JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online
2022 Volume 12
http://doi.org/10.47459/jssi.2022.12.4

MANAGING THE NEW WAVE OF MIGRATION WITH BIOMETRIC IDENTIFICATION

Péter Ujhegyi[1], Tibor Kovács[2]

[1,2] Óbuda *University, Doctoral School for Safety and Security Sciences, H-1081 Budapest, Népszínház utca 8., Hungary*

E-mail: [1]ujhegyi.peter@phd.uni-obuda.hu (Corresponding author)

Received 15 January 2022; accepted 5 March 2022; published 30 March 2022

Abstract. Due to the geopolitical situation, the scarcity of raw materials, the foreign policy actions of the major powers, the excessive use of resources worldwide and the struggle for them, as well as the inequalities caused by the demographic explosion of developing countries, europe and thus Hungary from the wider Middle East region have been under considerable migratory pressure for a long time, and this has increased further in 2021 on the basis of statistical data. (Frontex). Europe is trying to provide more answers to the problem. It is trying to keep refugees as far away as possible by developing and improving living conditions in the countries where migration flows originate, as well as by establishing migration zones beyond the EU's borders and financing them, because these problems need to start to be addressed and solved at local level. Despite all this, refugees are constantly reaching Europe, and unfortunately among them are not only those who fear for their lives and lose everything, fleeing war, but also economic migrants who join the wave of migration and are probably members of organisations that pose a threat to European values and public security. (Kotzur, Moya, Sözen, Romano 2020). By building physical border closures, several EU countries have closed certain migration routes, but this has not eliminated the problem, only the routes have been reorthled. The registration and clear identification of immigrants in the attempt to cross the border and their identification within the EU pose a number of unresolved problems for the authorities. (Beňuška, T., Nečas, 2021). We are reviewing and comparing the methods of identification used in border policing with modern biometric identification methods in order to draw attention to the fact that technology has long been ready to be used to protect our security in the service of European values and security. But at the same time, a significant deterrent is the difficult transition from entrenched solutions to the fear of misuse of biometric data. In order to achieve this, it is necessary to consider trade-offs in use and technology and to think more effectively together at EU level as a common solution on the regulatory side. (EU Regulation 399/2016).

Keywords: Migration Routes; Immigration; Border Closure; Migration Statistics; Identification For Law Enforcement Purposes; Entry; Biometric Identification Solutions; European Union; Border Protection

Reference to this paper should be made as follows: Ujhegyi, P., Kovács, T. 2022. Managing the new wave of migration with biometric identification. *Journal of Security and Sustainability Issues*, 12, 39-49. http://doi.org/10.47459/jssi.2022.12.4

JEL Classifications: D74

1. Introduction

1.1. Migration Routes

"Hungary continues to be included as a transit country along the international illegal migration route, but in the longer term it cannot be excluded that it will become a destination country for those who have been exposed to illegal migration. Based on geographical location and transport infrastructure characteristics, three inward-looking illegal migration channels affect Hungary's external borders. The most significant of these is the Balkan route, which reaches Hungary through Turkey, Greece, serbia and continues to Western Europe. The other route also reaches Hungary via Bulgaria and Romania via Turkey, while the third route reaches Hungary from Russia, Ukraine, the Ukrainian-Hungarian border basin, and continues towards Austria, Slovakia and Germany on the other side. Hungary security is also directly affected by the situation in Greece, as illegal border crossers on the Greek-Turkish border reach the Hungarian external border through secondary migration." (Besenyő, Miletics, Orbán 2019).

Based on the organizational structure, the length of the border sections and the main directions of illegal immigration in the country, the executing staff of local bodies at the external borders is present in the largest number on the Hungarian-Romanian (447 km) and Hungarian-Serbian (174.4 km) border sections, then in Hungarian-Ukrainian (136.7 km) and finally in the Hungarian-Croatian (344.8 km) border section. The use of live force is greatly influenced by the availability of border security infrastructure and reconnaissance capabilities with different technical content in each border location. Among the external border sections, the Hungarian-Serbian relationship is clearly under constant pressure, and thanks to the forces and tools focused on it, it is here that the greatest opportunity is possible to detect and prevent illegal attempts to enter the country either independently or in cooperation with Serbian border police. Based on the data of recent years, it can be concluded that persons crossing the state border illegally try to circumvent the border security system in a more organized way, using new methods, and a larger number are caught further away from the state border, which is made possible by the cooperation between the border police patrol service operated in several interdependent lines and the authorities involved in integrated border management. Further strengthening this system, which also covers areas further from the state border, is of paramount importance for maintaining the security of the external borders. To this end, the National Programme supports the development of cooperation between public authorities and joint risk analysis. (National Program for Border Management and Visa Facility).

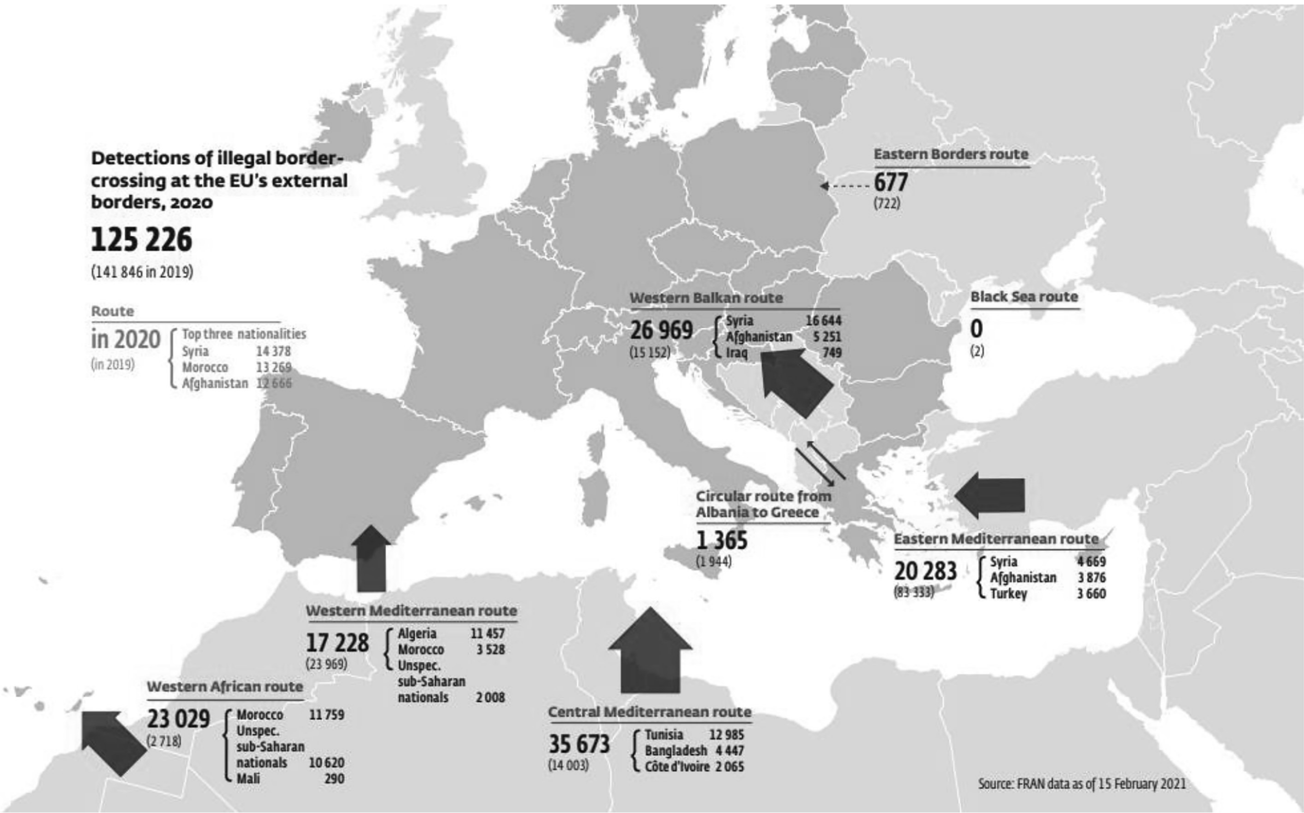
2. Border Closure

An important advantage of technical border closures is that they put the border crossing into a controlled direction, where identity verification can be enforced and and gives border police the means to prevent the smuggling of the means necessary to carry out the attacks (Besenyő 2017).

In domestic politics, government-side and opposition communication, although with opposing opinions, the construction of the border fence has been given a prominent role. "The Hungarian government finally decided on 15 June 2015 to build the southern border fence. The construction was based on Government Decision No. 1401/2015 (VI. 17). In it, a temporary border barrier of 175 kilometers in length and a height of 4 meters was provided for." (Novák 2021).

The Western Balkans corridor is one of the busiest migration routes, according to Frontex data. In recent years, due to the continuous influx of migrants, several countries have decided to build border closures**,** despite the fact that opinions on how to deal with the problem remain divided within the EU and opinions on fences are conservative (Weinar, Bonjour, Zhyznomirska 2021).

Headquartered in Warsaw in 2004, Frontex, the European Border and Coast Guard Agency, is responsible for border control in the European Schengen area, in cooperation with border and coast guards of the Schengen area Member States. According to the Frontex Risk Analysis report in 2021, the EU's external borders were breached by 125,226 illegal border crossings in 2020, compared to 160,000 in October 2021, based on statistics for 10 months of the year. This is a significant increase, and as we look at foreign policy events, at the beginning of 2022 another situation will escalate in Ukraine, which is likely to lead to a new influx of refugees (Frontex).



Source: FRAN data as of 15 February 2021

Figure 1. Number of illegal EU border crossings in 2020

According to Eurostat, at the beginning of 2020, 23 million non-European citizens lived in the EU, which is 5.1% of the total EU population (Migration and migrant population statistics). See Figure 1.

3. Other problems and challenges of illegal border crossing:

In addition to illegal border crossings, border police face a number of other serious problems. Terrorism, man, drugs, cigarettes and arms smuggling are just a few examples. Migration poses a threat not only because of the political persecuted and refugees in Syria or Afghanistan, but because of the real enemies who are able to organize and arrive with this intention. These challenges affect not only richer European states, but also smaller, less important states, such as the Baltic states and Hungary. (Kriviņš, Teivāns-Treinovskis, Tumalavičius 2021).

The border police service branch of the police has a special task in ensuring the security of the region, going beyond domestic legislation and internal norms, in accordance with the directly applicable legal norms of the European Union. Using selective and differentiated control methodologies, the most necessary control elements should be applied to ensure the expected level of security. The level of risk of the citizenship classification adapted to the maintenance of security basically determines the number of elements of the audit and the level of control.

The travel document shall entitle you to cross the state border, inter alia, if the pointer is identical to the person to whom it was issued. The passport manager should therefore examine identity and make a decision on identity or discrepancy, regardless of the content of the verification, namely that a person with EU free movement rights or a third-country national should be checked. The identification shall be carried out on the basis of the travel document between the tasks to be carried out during the inspection and their order, after the passenger's nationality, visa-freeness and visa requirements have been stopped.

Identification is a thought activity in which a decision must be taken as to whether the person handing over the document for verification is the same as the person to whom the document was issued by the competent authority. The relationship between the person to be identified and the document handed over by him shall be established by the inspector. There is no direct link between the document and its holder, except for a document containing biometric data, where data is also verified, which could be verified by technical means in the event of suspicion. Therefore, identification is very often based on the intuition of the control person, which does not always guarantee the right decision (Balla 2019; Sharan et al. 2021).

It would therefore be a very important task and it seems increasingly justified to clearly identify and register all border crossers at all external borders, and I think there is a growing need to monitor and monitor the movement of persons requiring entry with reliable means between the borders of the Member States. Biometric identification methods could be used in combination to reduce the possibility of deliberate fraud and deception, while controlling several biometric parameters could reduce the need for special expertise of the person performing identification for law enforcement purposes and, in many cases, problems arising from environmental factors. The following biometric solutions are available.

4. Possibilities and metrics of biometric identification (Kovács, Ujhegyi 2021)

It is important to distinguish between identification and authentication. We are talking about type 1:n identification when we compare the currently measured biometric sample ("1") with all the samples stored in a database ("n") and if there is a match, the requester of eligibility is determined and, say, an entry is made. So we compared a sample with a set of data from a lot of people. A key part of this process is that the legal conditions for storing biometric templates and samples must also be met, as the biometric template is considered personal data and is subject to appropriate regulations in order to protect personal data.

Authentication ("1:1") involves a template ("1"), i.e. a biometric data is stored and compared to the pattern just taken down ("1"). In this method, we examine whether the person belonging to the given and stored sample is right there and at the moment of identification he or she provides the biometric sample. This authentication procedure is used by your mobile phone for biometric verification if you enter the device or bank or want to pay, but from the point of view of the process, this also includes the method of using the biometric data stored by your passport. So, the match between the freshly taken and previously stored samples is examined by the given methodology.

The authentication process is usually much faster, as you don't have to compare in hundreds, thousands, or even millions of database records, and protecting a database with a lot of sensitive data is not a big risk, because that's not how you store the data.

An important feature of the identification process and the biometric measurement solution used are the FAR and FRR values. The FALSE Acceptance Rate (FAR) value shows how many cases are identified as unauthorized users during enrollment. Less problematic than this indicator is the FALSE Rejection Rate (FRR), i.e. the rejection of eligible users.

In the case of identification solutions, the number of biometric features recorded by the technology used is also a characteristic aspect. The number of recorded data varies widely, we are talking about 15-35 points for a fingerprint, but a palm network-based solution can record up to 5 million reference points. The professional know-how of biometric solutions companies is how many of the data collected accepts in successful identification and how many have the limit where the system rejects the process. The pandemic situation in the 2020s and 2021s reinforces this, because a number of disturbing circumstances can affect the transmission of a successful sample. Before we get to this, let's look at the identification methods and what links biometric identification can be to critical infrastructures or object security, especially in the case of special objects, and how this changes in the pandemic situation.

5. Fingerprint, palm print biometric identification

The groove of the skin on the surface of the finger or palm, is formed by the so-called frills and spear lines. A quick identification solution, due to the early use of law enforcement, is one of the oldest biometric technologies, so it is quite accepted and widespread. In the process, approximately 15-50 external characteristics are measured, but usually not contactless technology, so the detector must be constantly disinfected. The pattern is easy to copy because it may inadvertently remain on the suitable surface (e.g. glass cup). It is not applicable to 3-5% of humanity because they do not have fingerprints suitable for electronic sampling. A sample of two palms or even ten fingers is available, but work with chemicals or physical activity in certain areas of the construction industry can cause the leather folds of the palms or fingers to easily deteriorate, which makes such identification possible. Sometimes, in the case of a border crossing, the upper epithelials are damaged with strong acids "in order" to fail fingerprint identification, thus avoiding clear identification. Over the years, the pattern does not change and develops from 18 weeks of age. In the case of use in the health field, the use of medical rubber gloves may be a disqualifying reason.

6. Hand geometry-based biometric identification

It is a commonly used technology that takes into account the shape and physical dimensions and proportions of the hand. Newer technologies can now identify without positioning spikes. It is widely applicable in terms of population, there are no significant disqualification factors and the identification time is not significant (a few seconds). The process of identification is acceptable to users, there is no resentment towards the process and technology of identification and the need to cooperate with the device is not very high. It measures external parameters, identification is based on approximately 30. Weight gain, a hand changed due to joint disease can cause identification problems, sensitive to this technology, in the field of health, or due to pandemic protection, rubber gloves can cause a decrease in the number of identification parameters. (Gulyás, Kovács 2021).

7. Facial recognition-based biometric identification

It is one of the most well-known technologies and the most used solution in our daily lives. Due to the method of biometric identification used by tablets and notebooks to unlock phones, it has reached everyone and is a popular convenience solution. Today, almost most camera systems offer some kind of face-based identification solution. The acceptance of the technology is therefore high, authentication is based on external paramters, it does not require physical contact during the measurement, but the position of the camera and the person and many other external factors (e.g. lighting) significantly affect the success. You don't need the person's consent or cooperation to successfully identify you, which makes the solution suitable for multipurpose and hidden use. During identification, the comparison of samples may not necessarily be carried out with a registered database of users who have consented to the purpose of data processing. Identification can work on the basis of an image taken from or downloaded from a movie, and with AI-assisted solutions, it is not necessary to look at the camera and identification can be successful based on very few parameters (Heilweil 2020).

The technology measures the characteristic points of the face, their distance and proportion. The search for moles and other characteristic identifiers (scars, tattoos) helps the process, based on wrinkles and skin pole examination it is even possible to determine the age of the person. This includes some of the definition of persons based on the ear shape, and among the new solutions there are technologies that can identify by head shape and ear shape as an additional solution, but also from a profile. The accuracy of the technology is low, its vulnerability is very high, it is easily accessible to exploit the vulnerability of payment or identification services using masks based on high-quality high-resolution images. Typically, systems do not include hardware software solutions for live sample recognition. (Ngan, Grother, Hanaoka 2021).

8. Iris-based biometric identification

We process the pattern of the iris of the eye. The iris image does not change from the 8th month of the fetus until death, it is widely used and the chances of matching the samples of two different individuals are 1070. Internal biometric feature, technology contactless. In the case of an active solution, you need to look closely into the sensor, therefore there is a high need for cooperation in the implementation of the identification process, as well as the acceptance of the method mainly due to the risk of possible infection. It takes about 400 characteristics into account in identification, one of the most accurate techniques, but these solutions are sensitive to various eye diseases. (Tajti 2021).

9. Retinal biometric identification

By scanning the vascular network running on the back wall of the eye, the structure of the retinal blood vessel is identified by the camera, which uses infrared light-based lighting. A very high-precision solution and the uniqueness of the retina ensure that it can be used widely. Acceptance of the procedure is low, because those who do not know the technology are averse to "illuminating" the eyes. Retinal identification provides one of the best biometric methods with low FRR and nearly zero percent FAR values. For identification, the need for the positioning of the head is also not favourable, the solution is disadvantageous in case of mass rapid read-down demand, and it is not beneficial from a hygienic point of view either.

10. Vascular network-based biometric identification

We measure internal data when identifying finger or palm vascular network. When illuminated by infrared light, the sensor detects the flow of carbon dioxide-enriched blood in the blood vessels, so it can only measure a living sample. The measured reference points are in the order of millions, a high-precision and fast solution. The latest technologies do not require any special cooperation, the finger or the hand is pulled over a surface and is identified within a few seconds without touching. It does not affect the identification of contaminated skin or superficial injuries. It can be applied to the widest range of the population, there are few grounds for exclusion. The latest technologies do not require any special cooperation, the finger or the hand is pulled over a surface and is identified within a few seconds without touching. It does not affect the identification of contaminated skin or superficial injuries. It can be applied to the widest range of the population, there are few grounds for exclusion.

11. Voice-based biometric identification

When identifying sound, the frequency of the sound is first identified, and then in the later phase other properties of the sound: tone, tone, rhythm. There is a significant difference between two methods, in the case of so-called "speech recognition", speech is recognized by the system, while in the "speaker recognition" method the sound itself and the unique characteristics of its emitter are recognized. The measured sound depends not only on the medium, distance and method of recording, but also on the biological characteristics of the individual's vocal organs, as well as on his personality, sociocultural environment, intelligence and many other factors. Each pattern is unique. In general, the consent of the individual is not required for sampling or identification. It is an internal identifier, an accepted technology. Its weak point is that the sound changes due to illnesses, or even emotional or physical exertion, which affects the pattern giving and the success of identification. Under ideal conditions, the technology is highly accurate, but there is no live sample identification in general applications and ideal conditions are rare, so it is more of a secondary solution. (Fejes 2018).

12. Identification for law enforcement purposes

'Establishing a direct link between the person under control and the document he/she has provided for identification by means of the facial image/photograph, personal data and the recorded biometric identifier at the point of the check, built into the verification process and with an immediate response to identity or deviation. The purpose of identification is to determine whether the person showing the identity document is the same as the person to whom the document was issued.' (Balla 2019).

Passports issued in the European Union, including in Hungary, with a validity period of more than one year, are mandatory to include a facial image as a primary biometric identifier and a fingerprint on the chip as a secondary biometric identifier. If it is not possible to record fingerprints on a permanent or temporary basis at the time of issue, the period of validity of the passport may be up to one year. Under current rules, biometric fingerprint samples do not have to be stored from people under the age of 12. This constitutes a vulnerability point in the current system, because it is not possible to use another biometric solution or to verify the identity of the person by clearly identifying it, i.e. establishing a direct link between the document and the person who transmitted it for verification. Consider the security risks of identifying a 10-month-old baby on the basis of a travel document issued at the age of five days, and the determination of his relationship with the parents is also doubtful because the travel document does not support it. (Balla 2013).

Fingerprints in passports are already a personal data with extended protection, which cannot be stored or checked from the electronic data store due to the legal environment – the processing of personal data. This means that the authority is also subject to strict rules when checking, because a certificate is required from the passport to query biometric data. The Hungarian police officer can retrieve the data from the Hungarian document and perform the biometric identification, because he has the necessary certificate, but for the sake of the example, only if he has the necessary certificate from the Austrian passport. Beyond the border, e.g. the Austrian police officer must have a similar background data and certificate in order to be able to use biometric data stored electronically from the Hungarian document for the safe execution of personal identification.

Biometrics are a mandatory element of the document for EU citizens, more specifically for persons with EU free movement rights, but since there are green borders, border crossings at member states' internal borders can only be discussed in principle. At the Schengen external border, the possibility of identification on the basis of biometric data should also be provided in this category of passengers, for which those certificates are required. For third-country nationals subject to a visa obligation, there is no mandatory biometric data in the passport (although it may be included), but the Visa Information System (VIS) and the exchange of data on short-stay visas between Member States (VIS Regulation, HL L 218 2008.8.13.) are recorded in the fingerprint data, which must be applied to identification at each entry into the Schengen area. Visa-free third-country nationals are currently "excluded" from the possibility of identity based on their biometric data (Balla 2017). See Table 1.

Table 1. Indentification

Category	**Whether the document must contain biometrics**	**Should a person be biometrically identified upon entering Hungary?**	**Can a citizen be certified by the authorities by means of a roadside certificate in the EU Member States or can the authority verify the citizen by biometric identification?**
Member States of the European Union	yes	no	Citizens of their own country, yes, and other Member States, access depending on insurance.
Visa-free 3rd country	no (but may be a consideration for the acceptance of travel documents)	no	access depending on insurance
Visa-bound 3rd country	visa (may be a consideration for the acceptance of travel documents)	yes	yes

Fingerprint-based identification is the most common identification solution due to the entrenchments and customs of law enforcement, but it is also one of the obstacles to the development of methods. New solutions could be explored from the lens of the tool and method-specific requirements, but since it is used by 27 Member States on a mandatory basis, it would be difficult to replace it with other biometric data.

"There are at least 10-15 possible variants of identification based on biometric data that can be used to establish a doubtful identity. They require different identification procedures, technical infrastructure and expertise. As a result, there are currently three applied procedures in law enforcement identification that also essentially meet the professional requirements for biometric identification. These procedures are also preferred and supported by ICAO and the European Border and Coast Guard Agency (Frontex) and will apply in the future under the legal or applicable standards applicable in the EU when identifying persons. (EU Regulation 2019/1986).

The ICAO also examined a number of biometric identification technologies, including facial recognition, iris, fingerprinting, hand geometry, sound and signature identification procedures for document testing in its 2001 assessment, including facial recognition, iris and fingerprint identification (ICAO 2007). Frontex also supports these three identification procedures in the context of biometric identifiers, but in the case of the Automated Border Control System (ABC system) and the Registered Passenger Programme (RTP system), it says that if the order does not rely on the use of a travel document containing biometric elements, other biometric identifiers may be used as personal identification on the basis of separate sampling." (Balla 2019).

There are several central databases containing biometric data in the EU, one of which is EURODAC, which facilitates the processing of fingerprinting systems and asylum applications. The legal basis for this system is the Dublin Convention, also known as the Dublin Regulation, which was adopted in 2003 by 12 signatory states (Belgium, Denmark, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain and the United Kingdom) Under the current border protection rules, two biometric data are stored in the passport, which is the photo and fingerprint, these are recorded in the EU passport in order to establish clearly the relationship between the document and its holder and this also applies to illegal border crossers. There is also a more than 100-year tradition of fingerprint identification in criminal identification. (EU regulation 2017/2226).

The current EURODAC Regulation only allows comparisons of fingerprint data. In 2015, the European Agenda on Migration proposed to supplement EURODAC with other biometric identifiers, thereby somewhat reducing the difficulties that Member States often face due to the refusal of damaged fingerprints or fingerprinting procedures. This proposal requires Member States to produce facial images of the person concerned for transmission to the central system and provides for a combination of fingerprints and facial images and for comparing facial images separately under certain specified conditions. Thanks to the integration of facial images into the central system, queries with facial recognition software will also be possible in the future. (eur-lex.europa.eu 2016).

By 2020, eu-LISA will conduct a study on the technical feasibility of supplementing the central system with additional facial image recognition software that provides reliable and accurate results after comparing facial image data. (eur-lex.europa.eu 2016).

In the United States, regulations are looser, and no biometric data is required. The question may arise, of course, whether, on the basis of the principle of necessity-proportionality, this violates Community law and the right to privacy declared by Community law. The combination of biometric databases, profiling, total control and automation in the field of observations should always be avoided. Solutions that are least restrictive of constitutional rights may be considered.

13. Vascular network-based solution instead of fingerprint

The identification solution currently in use is photo and fingerprinting. Both are based on external criteria in the identification process. Fingerprinting has a great advantage due to law enforcement, it is widespread, it remains on all surfaces, it can be removed from 10 fingers, its uniqueness is high, but the destruction of the skin folds on the fingertip is very easy, the falsibility of the sample is high. Refugees can take advantage of this, because if they are not granted asylum and deported during registration and identification in one Member State, they may even be prevented from being clearly identified by another Member State by destroying their fingerprints.

Based on a photo or digital portrait, a law enforcement professional also carries out identification during the verification of an ID card, the facial recognition technology has developed greatly. Analysis and image analysis software can help you identify, either by photograph or by creating an older state from a previous image. Identification can be done remotely without the knowledge of the subject. It is easy to influence or hinder the success of identification with makeup, hat, wig, sunglasses or face plasticity solutions.

During vascular network-based identification, it requires minimal cooperation from the subject, it is enough to pull the hand or finger over the surface of the sensor. The success of identification is not or is difficult to influence, the pattern is not affected by damage or contamination of the skin surface, no falsified hand or vascular structure can be used, the measurement can only be carried out on living tissue, the sensor measures the pattern of the vascular structure based on changes in blood flow. It measures an internal standard. It is not sensitive to skin color, each person has at least one hand, there are few disqualifying factors. The data used in the identification is permanent over the age of 12, the structure of the vascular network does not change until we die. New sampling is proposed every 1-2 years under the age of 12 or at the same time as the renewal period of the documents. The solution is not particularly susceptible to diseases, but using a sample of two hands minimizes this exclusion factor. It can be palms, it can be finger-based, or it can be taken on the forearm. The technology can be contactless, there is no need to deal with hygiene problems, but positioning requires practice when sampling. The rejection of the solution is small, because we do countless things in everyday life with our hands, so it does not cause any inconvenience to use for the identification process, even at the cost of physical contact. The identification solution has little exposure to light conditions, can be performed in the dark, in the field, and can be used in non-extreme temperature weather conditions. The identification accuracy is high compared to other biometric solutions and the speed is good, but these parameters are obviously also dependent on background systems. Perhaps the only negative factor is that the price of the solution among biometric solutions is considered to be moderately high.

Vascular network-based identification cannot be used as a remote identification solution as opposed to a facial recognition solution, but it does not allow hidden identification, it cannot be used without the consent of the subject. The print of the vascular network will not remain on a glass surface like a fingerprint or a DNA sample, so it will not replace the fingerprint used in law enforcement.

14. Summary. Conclusion

The great power games continue to sharpen the problems of the Middle East. Due to the effects of climate change caused by global warming, the growing shortage of food and drinking water in different regions and the promise of a stable democratic legal order and security, the EU will continue to be an attractive destination for migration. With the expansion of the Member States, the increase in bureaucratism and the rise of dissension due to a wide range of interests, the Union is becoming a slowed-down machine, difficult or unable to make a unified decision and unable to respond effectively to a variety of global problems. However, the culturally enriching effect of immigration is recognised as creating further tensions, with most European citizens not wanting such a colourful cultural environment within the EU and many immigrants abusing the flexible immigration policies of Western countries. On this issue, Hungary quite vocal, because according to the government-side narrative, we do not take in migrants and we want to preserve our national sovereignty. On the issue of fencing, the EU has been opposed to the construction of new fences since the dismantling of the Iron Curtain, and has refused to do so on the issue of closing borders and building new fences, but several countries have decided to do so in recent years as a result of the independent decisions of the Member States. As long as the EU catches up with itself on these global issues and reaches a decision, all support must be given to border protection agencies, both legally and technologically. The identification solutions currently in use do not provide adequate solutions to many new challenges, so it is time to consider expanding them with new methods. Nevertheless, such a complex issue as migration management and the usability of identification methods depend not only on technological issues, but also on policy decisions, the widespread and comprehensive application of solutions, and the complexity of solutions. (Kui 2020).

References

399/2016 EU regulation, https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016R0399&from=HU (downloaded: 2022.01.20)

A regulation by the EU Parliament and Council (EU) 2017/2225 (30th. November. 2017.) The regulation (EU) 2016/399 border registration system (EES) HL L 327, 9.12.2017, page 1–19.

A regulation by the EU Parliament and Council (EU) 2017/2226 (30th. November. 2017.) establishing an EES system for recording data on the entry and exit of third-country nationals crossing the external borders of the Member States and determining the conditions for access to EES for law enforcement purposes and implementing the Schengen Agreement, regulation No 767/2008/EK 1077/2011/EU and regulation No HL L 327, 2017.12.9., page 20–82.

A regulation made by the EU Parliament and Council (EU) 2018/1240 (12. September. 2018.) establishing the European Travel Information and Authorisation System (ETIAS) and amending Regulation (EU) No 1077/2011, Regulation (EU) No 515/2014, Regulation (EU) No 2016/399, Regulation (EU) No 2016/1624 and Regulation (EU) No 2017/2226 HL L 236, 2018.8.19., page 1–71.

A regulation made by the EU Parliament and Council (EU) 2019/1896 (13. November. 2019) on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624 (downloaded: 2022.02.16)

Balla József, 2017. A schengeni elvek szerinti határforgalom-ellenőrzés tartalmi elemei Magyarországon 2016-ban, Magyar Rendészet 2017/3. szám, 24

Balla József, A biometrikus adatokat tartalmazó úti és személyazonosító okmányok biztonságnövelő hatása a határ-, illetve közbiztonság alakulására, 82. page, https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/Balla_Jozsef_biometrikus_adatok-okmany.pdf (downloaded: 2021.02.14)

Balla József, A. 2019. biometrikus adatokat tartalmazó úti és személyazonosító okmányok biztonságnövelő hatása a határ-, illetve közbiztonság alakulására, 2019, 114. oldal https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/Balla_Jozsef_biometrikus_adatok-okmany.pdf (downloaded: 2021.01.28)

Balla József. 2019. A biometrikus adatokat tartalmazó úti és személyazonosító okmányok biztonságnövelő hatása a határ-, illetve közbiztonság alakulására, Dialóg Campus Kiadó, pp. 94-95. https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/Balla_Jozsef_biometrikus_adatok-okmany.pdf (downloaded: 2021.11.22)

Balla, József. Biometric data in documents, https://www.academia.edu/33526570/Biometric_data_in_documents_Biztonsagpolitika_2013 7. page, (downloaded: 2021.01.30)

Beňuška, T., Nečas, P. 2021. On societal security of the state: applying a perspective of sustainability to immigration. Ent-repreneurship and Sustainability Issues, 9(2), 473-487. http://doi.org/10.9770/jesi.2021.9.2(31)

Besenyő János 2017.Fences and Border Protection: The Question of Establishing Technical Barriers in Europe. Academic and Applied Research in Military and Public Management Science, Vol 16, Issue 1, pp. 77-87. https://folyoirat.ludovika.hu/index.php/aarms/article/view/1617 , (downloaded: 2022.02.10)

Besenyő János. 2019. Migrációs útvonalak, In: Besenyő János; Miletics Péter; Orbán Balázs: Európa és a Migráció, Zrínyi Kiadó, 2019, 31-64
Fejes Attila, Beszéd alapján történő személyazonosítás új kihívásai a kriminalisztikában, Magyar Rendészet, 2018/2. 117-126, http://real.mtak.hu/92529/1/web_MR_2018_02%20fejes.pdf (downloaded: 2021.02.12)

FRONTEX. https://frontex.europa.eu/assets/Publications/Risk_Analysis/Risk_Analysis/Risk_Analysis_2021.pdf 49p, (letöltés ideje: 2021.11.02)

Gulyás, Laura, Kovács, András. 2021. Biometric Authentication System based on Hand Geometry and Palmprint Features, In Proceedings of the International Conference on Image Processing and Vision Engineering (IMPROVE 2021), pages 58-65, ISBN: 978-989-758-511-1, https://www.scitepress.org/Papers/2021/104089/104089.pdf (downloaded: 2021.01.30)

Kotzur, Markus, Moya, David, Sözen, Ülkü Sezgi, Romano, Andrea. 2020. The External Dimension of EU Migration and Asylum Policies: Border Management, Human Rights and Development Policies in the Mediterranean Area, Nomos Verlag, pp. 39-43.

Kovács, T., Ujhegyi, P. 2021. Reduced-parameter biometric identification capabilities to protect critical infrastructures and special objects, Biztonságtudományi szemle, III. évf 1. különszám, 137-146 oldal.

Kriviņš, A., Teivāns-Treinovskis, J., Tumalavičius, V. 2021. Issues of state and national security: Religiously inspired terro-rism in the Baltic States: internal and external factors. Insights Into Regional Development, 3(1), 65-79. http://doi.org/10.9770/IRD.2021.3.1(4)

Kui László, A Magyar határőrizet technikai generációváltásai és lehetséges fejlesztési irányok, PhD degree thesis, 2020, https://www.uni-nke.hu/document/rtk-uni-nke-hu/A_magyar_hatarorizet_technikai_generaciovaltasai_es_lehetseges_fejlesztesi_iranyok.pdf (downloaded: 2022.02.10)

Migration and migrant population statistics, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Migration_and_migrant_population_statistics#Migrant_population:_23_million_non-EU_citizens_living_in_the_EU_on_1_January_2020 (downloaded: 2021.11.20)

Migratory situation in October: Persisting pressure on Eastern Border, https://frontex.europa.eu/media-centre/news/news-release/migratory-situation-in-october-persisting-pressure-on-eastern-border-flfAwy (downloaded: 2021.11.29)

National Programme for Border Management and Visa Instrument, http://belugyialapok.hu/alapok/sites/default/files/HAVE_NP_partners%C3%A9gi_egyeztet%C3%A9s.pdf (letöltés ideje: 2021.07.05)

Ngan, Mei, Grother, Patrick, Hanaoka, Kayee. Ongoing Face Recognition Vendor Test (FRVT) Part 6B: Face recognition accuracy with face masks using post-COVID-19 algorithms, National Institute of Standards and Technology Interagency, https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8331.pdf

Novák András, Műszaki zárak hatása és jelentősége a balkáni migrációs útvonalon, PhD értekezés, Óbudai Egyetem, 2021, 81. oldal
Proposal For a Regulation of the European Parliament and of the Council establishing a European System for Passenger Information and Authorisation (ETIAS) and amending Regulation (EU) No 515/2014, Regulation (EU) No 2016/399, Regulation (EU) 2016/794 and Regulation (EU) 2016/1624 Brussels, 16.11.2016., COM(2016) 731 final 2016/0357 (COD)

Rebecca Heilweil, The World's scariest facia recognition company, https://www.vox.com/recode/2020/2/11/21131991/clearview-ai-facial-recognition-database-law-enforcement?fbclid=IwAR0c4rkztQXDWxguNFeCa-iGHMhPKC2VVPBEiWqVA_Sey78rcA5ZJLfM-7LY (downloaded: 2022.02.01)

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, Brussel, 2016.5.4, COM(2016) 272 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016PC0272(01)&qid=1645100261828&from=EN 13. pege (downloaded: 2021.01.10)

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, Brussel, 2016.5.4, COM(2016) 272 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016PC0272(01)&qid=1645100261828&from=EN 99. page (downloaded: 2021.01.12)

Sharan, Y., Gordon, T.J., Florescu, E. 2021. Deep Fakes. In: Tripping Points on the Roads to Outwit Terror. Advanced Sciences and Technologies for Security Applications. Springer, Cham. https://doi.org/10.1007/978-3-030-72571-6_12 (dowloaded: 2022.01.18)

Tajti Balázs, A biometrikus ujjnyomat azonosításának új lehetőségei, Hadmérnök, VII. Évfolyam 1. szám, http://hadmernok.hu/2012_1_tajti.pdf (downloaded: 2021.02.08)

Weinar, Agnieszka, Bonjour, Saskia, Zhyznomirska, Lyubov (eds): 2018. The Routledge Handbook of the Politics of Migration in Europe, Routledge, p.140

Péter UJHEGYI
ORCID ID: http://orcid.org/0000-0001-9143-6712

Tibor KOVÁCS
ORCID ID: https://orcid.org/0000-0001-7609-9287