific and unique human features (such as fingerprints or facial image) in order to uniquely identify the identity. It should be stated that the application of biometrics at the EU level is wide, and after 2015 a significant development of this phenomenon has been observed.

The article presents the development of the phenomenon of biometrics at the level of using biometric data via large-scale IT systems. The main part of the paper presents the origins and basic goals of creating the Entry Exit System (EES), as well as the European Travel Information and Authorization System (ETIAS). Based on the analysis of official EU legal acts, the rules and legal framework of the new systems were defined. The usefulness of the systems in terms of improving security and improving border management in the Schengen area was assessed. It is worth noting that, despite the establishment of the legal basis in 2017 and 2018, there is still a noticeable deficit in scientific studies devoted to the issues of new large-scale systems and the broadly understood concept of biometric control of the movement of people.

The need to implement new system solutions resulted from the challenges that the European Union had to face. Their intensification took place after the refugee crisis in 2015. The scale of these challenges can be illustrated on the example of selected statistical data, which are the starting point for the analysis of the functionality of ‘smart’ border control systems in terms of improving security. In 2014, nearly 16 million uniform visas (Schengen visa type C) were issued to non-EU travelers traveling to the Schengen area. In 2015, more than 50 million third-country nationals traveled to the EU for tourism, education and business purposes, thus responsible for over 200 million crossings of the external border of the Schengen area. It should be emphasized at this point that currently citizens of over 60 countries are exempt from the visa requirement and their data is not processed, so there is a clear information gap with regard to this category of foreigners. Every year, the external borders of the EU are crossed by nearly 700 million EU citizens and third-country nationals. Moreover, it is assumed that this number will gradually increase in the future.

According to Eurostat data, a total of 4.4 million people emigrated to one of the EU Member States in 2017. About 2.4 million immigrants came from third countries, while 1.3 million were nationals of another Member State. The rest of the immigrants were people with the citizenship of the destination country (returning citizens) and stateless persons. The total number of third-country nationals residing in one of the Member States at the beginning of 2018 was 22.3 million, which was 4.4%. of the EU population[1].

One of the greatest threats to European security is the phenomenon of illegal immigration. The data of the European Border and Coast Guard Agency (Frontex) show that in 2015-2016, a total of about 2.3 million cases of illegal crossing of the external border were detected, with over 1.8 million crossings in 2015[2]. In 2017, this number fell to around 204,000, but the migratory pressure still remains relatively high. In addition, 439,505 people were refused entry to the Schengen area in 2017[3].

On the other hand, on the basis of Eurostat data, it is possible to analyze trends related to the phenomenon of illegal stay of third-country nationals on the territory of the EU. In 2015, this number was 2.1 million. In 2016, it dropped to the level of 983,000, while in 2017, over 618,000 people resided illegally in the EU. (Eurostat, Third country nationals, 2019a). Threats related to the processes of illegal border crossing and unauthorized stay in the Member States are not the subject of this article, therefore they will not be analyzed in detail, however, the severity of the problem was the main determinant of the introduction of new reforms and modernized control mechanisms.

The first stage in creating systems based on modern personal data control technologies was the so-called *Smart Borders Initiative* of 2011, which specified the issues contained in the Communication of the European Commission of 2008 (Press release IP/08/215). Both

[1] *Third country nationals found to be illegally present - annual data (rounded),* Eurostat, 2019. http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=migr_eipre&lang=en [15.11.21]

[2] https://frontex.europa.eu/assets/Publications/Risk_Analysis/Annula_Risk_Analysis_2016.pdf, [13.10.21].

[3] European Parliamentary Research Service, 2019. *Migration and asylum*, http://www.europarl.europa.eu/thinktank/infographics/migration/public/index.html?page=migration, 15.09.21.

documents confirm that in the face of new challenges related to mobility to the EU and facing future problems, it is necessary to implement a modern and effective system of managing the flow of travelers. According to the documents, the purpose of using technologies based on biometrics was to '*make life easier for foreigners who frequently travel to the EU and to improve the system of monitoring third-country nationals who cross the borders*' (Press release, IP/11/1234).

Similar assumptions were set out in the 2013 'Smart Borders' Communication. According to its conclusions: '*the use of new technologies will enable smoother and faster border crossing for third-country nationals wishing to enter the EU. The aim is to facilitate access for foreigners to the EU. It will be in the interest of not only travelers, but also of the European economy*' (Press release, IP/13/162). Mobility issues were presented as a priority, and the issue of ensuring the safety of citizens as a complementary element. The document presents specific system foundations and proposes the implementation of two new mechanisms: Registered Traveler Program and Entry/Exit System. The proposal for a regulation on the RTP was withdrawn by the Commission in 2016. In turn, the Communication of 6 April 2016 proposed the shape of the regulation on the scope of use of the EES.

Following the intensification of threats related to migration pressure, the refugee crisis and terrorist attacks, the narrative convention has also changed. This was confirmed by the 2016 statement of Jean-Claude Juncker, in which he wrote that '(...) *tolerance must not be shown at the expense of our security* (...) *We need to know who is crossing our borders*' (Juncker 2016). This change of narrative is in line with the opinions of circles and researchers who have already warned of the consequences of an uncontrolled influx of migrants following the *„Herzlich Wilkommen"* policy (Wilczyński, 2015).

Biometric data in legal terms

At the EU level, the provisions on biometric data have been regulated in the *Regulation* (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the processing of personal data and on the free movement of such data, and repealing *Directive 95/46/EC*. According to the provisions of the document, biometric data are personal data related to physical, behavioral or physiological characteristics, such as facial image or fingerprints, which at the level of technical processing allow for unambiguous identification (Art. 4, par. 14). From May 25, 2018, biometric data has been classified as sensitive data, the processing of which is allowed only in exceptional situations specified in the Regulation. In turn, data processing itself means '*an operation or a set of operations performed on personal data or sets of personal data in an automated or non-automated manner, such as collecting, recording, organizing, storing, adapting or modifying, downloading, viewing, using, disclosing by sending, disseminating or otherwise making available, adjusting or combining, limiting, deleting or destroying*' (Art. 4, par. 2).

The use of biometric data for a purpose other than that provided for in the Regulation would be a serious interference with the privacy of the persons whose data is processed. Moreover, it could pose a direct threat to the safety of these people. In art. 9. of *Regulation* it is indicated, *inter alia*, for cases that allow the processing of biometric data in terms of the protection of public health, ensuring security and counteracting cross-border threats:

'*- the data subject has expressly consented to the processing of these personal data for one or more specific purposes, unless Union law or law Member States provide that the data subject may not lift the prohibition on processing these data;*

- processing is necessary to protect the vital interests of the data subject or another natural person, and the data subject is physically or legally incapable of giving consent;

- the processing relates to personal data which are manifestly made public by the data subject;

- processing is necessary for the establishment, exercise or defense of legal claims or in the course of the administration of justice by courts;

- processing is necessary for reasons of important public interest (...) do not infringe the essence of the right to data protection and provide for appropriate and specific measures to protect the fundamental rights and interests of the data subject;

- processing is necessary for reasons of public interest in the field of public health, such as protection against serious cross-border health threats (...);

- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or for statistical purposes pursuant to Art. 89 para. 1, on the basis of EU or Member State law, which are proportionate to the aim pursued, do not infringe the essence of the right to data protection and provide for appropriate, specific measures to protect the fundamental rights and interests of the data subject' (art. 9).

The use of new technologies in the field of personal data processing has also become the subject of the work of the European Commission, which issued a *White Paper* in 2020. The document was to define the risks of using artificial intelligence for data processing purposes, as well as indicate recommendations in this regard. An important aspect concerned facial recognition systems and biometric data. As indicated, the collection and use of biometric data for the purposes of remote identity identification carries a particular risk for the fundamental rights of citizens. Therefore, it was emphasized that remote facial recognition must be considered from the angle of the right to respect for private life and the protection of personal data. Biometric data may be processed in public places in the situations indicated in art. 9 GDPR when it is important to the public interest. In line with the applicable EU data protection law and the provisions of the Charter of Fundamental Rights of the EU, artificial intelligence may be used for remote biometric identification purposes only if such use is duly justified, proportionate and subject to appropriate safeguards to protect citizens' privacy (*White Paper*, 2020).

It is worth noting that the functioning of individual institutions, IT systems and databases that introduce, collect and process biometric data are regulated by separate documents establishing these mechanisms, which regulate in detail the scope and cases of using biometric data. The European Data Protection Supervisor controls the proper use of data, i.e. in accordance with the legal scope and respect for the principle of privacy. Its role is also to monitor the impact of new technologies on data protection.

Evolution of biometrics in the Schengen Information System, Visa Information System and Eurodac

So far, AFSJ[4] has had three key large-scale IT systems managed by the eu-LISA Agency: the Schengen Information System (SIS), the Visa Information System (VIS) and Eurodac. The first of these was created as a result of the abolition of border controls between the countries of the Schengen Area. The legal basis for the operation of the second generation SIS is *Regulation (EC) No 1987/2006* and *Council Decision2007/533/JHA*. Until 28 December 2021, SIS II will operate under three new Regulations: *Regulation(EU) 2018/1860* (return of

[4] The area of freedom, security and justice (AFSJ) is a collection of home affairs and justice policies designed to ensure security, rights and free movement within the EU.

illegally staying third-country nationals); *Regulation (EU) 2018/1861* (border checks); *Regulation (EU) 2018/1862* (police cooperation). SIS II collects data on persons who have gone missing, persons who may have committed crimes and items that may have been used in such acts. The system is primarily to facilitate the identification of persons from third countries who want to illegally cross the border of the Schengen area; persons against whom a European Arrest Warrant has been issued; as well as searching for persons to facilitate judicial procedures or the prosecution of criminal offenses (Art. 26-38 of the SIS Decision). Alerts in SIS II shall contain data such as: name and surname; specific, objective physical characteristics that cannot be changed; place and date of birth; sex; photographs; fingerprints; citizenship; information whether the person is armed, aggressive or a fugitive; reason for the entry; issuing authority; reference to the decision giving rise to the entry; actions to be taken; the type of offense (Art. 20 of the SIS Decision; Art. 20 of the SIS *Regulation*).

In December 2016, as a result of the threats related to the migration crisis, as well as the intensification of terrorist attacks in EU countries, the European Commission started a debate on the need to strengthen the SIS in terms of modernizing the system and introducing new categories of alerts. The new package of regulations in the form of three new Regulations, adopted in 2018, is to prevent threats such as illegal border crossing or terrorism. The regulations, to be implemented by the end of December 2021, add new categories of alerts: for the purposes of the preliminary interview, being an intermediate step between discreet and in-depth checks, allowing the person to be interviewed; alerts on unknown suspects or wanted persons, i.e. entering into SIS fingerprints or handprints found at the scene of a serious crime or terrorist incident and recognized as belonging to the perpetrator; preventive alerts for children at risk of parental abduction, as well as vulnerable children and persons who must be prevented from traveling for their own protection (e.g. trafficking in human beings); alerts for the purpose of return, i.e. the recording of return decisions of illegally staying third-country nationals. They also extend the list of items that may be entered for, e.g. for false documents and high value identifiable items and IT equipment. In addition, it becomes obligatory to enter alerts on entry bans for third-country nationals in the SIS (Press release, 19/11/2018).

The second basic system allowing to manage migration in the AFSJ is the Visa Information System, established in 2011 in order to facilitate the procedures related to issuing short-term visas for stay in the Schengen Area countries for third-country nationals. For several years, there has been a debate on the development and modernization of this system as well. On December 8, 2020, the EU Council and the European Parliament, as the main EU institutions participating in the legislative procedure, reached an agreement to adopt new regulations to extend and improve the functionality of the VIS. The main priorities of the new Regulation are to increase the procedures for examining visa applications; integrating the system of long-stay visas and residence permits into the database and ensuring interoperability with other systems and databases. The new regulations are to regulate the possibility of checking individual applicants in other databases of individual systems and institutions. In addition, international carriers will have access to information on whether individual visa or residence documents are valid. As for biometrics, the most important changes relate to the age of the people for whom such alerts are made. In order to tackle child trafficking, the fingerprinting age will be lowered from 12 to 6. There will also be an upper age limit. According to these provisions, the fingerprint data of persons aged over 75 will not be included in the VIS. The current paper photo will be replaced with an image of the face taken in place, which is of sufficient resolution and quality to be used for automated biometric matching.

The European Automated Fingerprint Identification System collects fingerprint data of asylum seekers in the EU. It allows to verify whether the applicant has not already lodged an application for asylum in another Member State or has not been previously detained while attempting to enter the EU illegally. It also allows to check which Member State is responsible for consideration the asylum application (*Regulation, 603/2013*). In May 2016, the Commission launched a debate on the reform of the EU's asylum rules, including the introduction of new regulations on the Eurodac base. Their aim is to improve the system by expanding the amount of collected data (e.g. with a face image); extending its scope to data on third-country nationals whose status in the EU is irregular and who do not apply for asylum, as well as facilitating access to the database for law enforcement authorities (Press release, 9/12/2016).

Entry/Exit System as an instrument for managing migration processes

The legal basis defining the conditions, objectives and principles for establishing the EES is the Regulation of the European Parliament and the EU Council of 30 November 2017. According to its content, the new system applies to third-country nationals, both covered and exempt from the visa requirement, who are subject to the short-term stay. The data of persons belonging to the first of the above-mentioned categories of foreigners (visa applicants) are collected in the Visa Information System (VIS), however, there is a clear information gap in relation to the latter group. Their data is not comprehensively stored in any of the existing large-scale systems (Zawadzka, 2019, p. 107).

The structure of current systems is also fragmented. Data relating to different categories of persons are stored in separate, autonomous databases, while the level of interoperability between them is not sufficient for the effective management of external borders. The EES was planned based on the assumptions of interoperability with the VIS, thanks to which the information located in the VIS will be available to authorized authorities using the Entry/Exit System. In turn, the relevant visa authorities and border services using the VIS will be able to consult the EES from the level of the VIS in order to facilitate the processing of visa applications and decisions (*Regulation, 2017/2226*, Art. 8). Downloading visa data from the VIS and importing them into the EES and updating VIS data from the EES will prevent duplication of this information in different systems while enhancing the comprehensiveness of data management.

The objectives of establishing the EES can be divided into three categories: 1) related to the improvement of border controls; 2) related to the facilitation of the crossing of external borders;3) strictly related to the prevention of serious crime. The first category includes: the need to increase the efficiency of border checks thanks to the monitoring and automatic calculation of the period of authorized stay at the time of entry and exit of persons covered by the right to a short stay; the possibility of identifying foreigners who do not meet the conditions for entry or stay on the territory of the Member States; the possibility of identifying persons exceeding the period of authorized stay; possibility of electronic verification of refusals of entry; granting visa authorities access to information on previous visas; collecting statistical data on the entry and exit of nationals of certain third countries and their exceeding the authorized period of stay in order to shape the EU migration policy. The second category of objectives includes: facilitating and streamlining the process of border checks by automating most of the related activities and the possibility of obtaining quick information on the permitted period of stay. The last category is strictly related to the protection of citizens of the Member States and the prevention of crimes in the Area of Freedom, Security and Justice (Zawadzka, 2019, pp. 107-109). This applies in particular to combating identity fraud and the unauthorized use of a counterfeit or stolen travel document; prevention of serious crimes, especially terrorist crimes; gathering information for the purpose of conducting preparatory proceedings in the field of these crimes (identifying perpetrators or persons suspected of committing serious crimes who have crossed external borders) (*Regulation, 2017/2226*, art. 6).

The above objectives can also be divided according to the category of the entity that is to realize them by exercising the right to access selected data under certain conditions and in accordance with the principles of purposefulness, necessity and proportionality. These are objectives pursued by the competent authorities of the Member States (border guards, immigration authorities, visa authorities) and non-state actors such as Europol with limited access to EES data to detect and prevent the most serious crimes. It is important for determining the impact of the new system on the level of security in the Schengen area. The high degree of sensitivity of data (including biometric data) entered into the system determines the scope of their use. It must comply with the principles adopted in the *Convention for the Protection of Human Rights and Fundamental Freedoms* (1951), the EU *Charter of Fundamental Rights* (2000) and the UN *Convention on the Rights of the Child* (1990), which is to prevent abuse and violation of the rights of third-country nationals (*Regulation, 2017/2226*, art. 10). This excludes voluntary and unlimited access by security services, which, on the one hand, guarantees that foreigners respect their fundamental rights to privacy and data protection, and, on the other hand, prevents the full use of the potential of the new system in terms of increasing the security of EU citizens when there are grounds for a crime, but they are insufficient to trigger the information access procedure.

Modern technological solutions will enable the countries using the system automation many activities related to the processes of entering, collecting and verifying the data of third-country nationals to which the EES will apply. Using a self-service system (so-called ‘self-service kiosks’), travelers can register their data, creating an individual register composed of a personal register and a register of border crossings, as well as check whether their data is already saved and perform border checks. During this process, the system automatically verifies alphanumeric data and biometric data, which are collected on the spot and compared with the information in the system. In addition, travelers answer a set of questions that are normally asked by officers of the relevant services during the traditional check-in. When a travel document is scanned in the self-service system, checks of security databases are launched, which means that the system searches certain databases in terms of looking for people who threaten security (*Regulation, 2017/2226*, art. 14).

This is in line with the Regulation of the European Parliament and of the Council of 15 March 2017, introducing the necessity to verify the travel documents of all persons, regardless of nationality, to use the Schengen Information System (SIS II) and the Interpol database containing the date of stolen or lost travel documents (Stolen and Lost Travel Documents database) (*Regulation, 2017/458*). These databases will also be searched by the EES in order to fight terrorism, organized crime and detect cases of multiple identities.

Third-country nationals' data entered into the system can be divided into several categories. The first is the travellers' personal data, such as: name, surname, citizenship, date of birth or gender. The second category relates to the travel documents held by a third-country national: the type and number of the relevant document, the code of the issuing country and its expiry date. If the information concerns nationals of countries subject to the short-stay visa requirement, the visa data should also be taken into account in this case, in particular: visa sticker number, code of the issuing Member State, end date of the authorized stay. Another type of information collected is border crossing data. The following may be classified as: date, time, place of entry (crossing the external border) and the name of the authority that authorized it. Each entry and exit is recorded in the register of border crossings. In certain cases, the system also records information related to the refusal of entry or the cancellation of the decision on the residence permit (*Regulation, 2017/2226*, art. 16 20).

Personal information listed above is included in the alphanumeric data directory. Another category, important in the context of increasing the level of security and use in modern control systems, are biometric data, such as facial image and fingerprints (dactyloscopic data). Determining the identity of the traveler in accordance with the implementation assumptions is to be based on the compliance of one biometric feature. All the information indicated will be kept in the EES databases for three years if the stay in the territory of the Member States ended within the prescribed period or for five years if the period of stay was extended, i.e. no alert was registered regarding the exit after the permitted period (*Regulation, 2017/2226*, Article 34).

In addition to citizens subject to the obligation to register their data with the EES and border officers, the system will also be used by visa authorities processing visa applications; immigration authorities to verify the identity and verify that all conditions for the legality of entry and stay have been met. Moreover, the Member States designate a special list of authorities authorized to consult the information collected in the EES for the purpose of law enforcement (*Regulation, 2017/2226*, art. 29).

State support in combating organized crime is also guaranteed by access to system data for the purpose of detecting serious crime. Such access, upon request and approval, shall be granted to the competent body of Europol. Viewing the data in this case is possible only if it is necessary and in accordance with the principle of proportionality and there is evidence or reasonable grounds justifying access by the possibility of increasing the detection of crimes and their perpetrators (Zawadzka, 2019, 107-112).

The EES is to strengthen the security of the European Union by identifying people who in various ways violate the right to stay in the territory of the Member States and pose a threat to public peace. The first group are foreigners who excessively extend the permitted period of a short-stay. The system will verify the traveller's status in terms of the legality of stay by automatically calculating the maximum remaining time until the deadline for leaving the Member States and recording all related information in the border crossing register.

An important document is the implementing decision of the European Commission, adopted on October 15, 2018 (*Commission Implementing Decision 2018/1548*). It lays down measures to establish, on the basis of EES data, a special list of foreigners exceeding the authorized period of stay and the procedures for making this list available to all Member States in order to warn against the possibility of illegal presence of such persons in their territory.

Another type of threats, the detection of which may increase thanks to the use of modern technologies based on biometrics, are identity-related crimes related to the illegal use of forged or stolen travel documents in order to enter the territory of the country of destination. EES is to be based on a pan-European IT network mechanism consisting of national interfaces linked to a central database managed at supranational level. This solution will allow for effective verification of personal data regardless of the place of crossing the external borders and automatic access to the necessary information, which is crucial for the effective and immediate operation of security services. Due to the automation of border controls, the EES electronic alert mechanisms will replace the procedures for manual stamping of travel documents, which will also affect border security by providing more reliable information on border crossing. Stamps in the passports of foreigners that indicate the dates of entry and exit are the only method available to immigration authorities and border guards to calculate the authorized period of stay. It is a procedure prone to errors taking into account the possibility of forgery, loss, destruction of the document or the lack of sufficient legibility of the stamp (eu-Lisa, *Report*, 97).

The EES also aims to prevent the entry into the territory of the Member States of persons whose presence may pose a threat to internal security, health and public order. They may be perpetrators of serious crimes or persons suspected of terrorist activity. This is a particular challenge related to the increasing number of terrorist attacks in EU countries.

According to the results of a report by Europol, in 2017, the number of attacks (committed, prevented and unsuccessful) gradually increased between 2013 and 2015. In 2013, there were 152 of them, while in 2015 - 211 in total. A decline was recorded in 2016 (142 attacks), but the threat remains high and border protection reforms are designed to prevent it.The statistics on people arrested in the European Union for terrorist activities in 2013-2016, which are also based on an upward trend, are also noteworthy. In 2013, 535 people were arrested on this charge, a year later - 774, and in 2015 - 1077. In turn, in 2016 there was a change in the tendency and a decrease in the number of people arrested on charges of terrorism to 1002. At the same time, a higher percentage, compared to 2016, were criminals motivated by the ideology of jihad (50% in 2015 and 70% in 2016).[5]

The aim of the new systems, based on modern control technologies, is to detect such persons before they cross external

[5] http://rcb.gov.pl/wspolczesne-oblicze-terroryzmu-w-unii-europejskiej/, 18.11.21.

borders and to identify those who may already be in the EU. The entry and exit system will use biometric data for this purpose, the collection and registration of which in the system will be a condition for crossing the border. In many cases, alphanumeric data is not enough, especially when the offender has multiple identities. In this case, the European Commission's plans to reform the interoperability of all large-scale systems are important, which are to be based on the creation of several components of intersystem cooperation, including the identity multiplication module, the purpose of which will be to detect such situations (Press release, IP/17/1788).

European Travel Information and Authorization System and its impact on improving EU safety

After the draft regulation establishing the European Travel Information and Authorization System was drafted in November 2016, Jean-Claude Juncker stated that the main goal of the Commission's actions in terms of implementing the new solutions is to increase the information resources on people crossing the border and to create a permitting system for travel to the Member States after an electronic prior check which would precede the proper check at border crossing points (Press release, IP / 16/3674).

The first official document that referred to the creation of new EU IT systems and the development of personal data infrastructure, especially with regard to visa-exempt foreigners, was the aforementioned Commission Communication of April 6, 2016. The document emphasizes that officers of the competent services responsible for external border controls, do not have information on this group of foreigners. Thus, it was announced that the work on a project of a system that could fill the information gap will be started. The analysis of its capabilities was completed in November 2016. The basic principles and objectives of the system's operation were developed, which were extended in the relevant Regulation of September 12, 2018 establishing ETIAS.

According to art. 4. of this Regulation, the primary objective of the new IT system is to strengthen the security of the Member States by carefully assessing applicants for a travel authorization before their arrival at the external borders. In this respect, ETIAS differs from an EES. The latter is also to apply to foreigners subject to the visa obligation. Moreover, the registration of personal data in the EES takes place already at border crossing points. Nevertheless, the functions of both are closely related to each other. ETIAS is intended not only to reduce the deficit of information on the indicated category of people, but above all to enable their initial assessment. The system is to determine whether third-country nationals exempted from the short-stay visa requirement do not pose a serious threat to internal security and whether a trip to the Schengen area is associated with the risk of illegal immigration or a high epidemiological risk. Persons whose presence on the territory of the Member States could constitute a potential threat to public peace and health will be identified even before the proper border control. Taking these assumptions into account, ETIAS complements the EES functionality as an instrument for intelligent border management and at the same time a means of building a Security Union (Zawadzka, 2019, 110-112).

The system is also to support the goals and activities of the authorities using the second generation SIS in the context of the identification of wanted persons (in order to arrest or initiate extradition procedures); missing; participating in court proceedings and other categories of persons whose data is stored in SIS II (*Regulation, 2018/1240*, art. 4). The main aim of ETIAS is to help prevent the entry into the territory of the Member States of persons who could become the perpetrators of serious crimes, such as terrorist attacks. However, ETIAS cannot be defined as a fully autonomous visa policy instrument. It is part of a coherent border management policy and should be treated as a complementary mechanism to the existing solutions (Kosińska, 2017).

An important issue in the analysis of the practical use of ETIAS is its basic technical structure, which includes national units operated by the relevant authorities of the Member States, a central unit managed by Frontex and an information system coordinated by eu-LISA. The information system is particularly important. It is composed of the following elements: the ETIAS Central System, including the watchlist[6]; a national uniform interface in each Member State; an encrypted communication infrastructure between the Central System and the National Uniform Interfaces; a public website and application for mobile devices; e-mail function; a secured account feature enabling applicants to provide any additional information or documents as required; verification tools for applicants; a mechanism enabling applicants to

[6] Such a list is based on information related to serious crime, including terrorist offenses. The list includes the data of persons suspected of committing or participating in such crimes (S.Z.), for more information: *Regulation, 2018/1240*, art. 34.

grant or withdraw consent for an additional retention period of their application file and a portal for carriers who use it to obtain information on the status of a permit for the entry of a third-country national into the territory of the Union(*Regulation, 2018/1240*, art. 6).

A third-country national who is obliged to apply for a travel permit to an EU Member State fills in the form by providing basic data, including in particular: name and surname; gender, place of birth; address; citizenship; parents' data; details of the travel document he is using; level of education and profession; e-mail address; Member State of the first intended stay. In the next step, the applicant answers the questions that will allow to determine the degree of risk caused by the presence of the person in the EU. The questions mainly concern the crimes committed in the last 10 years. If the question concerns terrorist offenses, an answer is required within the last 20 years. The Member State on whose territory they were committed should also be indicated. Another category of questions concerns the stay in war-torn areas, as well as the reasons for this stay (*Regulation, 2018/1240*, art. 17). In terms of reducing the risk to public health, it is important to analyze the health condition of the applicant in terms of epidemiological risk, and therefore a separate part of the questions will also concern these issues. By submitting an application, the person concerned certifies the reliability, completeness, authenticity and correctness of all information provided. Moreover, the data processed in ETIAS should be compared with the databases of other information systems (SIS, VIS, EES, Eurodac), which is why it is so important in the process of implementing new systems to strengthen their interoperability with the existing ones.

Application will be subject to automated processing. At this stage, ETIAS compares the applicant's data with the information in the above-mentioned systems in order to find 'hits' or inter-system convergences of information that would indicate the threat posed by the presence of a person in the territory of a Member State. The specified hits are primarily intended to verify that the travel document used by the applicant is present in the systems containing information on stolen or lost documents, as well as whether there is an alert on it in other systems (e.g. SIS II) for entry or visa refusal. In addition, automatic processing is to show whether the foreigner has been indicated in other systems as a wanted or missing person and whether he poses a threat to others. Another category of undesirable persons are third-country nationals who have exceeded the authorized period of stay. According to the assumption of the ETIAS Regulation, in the event of a lack of a hit, the system generates an automatic travel authorization, and if the initial data verification process indicates a specific hit, the application is consulted at the level of the central unit in terms of specific risk indicators. According to art. 26: '*Where an automated processing operation pursuant to art. 20 paragraph 2-5 generated at least one hit, the request is processed manually by the ETIAS National Unit of the Member State responsible*' (*Regulation, 2018/1240*, art. 26). It should be noted, however, that the responsible country is the Member State which provided the data generating the specific hit. After this procedure, the national unit issues an authorization or a refusal to travel.

ETIAS is to be a response to the EU security dilemma related to the migration crisis and the threat posed by terrorist groups. On the one hand, they will help maintain visa-free travel with countries with which the EU has concluded visa liberalization agreements, and on the other hand, they will strengthen the security of the Member States by increasing the information potential of foreigners who want to cross the external borders of the Union.

Moreover, the procedure related to the refusal to issue a travel authorization is to be a preventive measure aimed at 'closing' the external borders to persons whose presence in a Member State is undesirable and poses a risk of illegal immigration or increases the epidemiological risk. Given the preliminary analysis of the information in the electronic system and the possibility of refusing applications from third-country nationals who do not meet the entry conditions, ETIAS increases the chance of preventing such threats.

Conclusions

The challenges of the second decade of the 21st century forced the EU authorities to redefine the concept of security and protection of external borders. The threats related to illegal migration, organized crime and the increase in the number of terrorist attacks played an important role in the public debate. They can be considered as the main determinants of the introduction of reforms in border management policy and the implementation of innovative 'smart control' systems. Their priority is to intensify the fight against threats and broadly understood prevention, especially in the context of early detection of potential perpetrators of serious crimes. The development of biometrics of the flow of people was of key importance in this respect.

The institutional and legal analysis confirmed the hypotheses related to the usefulness of the smart borders package in terms of improving security in three main areas: combating organized crime; the fight against illegal migration and the detection of illegally staying in the EU mainly through the use of biometric data. The new large-scale systems, such as the Entry and Exit System and the European Travel Information and Authorization System, will not only improve the administration of external borders, but above all will increase security standards both for EU Member State nationals and for foreigners traveling from third countries who they can become victims in the event that the persons representing the threat are not identified in advance by officers. Modern control systems based on automatic procedures of identity verification with the use of biometric data will increase the detection of threats and thus facilitate their fight.

The intensification of mobility on a global scale requires adequate instruments for the administration of migration flows. The Schengen area as an 'area without internal borders' requires increasing the information potential and optimization of the policy in the field of collecting, processing and using data, including biometric data. In particular, it is essential to fill the information gaps for all third-country nationals. The second key premise is to strengthen the interoperability with existing large-scale systems and to exploit their combined potential. It is also important to improve the exchange of information between Member States and between Member States and supranational bodies such as Europol to support their action in the fight against transnational crime. The new large-scale systems are to increase information resources by using two mechanisms: the provision of biometric data to establish the identity of the traveler (under the EES) and an initial risk analysis based on the verification of the travel authorization application (under ETIAS), and thus affect the level of security. It is therefore legitimate to assess the new systems as the missing link in the EU border management system.

References

Juncker, J.C., 2016. State of the Union Address 2016: *Towards a better Europe - a Europe that protects, empowers and defends,* SPEECH/16/3043.

Kirpsza, A., 2013. *Biometryczna identyfikacja tożsamości ludzkiej w świetle standardów praw człowieka: przykład paszportu biometrycznego* [in:] J. Jaskiernia (ed.), *Wpływ standardów międzynarodowych na* *rozwój demokracji i ochronę praw człowieka*, Wydawnictwo Sejmowe, Warszawa, pp.495-511.

Kosińska, A., 2017. *ETIAS czyli szczelne granice Unii*, https://ec.europa.eu/poland/news/170201_etias_pl, 12.11.21.

Szachoń-Pszenny, A., 2018. G*ranice strefy Schengen a granice Unii Europejskiej – uwarunkowania normatywne*, Pogranicze. PolishBorderlandsStudies, 6/1, pp. 51-75.

Wilczyński W.J., 2015, *Zmierzch Europy – demograficzne konsekwencje przemian cywilizacyjnych*, [w:] T.Z. Leszczyński (red.), *Bezpieczeństwo Europy. Uwarunkowania społeczne*, Polskie Towarzystwo Geopolityczne, Kraków, pp. 15-36.

Zawadzka, S., 2019. *System wjazdu i wyjazdu (EES) i Europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS). Rola i znaczenie nowoczesnych systemów w zakresie działań prewencyjnych i wzmacniania bezpieczeństwa UE*, Bezpieczeństwo. Teoria i Praktyka, 4/2019, pp. 103-118.

EU documents

*A comprehensive vision for an integrated European border management system for the 21st Century,*2008, EC Press release, IP/08/215.

Commission Implementing Decision (EU) 2018/1548 of 15 October 2018 laying down measures for the establishment of the list of persons identified as overstayers in the Entry-Exit System (EES) and the procedure to make that list available to Member States.

*EU 'Smart Borders': Commission wants easier access and enhanced security,*2011, EC Press release,IP/11/1234.

Migration and asylum, 2019. European Parliamentary Research Service, http://www.europarl.europa.eu/thinktank/infographics/migration/public/index.html?page=migration, 15.09.21.

Migration and migrant population statistics, 2019,Eurostat. https://ec.europa.eu/eurostat/statistics-explained/pdfscache/1275.pdf, 13.11.21.

Reforma wspólnego europejskiego systemu azylowego: Rada gotowa do negocjacji w sprawie Eurodac, 2016, EC Press release,09/12/2016.

*Regulation (EU) No 603/2013*of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac'.

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).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States.

Regulation (EU) 2017/458 of the European Parliament and of the Council of 15 March 2017 amending Regulation (EU) 2016/399 as regards the reinforcement of checks against relevant databases at external borders.

Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS).

Security Union: Commission delivers on interoperability of EU information systems, 2017. EC Press release, IP/17/1788.

Security Union: Commission proposes a European Travel Information and Authorisation System, 2016, IP/16/3674, European Commission (Press release).

'Smart borders': enhancing mobility and security, 2013.EC Press release, IP/13/162.

Smart Borders Pilot Project, Report on the technical conclusions of the Pilot, 2015, Eu-LISA Volume 1.

Stronger and Smarter Information Systems for Borders and Security 2016 Communication from the Commission to the European Parliament and the Council, COM(2016)205 final.

*System informacyjny Schengen: nowe przepisy Rady zwiększą bezpieczeństwo w UE,*2018, EC Press release,19/11/2018.

*Third country nationals found to be illegally present - annual data, 2019,*Eurostat,http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=migr_eipre&lang=en 15.11.21.

White Paper On Artificial Intelligence - A European approach to excellence and trust, Brussels, 19.2.2020 COM(2020) 65 final.

Wizowy system informacyjny: wstępne porozumienie prezydencji z PE co do głównych elementów, 2020, EC Press release, 08/12/2020.

Technologie biometryczne w zarządzaniu granicami Unii Europejskiej po roku 2015

Celem artykułu jest zbadanie ewolucji procesu biometryzacji przepływu osób w UE po kryzysie migracyjnym oraz wpływu nowych wielkoskalowych systemów informatycznych na poprawę bezpieczeństwa UE. W warunkach wzmożonej mobilności i wyzwań związanych z nielegalną migracją i zorganizowaną przestępczością, konieczna jest poprawa bezpieczeństwa migracyjnego w strefie Schengen. Odpowiedzią na te wyzwania jest implementacja realizowanego przez Unię pakietu „inteligentnych granic", który związany jest z zastosowaniem innowacyjnych technologii kontroli i przetwarzania informacji. W artykule została zaprezentowana analiza komparatystyczna dwóch systemów: Wjazdu i Wyjazdu (EES) oraz Europejskiego systemu informacji o podróży oraz zezwoleń na podróż (ETIAS). Na podstawie rozporządzeń ustanawiających nowe systemy, przeanalizowano najważniejsze kwestie z zakresu genezy, celów i zasad ich funkcjonowania. Głównym elementem procesu badawczego było określenie oraz ocena determinantów, które wskazują na przydatność systemów w aspekcie poprawy bezpieczeństwa w strefie Schengen, a także ocena procesu biometryzacji oraz jej wpływu na wczesne wykrywanie transgranicznych zagrożeń.

Słowa kluczowe: biometria, ETIAS, EES, inteligentne granice, kryzys migracyjny, strefa Schengen.