Zbornik Instituta za kriminološka
i sociološka istraživanja
2018 / Vol. XXXVII / 2 / 271-284
Originalni naučni rad
UDK: 351.756:57.087.1(497.11)

BIOMETRIC REGISTRATION OF MIGRANTS IN THE PROCESS OF MANAGING MIGRANT CRISIS IN EUROPE

Aleksandar R. Ivanović*
International University of Novi Pazar

Aleksandar B. Ivanović*
International University of Novi Pazar

In the paper authors dealing with the issue how system for biometrics identification are being used to manage the migrant crisis in Europe. Regarding to that, authors underlying problem of identification of migrants, due to the fact that many of migrants escaping from the war don't always have personal identification document with them, which means lot of problems from state authorities in the countries where them seeking asylum. Whit the intention to provide balance between need to quickly process, protect and place huge numbers of refugees, with one side, and maintaining a security, with other side, authors try to represent importance of implementing biometrics identifications system of migrants as well as cooperation and sharing of that data's between neighbour countries which are on the so called migrants routes to Europe.

KEYWORDS: migrants / security / biometrics / registration / identification

* E-mail: a.ivanovic@uninp.edu.rs.
* E-mail: ialeksandar@t-com.me.

1. INTRODUCTION

Under term migrant crisis in Europe (or also called European refugee crisis) is usually understood phenomenon of increased number of migrants, mostly refugees, which from the 2015 until now, arrived in Europe from Muslim-majority countries which are located in region of south and east of Europe, including the Greater Middle East and Africa. This huge wave of refugees is mainly caused by ongoing civil war in Syria which began in 2011. More than 1,8 million of migrants travelling across the Mediterranean Sea or overland through Southeast Europe came from 2015 until now in Europe as asylum seekers. From the early start of increasing migration to Europe from these areas, there were many concerns from European Union member states, as well as from the states which are located on the so called migrant route. This concern is mostly related to protecting of security due to fact that so huge number of refugees carries with it certain risks and security threats.

Terrorist attacks which has been occurred in territory of Europe, such as Paris attack in November 2015 with 130 killed persons, Brussels bombings in March 2016 with 32 killed persons, Atatürk Airport attack from June 2016 with 45 killed persons, Nice truck attack from July 2016 with 86 killed persons, Manchester Arena bombing from May 2017 with 22 killed persons, just increased concern regarding managing of migrant crisis and protecting of security at destination countries and its population. The call for tighter controls of frontiers and safer travel documents, as well as significant increases in inter-departmental and cross-border cooperation has been virtually unanimous among concerned states. Building capacities and increasing cooperation in these areas has become a priority in both domestic and foreign policy (Redapth, 2005:5).

Managing of the European refugee crisis faces with two main and mutually opposed challenges, first is to providing quick and safe passage and basic aid to asylum seekers, and second is protecting of security with other side. Namely, in the process of managing with refugee crisis key role is laid on process of refugee registration. Refugee registration is crucial to the monitoring of identification data, state of health and number of refugees. Registration ensures that records are kept of their status, and it helps protect refugees against forced return, arbitrary arrest and detention, forced employment, ect. and assists the UNHCR in re-uniting separated children with their families (Lodinová, 2016:91).

Regarding to everything above mentioned, according to our opinion implementation of biometric system of registration in this area is one of the most adequate solutions. We must also point out that there is some concern regarding the application of biometric systems for registration and identification in managing of refugee crisis and above all is related to maintaining informational and physical privacy and accepting religious objections. But taking in consideration two main challenges from which refugee crisis managing is faces down, we think that application of biometric system can have more positive than negative effects and we will try in the remaining part of the paper to represent that.

2. MEANING AND MODELS OF BIOMETRICS REGISTRATION AND IDENTIFICATION

Biometrics is a science that deals with the development of automated methods for identifying people based on measurable characteristics of the human body. Biometric-based identification: - biometric identification is based on the physical characteristics of a person. It belongs to the earliest identification methods. These methods in rudimentary forms were applied by Sumerians and Egyptians and during the Babylon era, the fingerprint on a clay tile was used during the conclusion of the contract. Later in the history, as a biometric identification method, tattoos were used in the case of people (flagging criminals in France) or animal stamping as proof of ownership. In the 19th century, the use of a fingerprint began as a method for identifying criminals, and this method has become widely accepted in the 20th century, and the police of all countries create databases based on this method. By developing computer techniques at the end of the 20th and the beginning of the 21st century, the possibilities of biometric identification are obtained both on the quality and the speed, as well as on the diversity of applied technologies. Also, here should be noted that biometrisc was named by the influential MIT Technology Review by „on of the `top ten emerging technologies that will change the world`" and soon after the September 11, 2001 terrorist attacks on New York and Washington the biometrics industry was further catapulted into the international spotlight by governmets eager to deploy biometric system in order to allay concerns about national security (Pugliese, 2010:1).

Biometric identification systems rely on measurement techniques and statistical analysis of human characteristics. Also it should be noted that the basic requirement for the application of biometric identification is the possibility that the physical and other facial features can be used in the process of automatic identification (Čimburović, Ivanović & Ivanović, 2011:86). Biometric identification methods can be divided into two groups:

- Static biometric identification - checks physical characteristics that are unique to the user. In this type of authentication, fingerprint, hand, face shape or eye length are usually checked.
- Dynamic biometric identification - Identification checks various behavioral characteristics that are characteristic of the user. In this type of authentication, the user's voice or manuscript is most often checked.

When it comes to biometric identification systems, it should be borne in mind that everyone has certain problems in identifying downloaded (scanned) data. For each method, manufacturers give a percentage of cases where misreading occurs. Depending on the applied biometric identification method, the number of false identifications is proportional.

The main biometric techniques being used for verification and identification processes in all sectors of society include fingerprinting, iris scanning, facial

imaging, hand geometry, voice recognition and signature verification (Redapth, 2005:6).

Fingerprinting involves the placing of the finger/s on an electronic scanner and starts digital recording and input into the system, with the help of the mouse, the positioning of the print on the computer screen is performed, and then the center of the fingerprint is determined and marked. Scener reading unique ridges (papillary lines) on the finger and digitalize its, and the identification features are automatically recognized and marked. Using a special program system doing control of the entered data, as well as the quality of the image of the print of the drawing of the papillary lines, is the change of the entered data, the change of the classification of individual prints of the papillary lines, the rotation of the print, the replacement of the prints taken by rolling with the control print. Human fingerprint is constructed of numerous ridges and vallez on the surface of finger whihc are unique to each and every human. Ridges are top skin layer portions of the finger and valleys are the lower portions. The particular individuality of a fingerprint could be determined by the several patterns of ridges and furrowa plus the minutiae points. Fingerprint authentification in actual and automated method of verifying a match among different human fingerprints (Saini & Rana, 2014:26)

Iris scanning involves the photographic scanning of the unique coloured patterns of the iris. Namely, the human eye contains an extremely large number of individual characteristics that make it very favourable for the process of identifying persons. Especially suitable for identification is iris. Iris, as a part of the optical eye system, enables the identification of persons based on a network of radial lines that is unique, time immutable to each person and independent of genetic origin (Radovanović & Pešić, 2009:438). Iris is an inner organ of a man seen from the outside. It is located between the cornea and the lens, its thickness ranges from 0.3 to 0.4 mm, while its diameter is about 11 mm. It consists of a muscle for the control of pupil, chromatofora, melanocytes and pigments (Radovanović & Pešić, 2009:438). Identification of persons based on iris is one of the safest biometric methods, since the appearance of iris cannot be altered throughout life, except in case of illness, surgery or injury when it's damaged and just an eye. Biometry of iris uses unique characteristics and features of human iris in order to verify the person's identity and is based on an analysis of the colour ring details which surrounding the eye. Iris has about 250 features that can be used for comparison. Iris readers use a normal video camera and do not require contact with the user. The person stays in front of the iris reader, so that the device can see the reflection of his eyes. After obtaining the image of the eye, the iris is distinguished, the pupil center is found, the edges of the iris are determined, they are connected to the center and filtered. The image is recognized radially to determine its contours. After determining the boundaries, characteristic points on the surface of the iris are found, and then its structure is transformed into a series of vectors in a complex plane and translates into a polar coordinate system. This allows that size of the iris, its position and orientation of the sphere, as well as the pupil size, does not affect the obtaining of the code. The obtained iris code is comparison with the codes in the database, and on that way is doing identification of person. Regarding the possibilities of misuse

during the application of biometric identification based on iris, the following should be pointed out follows: - The system cannot be deceived by wearing contact lenses, because there are algorithms for detecting false access; - A glass eye or a real eye removed from a person cannot be used to deceive, because there is no movement of their pupils (constant movement, contraction and spread). Of course, it should be underline that neither this method nor all other biometric methods of identification is not 100% reliable.

Facial imaging involves capturing images of the face, preferably from a certain angle and with controlled light and background. Namely, within this biometrics method of identification, in the controlled environment, frontal and profile photographs of human faces are taken, complete with a uniform background and identical poses among the participants. These face images are commonly called mug shots. Each mug shot can be manually or automatically cropped to extract a normalized sub-part called a canonical face image. In canonical face image, the size and position of the face are normalized approximately to the predefined values and the background region is minimized (Weng & Swets, 2006:66).

Hand geometry involves the placing of the hand on a scanner which measures the length, width and thickness of the hand and digits. Each human hand is unique. Finger length, width, thickness, curvatures and relative location of these features distinguish every human being from every other person. The hand geometry scanner uses a charge couple device (CCD) camera, infrared light emitting diodes (LEDs) with mirrors and reflectors to capture black and white images of the human hand silhouetted against a third-two thousand pixel field. The scanner record no surface details, ignoring fingerprints, lines, scars and colour. The process is much like placing a hand on beaded projector screen. The hand scanner read the hand shape by recording the silhouette of the hand. In combination with a side mirror and reflector, the optics produce two distinct images, one from the top and one from the side. This method is known as orthographic scanning (Zunkel, 2006: 89).

Voice recognition is method of identifying a person based on a voice by using technical means is based on the use of a special device for recording and analyzing voice. Namely, due to the development of electronics, devices were constructed which cut the recorded voice to the components according to: the strength, the frequency and the duration. Such devices are called various names such as spectrographs, sonographs, acoustic spectrographs, phonographs, voice analyzers, and the like. Since it is only used in recorded voice on a particular device, this method is also called phonoscopic identification (Greek: phon: phon, meaning voice, and skopein: study, watch;). The theoretical basis for the identification of persons based on voice is based on scientifically proven facts that the likelihood that two people have the same characteristics of voice and speech is practically equal to zero, that is, there are no two persons who have absolutely the same voice (Čimburović, Ivanović & Ivanović 2011:102). Voice is a sound wave that arises within a rather complex process. Namely, the process of occurrence of the voice starts in the trachea from which the air is pressed against the sound wires that produce their sound with sound. Each loud wire produces one ton. In addition to the vocal cords, in the

further creation of articulated voices, other organs are involved: oral cavity (which has the role of resonators), tongue, teeth, lips, palate, nose, breathing, etc. Thus, the voice of a man is the accompaniment of the basic tones and a series of accompanying harmonics (the harmonics are higher and lower frequencies of the basic tone), which is specific to every human being. The voice of each face has three basic characteristics: strength, height and colour. Thanks to the voice device, i.e. By putting a speech organ in a certain position, a person has the ability to change the height and strength of his voice. Since the strength and height of the variable category are the voices, they cannot be used as indifference characteristics as such, but the colour of the voice is taken as the indication characteristic. Namely, each voice besides the base frequency contains a whole series of accompanying harmonics, i.e. higher and lower sound frequencies that are close to basic. These more harmonics determine the colour of the voice, which is immutable and used as an identification feature. It was found that even the closing of the nose, the deliberate change in the voice - whispers, hoarseness, tooth extraction cannot lead to a change in the colour of the tone. However, it is possible that to some extent the voice of the voice is affected by the resonant properties of the room in which it is spoken or the various electronic voice effects that are transmitted over the phone, by mute certain tones, which may result in a change in the colour of the voice. However, in such cases, the tones only mute, and do not eliminate, which means that a sensitive ear, or even a more sensitive instrument, can register both damped harmonics (Maksimović, 2000:150).

Signature verification considers technique which is used to validate the identity of an individual on the base of analysis of its signature. The signature represents the name and surname of the author of the text, by which he confirms that he has signed the document, or accepts the content of the text of the document on which he has signed his signature. After many years of signing, a person begins to sign his name or surname, or both, in a shortened form, thus signing in the form of pure initials or combined (Simonović, 1965:101). One of the more important features of the signature is its individuality. The individuality of the signature is conditioned by the psychological and anatomical and physiological characteristics of the author, which practically influence the very mechanism of writing. In addition to the individuality and permanence of the signature, it represents its essential characteristic. Persistence means the preservation of the individual features of the signature for a certain period of time (Čimburović, Ivanović & Ivanović, 2011:402).

Identification features are divided into general and special identification features. General identification features are those features that characterize the signature and handwriting as a whole, regardless of the type of letter or digit (ie characters). General identification features include: handwriting and handwriting complexity. For manuscripts made are characteristic corrected lines and short cuts. Unlike the simple code of a complex signature, there is a wealth of shapes, elongated lines, and superfluous elements in letters; form of letter elements; size - letter gauge; the development of signature and the inclination of the signature. Special identification features are: the direction of performing

individual movements; position and shape of initial and final moves in letters and words; complexity of movement; forms of joining moves and letters; place of start and join letters and moves; the order of the movement; ratio of the length of individual moves in the letter and letters in the word, space utilization, space between words, the direction of letters, the form of letters, character letters, lettering, and other details of signature.

All the listed biometric identification techniques contain a basic model of work. The model consists of two separate parts. In the first part, there are taking biometric data is their compression and storage in a database. This ensures that when an entity arises and requests identification, there is information about it with which it will compare it. Two variants are possible: One variant is that when you take a biometric print, the system finds the appropriate record in the database and compares it with the captured print. The logic of this system is the question "Does the system know who owns the taken biometric data", and this is achieved by comparing the taked data and data in the database. The second variant is that when taking biometric data they are compared with the data on the smart card or some other data bearer that is locally loaded into the reader for the data to be compared. The logic of this variant is "Is the owner of the biometric impression really the one for whom it is issued", that is whether the identification is positive and the owner is recognized on the basis of the document.

The data acquisition process (1-3) and the recognition process (4-8)

1) The biometric scanning device accepts biometric data;
2) Processing of accepted data, their compression and preparation for entering into the database;
3) Entering data into a local database, a central database, or entering into a local portable device (smart card ...);
4) Scanning biometric data;
5) Processing of biometric data and preparation for comparison with previously taken data;
6) Comparison of taken data and data that were entered early. There are two ways of recognizing here:
    a) "Do I know who you are" take biometric data is compared with the data stored in the database on a computer - (variant one);
    b) "Are you the real one that you for which you are issued" the data are compared with the data the user has brought (smart card) - (variant two)
7) Results of the comparison are forwarded applications for further processing;
8) Final event entry with all supporting data.

Biometric identification is an area that is rapidly evolving. The technology that follows these methods is more and more reliable, but with their development, users are more and more afraid of unauthorized use or abuse. Particularly this concerns privacy issues. Problems that follow biometric identification systems are:

- Devices used for biometric identification and software solutions that follow are still expensive;
- Biometric identification systems are intrusive and dehumanized;
- They create discomfort in use;
- The use of biometrics permanently excludes persons with disabilities (damaged eyes, lack of finger, skin that is not readable by scanners);
- The durability of the device has not been verified in practice because technology is still relatively new;
- Unreliability of individual systems (percentage of lying);
- Training of users for working with such systems;
- Privacy issues. All listed systems have a large number of opponents who believe that this kind of data collection is problematic because it affects the privacy of users. The formation of data for biometric identification must be legally regulated;
- Formation of centralized databases. This is also a problem of privacy;
- The bases of biometric data are the ideal target for "identity thieves". Once stolen biometrics permanently excludes a business user;
- Lack of standards. Each manufacturer of biometric identification devices developed self-contained solutions. This kind of independent development without interaction leads to the fact that a biometric print from one device will not give the same results on the other.

3. IMPLEMENTIG OF BIOMETRIC SYSTEM IN MENAGING MIGRANT CRISIS AND PROVIDIN SECURITY IN EUROPE

Use of biometric systems in the management of migration can facilitate the efficient control of the border, particularly once the biometric is deployed in the travel document. When this is the case, those managing entry points can be quickly assured that the person holding the document is the one to whom it was issued. Routine and automated checks against a watch list could still be required, as could a review of the usual security features present on most passports and visas to ensure that the entire document is not fraudulent. In the new biometric passports this assurance could also be gained by electronically checking the validity of the issuance information encoded with the biometric on the travel document's chip against a database of authorized "private keys", a kind of

electronic signature that guarantees the validity of the issuance systems (Redapth, 2005:8).

When it the area of the European continent is in the question, the European Union recognized the importance of biometric identification for border control, and therefore established EURODAC in 2003. From the establishes an EU asylum fingerprint database (EURODAC). When someone applies for asylum, no matter where they are in the EU, their fingerprints are transmitted to the EURODAC central system. Since it was established in 2003, EURODAC has proved to be a very important tool providing fingerprint comparison evidence to assist with determining the Member State responsible for examining an asylum application made in the EU. Its primary objective is to serve the implementation of Regulation (EU) No. 604/20133 ('the Dublin Regulation[1]') and together these two instruments make up what is commonly referred to as the 'Dublin system'. Parallel to these developments have been EU moves to establish a "coherent approach...on biometric identifiers or biometric data for documents for third-country nationals, EU passports and information systems".[2]

Participating states are required to 'promptly' fingerprint all persons over the age of 14 who fall into one of the following three categories: a) applicants for international protection (Art. 9); b) third country nationals or stateless persons crossing the external border irregularly (Art. 14); c) third country nationals or stateless persons found illegally staying in a Member State (Art. 17).

In addition to fingerprints, EURODAC stores information on asylum applicants' gender and country of origin. It does not record a person's name. It should be noted that the data on asylum applicants (category 1) is stored for ten years, while the data concerning people irregularly crossing the border (category 2) is stored for 18 months and then deleted. The data on people in category 3 is not stored but run through the system for the purposes of comparison. In contrast to the first two categories, registering fingerprints of migrants from the third category is not mandatory. EURODAC was originally intended to prevent multiple asylum applications and unauthorised entry. Under the new EURODAC Regulation, however, access will no longer be restricted to immigration authorities, but will include police and public prosecutors, such as Europol. Namely, the Regulation establishes common procedures and standards but does not deal with enforcement. Among other modifications, the recast EURODAC Regulation No 603/2013 now allows national police forces and Europol to access EURODAC data for the purposes of preventing, detecting and investigating serious crimes and terrorism. However, the special agreements on the basis of which Denmark, as well as four Dublin Associated Countries (Norway, Iceland, Switzerland and Liechtenstein), participates in the Dublin and EURODAC Regulations currently only cover asylum-based purposes, although the Commission has proposed

[1] Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person, *OJ L 180, 29.6.2013, p. 31–59.*
[2] Presidency Conclusions, European Council of Thessaloniki, 19-20 June 2003, Bulletin EU, 6-2003.

opening negotiations with the countries concerned to also allow law enforcement access to their data.

The lack of systematic fingerprinting in some countries can be related to the lack of capacity in view of large flows of migrants. Greek authorities suggest that more than a third of migrants arriving on Lesbos, Kos and other islands are not fingerprinted. German police also confirm they lack resources to fingerprint all arriving migrants. Arrival countries' inability or unwillingness to meet the legal requirement of fingerprinting has led to a situation where asylum-seekers who move on within the Schengen area to reach other countries may not be identified. An additional aspect is the high number of applicants refusing to have their fingerprints taken, or intentionally damaging their fingerprints to avoid identification, as evidenced by the 2014 Annual Report on EURODAC. The reason could be either fear and mistrust of authorities, or a wish only to be first registered in a country with higher recognition rates or in which they have family and community ties. Such secondary movements undermine the proper functioning of the Common European Asylum System (CEAS), but it can be considered that both Member States and the migrants have incentives to evade the procedures. According to Frontex's annual risk analysis for 2016, around 1 million people travelled through the EU last year without proper travel documents. In a recent briefing on legislative reforms to EURODAC, the European Parliament described the associated problems with this situation as leading to "fears of threats to internal security, as the identity and motivation of migrants remained undetermined."

At the height of the refugee crisis in 2015, Greek authorities estimated that more than a third of the people arriving on the Greek islands were not fingerprinted. Similarly, German authorities back in 2015 could not keep up with the numbers. According to the European Commission, over the last few years this has led to a situation where "thousands of migrants have remained invisible in Europe, including thousands of unaccompanied minors, a situation that facilitates unauthorized secondary and subsequent movements and irregular stay within the EU."

Due to the large number of arrivals since the start of the migration and refugee crisis in 2015, some Member States became overwhelmed with fingerprinting all those arriving irregularly to the EU at the external borders, and who further transited through the EU *en route* to their preferred destination. As a consequence, thousands of migrants have remained invisible in Europe, including thousands of unaccompanied minors, a situation that facilitates unauthorised secondary and subsequent movements and irregular stay within the EU. As part of the first reform package of May 2016, the Commission presented a proposal to reinforce EURODAC to reflect the changes in the Dublin Regulation proposal and to make sure that it continues to provide the fingerprint comparison evidence it needs to function. In addition, the Commission also considered in its proposal the use of other biometric identifiers to be used for EURODAC, such as facial recognition and the collection of digital photos to counter the challenges faced by some Member States to take fingerprints for the purposes of EURODAC. The proposal also extends its scope for the purposes of

identifying irregularly staying third-country nationals and those who have crossed the EU external borders irregularly and contribute in an effective manner to the return procedure. Furthermore, the proposal:

- Introduces the obligation to take fingerprints and an additional biometric identifier – a facial image – and it lowers the age of taking fingerprints to 6 years old;
- Allows to store and compare all three categories of data and to retain fingerprint data for illegally staying third-country nationals or third – country nationals who have crossed an external border irregularly and who do not claim asylum for 5 years.

Discussions on the individual proposals are currently ongoing and follow a comprehensive approach on both reform packages.

According to the Dublin Regulation, the first country that an asylum seeker entered is ultimately responsible for an individual's asylum application. When an asylum seeker enters this first country, their fingerprints are taken and even though they might have entered another country later, the fingerprints remain in the EU wide EURODAC system that can tell authorities what the first country of entry was (Dockery, 2017). The system is hosted by the European Commission in Brussels. The fingerprints can also tell whether an asylum seeker illegally transited through another EU member state. If an asylum seeker winds up in another EU country than that of where they originally had their finger prints taken, they may be sent back to their original country of entry. Because of this strict rules the Dublin rules have long been criticised by migration advocates and governments alike. Between 2014 and 2016, Italy stopped fingerprinting every new arrival, and for a period of time, Germany and Sweden effectively suspended Dublin procedures for people escaping the Syrian war. There is broad consensus that the protocol does not equitably distribute the responsibility of processing asylum requests among the EU member states and that it has failed to prevent people from moving to their preferred destinations after landing in Europe. What it does do is push people towards becoming undocumented and increases the psychological stress of their long and arduous journeys. It also extends the length of time it takes for refugees to receive protection, and only then in a country where they didn't want to stay (Reidy, 2017). In November 2017, the European Parliament endorsed a proposal to overhaul the Dublin Regulation. At the foundation of the reform is a more equitable distribution of responsibility for asylum seekers among EU member states. Importantly, it would do away with the requirement for people to apply for asylum in the country where they first arrive and allow them to choose between four member states as their destination to live, unless they could prove a strong family connection in another country where they would want to go (Reidy, 2017).

Also it should be noted that according to EU rules, only the fingerprints of migrants who apply for asylum are shared among the member countries, which basically means that privacy concerns don't allow the use of the vast majority of migrants' fingerprints taken. This mean that for the Member States, which are

on the migrants route, it is not legally allowed to save and share with other European states more than 90% of the fingerprint data it takes of migrants fleeing war and poverty, a potential security problem at a major migrant hub. Namely, It is only required to upload onto EURODAC, the data of those who actually apply for asylum in the country. When are the Member States which are located on the migrants route such Slovenia, Hungary or Austria are in the question, this usually means less than 10% of total number of migrants which crossing its borders.

This mean that such countries of EU takes digital fingerprints of everyone entering the country, checks whether they have a criminal record, but does not save the data if they want to move in other countries of EU such Germany or France, which most of migrants in practice doing. Also problem with implementation of system for biometric registration and identification of migrants is various practice among Member States. For example, Croatia and Finland, save fingerprints of all migrants who arrive there, while Germany only lets in migrants who state they want to apply for asylum there. When it comes to non-EU Member States on the migrant route, such as the Republic of Serbia and Bosnia and Herzegovina, there is also a problem that each country carries out the biometric registration of migrants for itself, there is no common database of such biometric data's and what there is a poor level of exchange of such data's. All of this makes it difficult conditions to maintain under control the migrant crisis, their movement, the appearance of unregistered (formally invisible) migrants on the ground of Europe, more space for smuggling and trafficking in persons, and generally more difficult management of the migrant crisis.

CONCLUSION

Based on all of the above, we can conclude that the biometric registration of migrants is very important from the aspect of successful management of the migrant crisis. Of course, we also must have on mind fact that the issue of biometric registration of migrants is something that greatly affects the human rights of asylum seekers. And that there is also the danger of assimmilation of them with persons dealing with crimes and posing a threat to national security. Regarding to that it is reasonable to put in the question the necessity of application of biometric registration systems to this category of persons. However, on the other hand, if the objective of protecting security is not only national (European states), but also social and individual (which also include security of asylum seekers themselves), we believe that there is a need for the implementation of these systems. In support of this claim, speeks also the experiences of countries on a migrant route which say that, until a database has not been established, it has happened that, for example, a migrant enters a some city and presents himself as being from Pakistan when he arrives the another city is registered as a person from Afghanistan, and when it reaches the third city or is caught by inspectors for foreigners, it would happen that it was determined that same person registered different several times in the same country. This

creates space for abuse and numerous criminal behavior, and can be problem for providing security.

The biometric registration of migrants in all the countries through which it passes, the cooperation of criminal police in the fight against human trafficking and the exchange of operational data in the region is a field of utmost importance for all countries on the migrant route. Namely, the concealment of the actual situation and insufficient data exchange led to the emergence of thousands of migrants in one of the countries of the European Union in 2015, without any warning and information on their actual movement. This is something that must be prevented if it wants to successfully manage the migrant crisis.

That further means that every country on a migrant route must create its own biometric database of migrants that would be compatible with the bases in the region, as well as with those in the EU. In this way, conditions will be created to check whether one of these persons previously stayed in Europe and whether he had already applied for asylum and under what name. Also, the issue of relations and cooperation between the countries of the Western Balkans and FRONTEX is very important from the aspect of successful managing with migrant crisis and providing security.

Therefore, the successful management of the migrant crisis requires the establishment of a quality system of taking biometric data, a system that will be a unique system, and not each country entering the process individually and the system that will be consistent, not selective.

REFERENCES

(1) Čimburović, Lj., Ivanović, B. A., Ivanović, R. A. (2011) *Kriminalistička tehnika*, Beograd: Univerzitet u Novom Pazaru.
(2) Dockery, W., (2017) *Fingerprinting: How are asylum seekers registered in the EU?* http://www.infomigrants.net/en/post/3824/fingerprinting-how-are-asylum-seekers-registered-in-the-eu, available at 23.06.2018.
(3) Lodinová, A., (2016) Application of biometrics as a means of refugee registration: focusing on UNHCR's strategy, *Development, Environment and Foresight*, (2) 2, pp. 91-100.
(4) Maksimović, R., (2000) *Kriminalistička tehnika*, Beograd: Policijska akademija.
(5) Pugliese, J., (2010) *Biometrics: bodies, technologies, biopolitics*, New York and London: Routledge.
(6) Radovanović, M., Pešić, O., (2009) Biometrijska metoda identifikacije osoba prepoznavanjem irisa (dužice), *Zbornik radova: Pravo i forenzika u kriminalistici, Kriminalističko-policijska akademija Beograd.*
(7) Redpath, J., (2005) *Biometrics and internetional migration*, Genéve: International Organization for Migration.
(8) Reidy, E., (2017) *How a fingerprint can change an asylum seeker's life*, https://www.irinnews.org/special-report/2017/11/21/how-fingerprint-can-change-asylum-seeker-s-life, available at 21.08.2018.

(9) Saini, R., Rana, N., (2014) Comparison of barious biometric methods, *International Journal of Advances in Science and Tehnology (IJAST)* (2) 1, pp. 24-30.
(10) Simonović, Lj. (1956) *Veštačenje dokumenata*, Beograd: Mala stručna biblioteka.
(11) Weng J. J., Swets L. D., (2006) Face recognition, Biometrics, In: Jain A., Bolle R., Pankanti S., (ed.): *Personal Identification in Networked Society*, New York: Springer, pp. 65-86.
(12) Zunkel L. R., (2006) Hand geometry based verification, Biometrics: In: Jain A., Bolle R., Pankanti S., (ed.): *Personal Identification in Networked Society*, New York: Springer, pp. 87-102.

BIOMETRIJSKA REGISTRACIJA MIGRANATA U POSTUPKU UPRAVLJANJA MIGRANTSKOM KRIZOM U EVROPI

Autori se u radu bave pitanjem primene biometrijskih sistema identifikacije radi upravljanja migrantskom krizom u Evropi. U vezi sa time, autori podvlače problem identifikacije migranata zbog činjenice da mnogi migranti koji beže od rata nemaju uvek lične identifikacione dokumente, što prouzrokuje mnoge probleme za državne vlasti u zemljama u kojima oni zahtevaju azil. Sa namerom da se nađe ravnoteža između potrebe za brzim procesovanje, zaštitom i smeštanjem velikog broja migranata sa jedne strane, i očuvanja bezbednosti sa druge strane, autori pokušavaju da ukažu na značaj implementacije biometrijskih sistema za identifikaciju migranata, kao i na značaj saradnje i razmene podataka među državama susedima koje se nalaze na takozvanim migrantskim rutama ka Evropi.

KLJUČNE REČI: migranti / bezbednost / biometrija / registracija / identifikacija