

Criminological Significance of Biometrics Technology in the Context of Combating Cross-Border Crimes

Filippov Stanislav

PhD in Law, Associate Professor of the National Academy of the State Border Guard Service of Ukraine



Abstract. Border security system effectiveness is largely influenced by creation of the conditions under which the use of documents for committing cross-border crimes is impossible or provides for termination thereof. Implementation of biometric technologies in the sphere of documents production allows not only to increase the level of their protection, but also provides the tools necessary for identification of such a set of personal data, which eliminates any possible errors. In turn, this greatly enhances the opportunities for both crime prevention and termination of certain criminal acts.

Keywords: cross-border crime; criminology; biometric identification; biometric identity documents; International Civil Aviation Organization (ICAO); e-passport; ID-card; border control.

Problem statement

Timely and complete necessary information on persons crossing the state border ensures the functioning of the system for countering cross-border crime in the way that corresponds to the characteristics of optimality and efficiency. The undoubted factor that determines the effectiveness of the border security system is the presence of conditions under which the use of personal data and documents to commit cross-border crimes is either not possible at all, or creates opportunities for further suppression of crimes. The introduction of biometric technologies in the process of producing documents for traveling abroad provides an opportunity not only to raise the level of their protection, but also provides the possibility of identification using such a set of personal data, eliminates an error. It also enhances the possibilities of both preventing crime and stopping individual crimes.

Analysis of recent research and publications.

Anticriminal significance of biometric technology is a relatively new area of research for criminology. At the same time, in the related sciences, this topic has long been of interest to scientists. In particular, at the level of the thesis of L. Tallanchuk, a study of the criminalistic aspects of the problem was conducted [1]. International standards for the security of documents with biometric data are considered in the works of A. Vollevodza [2]. In the criminological policy in the field of cross-border relations, the strategy of reducing the possibility of committing a

crime is of particular importance. In this regard, criminology cultivates the idea that a crime is the result of the realization of the possibility underlying the theory of rational choice and standard activity, which was developed by the American criminologist M. Felson and developed by his followers (R. Lambert etc.). One of the conclusions of the theory is that the proliferation of technologies aimed at minimizing opportunities for the commission of crimes entails a decrease in the level of crime [3; 4]. The opportunity is considered as the cause of the crime.

Considering the above, **the purpose of the article** is to conceptualize the idea of the anti-criminal significance of the use of biometric technologies; it is to minimize the possibility of individual crimes and the corresponding impact of these technologies on the reduction of cross-border crime.

Presentation of the main research material.

1. Forged documents when crossing the state border are used in the commission of such criminal offenses as human trafficking or other illegal agreement regarding the transfer of a person; smuggling; production, storage, acquisition, transportation, shipment, import into Ukraine with the purpose of selling or selling counterfeit money, government securities or state lottery tickets, fraud; malpractice and the like. In art. 358 of the Criminal Code of Ukraine provides for the responsibility for forging documents, seals, stamps and forms, their sale, as well as the use of forged documents [1]. Earlier, we noted that among the conditions for the effectiveness of information support for countering cross-border crime in the coming years should be considered the following:

- within the framework of integrated border management – the trend towards international data exchange, the creation of supranational databases and accession to international information systems;
- application of advanced information from the contiguous side, from the subjects of interaction within the framework of the integrated border management system, etc.;
- the need to minimize the subjective factors associated with unauthorized unlawful interference with departmental databases;
- within the limits of technologization of border control – the use of databases that work with information obtained by means of contactless inspection of vehicles and persons, biometric identification [5, p. 111].

Thus, it dramatically reduces the risks associated with the use of forged documents, the use of biometric technologies, that is, automatic or automated methods for recognizing a person's personality by its biological parameters.

Ukraine's State Migration Policy Strategy for the period up to 2025 for the purpose of protecting documents certifying a person

confirms the citizenship of Ukraine or the special status of a person, it is determined that in order to increase the level of security of documents, Ukraine should ensure: "the issuance of biometric travel documents that meet the standards of the International Civil Aviation Organization (ICAO), including in consular offices of Ukraine abroad". It is anticipated that this will "expand opportunities for reducing irregular migration, combating transnational crime and terrorism" [6].

Biometric data is any data that characterizes a particular biometric parameter. With all the diversity of these parameters, a technology that takes into account the three facial recognition features (mandatory) is used in the field of the production of identity documents at the crossing of the state border (some other documents), as well as for biometric identification and verification in the world; fingerprint recognition; recognition of the iris of the eye. Of these, the first two are used in Ukraine. In 2018, a national system of biometric verification and identification of Ukrainian citizens, foreigners and stateless persons was established in Ukraine. The subjects of the national system are the State Migration Service of Ukraine, the State Border Guard Service of Ukraine, the National Police of Ukraine, the Ministry of Internal Affairs of Ukraine, the Ministry of Foreign Affairs of Ukraine, foreign diplomatic institutions, the Ministry of Infrastructure of Ukraine, the Security Service of Ukraine, the Foreign Intelligence Service Ukraine and the Ministry of Defense of Ukraine. The system administrator is the LCA of Ukraine [7]. Such a system, obviously, provides significant advantages in identifying offenders, facilitates the implementation of border formalities. In this case, biometric identification is the search "one to many" by recognizing and comparing one or two biometric data (parameters) of a person with biometric data (parameters) of persons in departmental information systems of subjects of the national system; biometric verification – the search "on a" one to one basis "between" the biometric data (parameters) received from the person at the moment and the biometric data (parameters) available in the departmental information systems of the subjects of the national system [7].

2. In the context of counteracting crime, A. Volovedov proposed the following view on the benefits of using documents with personal biometric data:

- a higher degree of protection against counterfeiting;
- the possibility of automatic verification of ownership of the document, reducing the time to identify the person, increases the speed of the specified procedure and excludes subjectivity in evaluating its results;
- the significant technological potential of the specified document, that is, the chip, other than identification data, can be recorded various other personal data;
- it makes no sense to fake and illegally use electronic documents with biometric data;
- biometric personal data collected when issuing electronic passports can be used in the investigation of offenses [2, p. 108].

3. Given the global nature of the unification of machine readable identity documents and increased requirements for aviation security, the development of regulations and standards in this area is the responsibility of the International Civil Aviation Organization (ICAO), which has been operating since 1968.

In 2005, 188 ICAO member states approved the Doc 9303 standard, according to which the identity documents are:

- machine-readable travel document (passport, visa);
- machine-readable passport (passport conforming to the specifications defined by Doc 9303);
- electronic passport – e-Passport (machine-readable passport containing a chip of a contactless integrated circuit on which the data is stored, including the biometric characteristics of the holder of the passport and data protection element) [8].

The unification of documents certifying a person when crossing the state border according to IKAO standards is in direct correlation with effective security provision in various spheres – border, aviation, and sea. Undoubtedly, technology in the areas of border control and others where there is control (for example, aviation security services) increases the possibilities for effective prevention of cross-border crime [10, p. 248]. It also speeds

up the implementation of border formalities and control procedures related to the need to provide increased protection of objects protected from penetration of unwanted persons, and secondly, it is connected with the need for control and passage of a significant number of people in limited time.

4. Any automated identification method is based on the comparison of the data of the identified object and the biometric standard. The units of border control for this purpose are equipped with software and technical complexes with functions of processing information about persons crossing the state border, their passport documents using electronic media of information, including the function of biometric control. Progress has not been in place and since the mid-2000s, automated Border Control systems – e-Gates (in the UK and Ireland), SmartGates (analogues in Australia and New Zealand), Parafe have been installed at various airports in the world. (in France), Global Entry (in the US), EasyPass system (in Norway), J-BIS (in Japan), Smart Entry Service (in Korea), Viajero Confiable (in Mexico). The number of e-Gates deployed globally at airports and train stations in Europe, Australia, Asia and America has tripled from 1100 in 2013 to over 3200 in 2018.

Travelers themselves pass ABC in the presence of a uniform ICAO ePassport. Upon completion of the identification process, a turnstile for the passage is opened. In addition, Dubai Airport – the only one in the world installed a LIDAR system that works when passengers pass through the corridor before luggage is delivered. Here, in automatic mode, they are identified by 3D scanning of individuals [11].

Today, more than 100 countries and international organizations issue ePassport, with over 490 million published. For example, the United Nations issued an electronic passport (e-UNLP) from 2012 for a period of five years [9].

5. The use of biometric technologies is extremely important in the fight against terrorism. This became clear with the spread of aviation terrorism. The first delights of the Arab terrorists of passenger aircrafts of the Israeli airline El-Al in 1968 were when the air safety system did not provide for thorough passenger control.

The focus of UN Security Council Resolution 2396 (2017) concentrates on the use of biometric technologies in the fight against terrorism [12]. In particular, art. 15 of this document stipulates that “Member States shall develop and implement systems to collect biometric data, which could include fingerprints, photographs, facial recognition, and other relevant identifying biometric data, in order to responsibly and properly identify terrorists, including foreign terrorist fighters, in compliance with domestic law and international human rights law, calls upon other Member States, international, regional, and subregional

entities to provide technical assistance, resources, and capacity building to Member States in order to implement such systems and encourages Member States to share this data responsibly among relevant Member States, as appropriate, and with INTERPOL and other relevant international bodies” [12]. Today, Interpol has biometric data of more than 41,000 foreign terrorist fighters (FTFs).

6. Border control units in Ukraine are equipped with an automated workplace with the function of fixing biometric data. The system of measures for improvement of border control is shown in the table 1.

Table 1

Place of biometric technologies in the system of measures for the improvement of border control

No c / n	Examples of Measures to Improve Border Control	Results
1	In the field of regime and control of compliance: a) risk management in the presence of a four-level entry and exit control system b) output of BCP of separate elements of control procedures using the system of transmission of the previous information	Responding to challenges and threats with simultaneous simplification for non-risk groups Systematization of the work of the control services
2	In the field of technical means of border control: a) systems for contactless inspection of vehicles and goods, as well as people, such as “body scanners” b) biometric readers	Increasing the likelihood of detecting caches and determining the type of substances with the help of a scanner Minimizing mistakes in personal identification and documents. Minimizing corruption risks. Increasing the level of integration, personalization and data transfer process of passports and other primary documents certifying a person. Fast and systematic transmission of information about lost and stolen passports to the Interpol database
	c) self-service kiosks such as “Smart border”	Minimize errors in person identification and documents. Reducing corruption risks to a minimum

№ c / n	Examples of Measures to Improve Border Control	Results
3	<p>In the area of database application:</p> <ul style="list-style-type: none"> a) introduction of common information systems with EU countries, in particular: <ul style="list-style-type: none"> – on the identification of passport documents for the right to cross the border by means of transport, etc.; – persons crossing the border who have committed offenses which are not allowed to enter the country or which are temporarily restricted to the right of departure, invalid, stolen and lost passport documents, etc. 	<p>Complete automation of detection processes of persons and vehicles that may be the subject of “interest” of law enforcement agencies.</p> <p>Concentration of attention of law enforcement personnel on “risk groups”.</p> <p>Sharp increase in the effectiveness of detecting criminal offenses or control over the actions of offenders</p>

This is made, in particular, for the purpose of implementing the measures envisaged by the Strategy of the State Migration Policy of Ukraine for the period up to 2025:

– by 2021 – to automate the processes of the National Biometric Verification and Identification System in the implementation of modern technical means, including biometric (parameters) recognition systems, in particular the face, and automatic photo quality check / matching;

– constantly – to intensify cooperation with EU Member States, international and non-governmental organizations in training on the safety of biometric travel documents and detecting forgery of identity documents.

Such systems have been developed, established and show positive results in some countries of the world. For example, from 2006 to 2016, the number of people who arrived in Australia increased from 21,7 million a year to 37,7 million, that is, almost 47%. This was due to the development and installation of the national system EBIS. The mentioned system is designed for 100 thousand transactions a day and greatly increased the possibility of collecting and storing biometric information, which obviously gives significant advantages in identifying offenders and facilitates the implementation of border formalities.

Conclusions

Recently, the information retrieval systems of biometric identification of a person by facial image on the operational data from cameras located in public places are becoming widespread in the world. Taking this fact into consideration, the possibilities of improving the automated information and information retrieval systems that are being armed with law enforcement agencies of Ukraine should be explored.

In some cases, a law-abiding ePassport owner is not interested in having a history of his travel discovered at the border. For example, some Arab countries are denied entry visas to third-country nationals holding Israeli visas. In some cases, a citizen, entering the United States through Canada, may not be interested in discovering the fact of a visit to a country that is included in the United States in the list of countries contributing to terrorism. Consequently, individuals with justified fears about entry bans are interested in partially falsifying passports by replacing a page with an unwanted visa or entry mark. These examples demonstrate the argument in favor of introducing an e-Visa electronic record that is recorded on the ePassport chip. This requires the improvement of the system for collecting

biometric information from applicants for a visa for the unique identification and further use of such data in the course of border control.

Since the introduction of electronic media containing biometric data of its owner allows to exclude the possibility of using these documents by another person, this is not only critical in light of the simplified visa (or visa-free) regime of movement across the state border, but also opens up new opportunities for the prevention of cross-border crime . In this case, the vulnerable place in the application of biometric technologies in Ukraine is the procedures for filing and processing applications for the issue of travel and primary documents. Another vulnerable place is the possibility of remotely removing data from the electronic chip, which determines the potential risk of unauthorized monitoring of people, which in turn poses a threat to human rights violations.

Perspective, in our opinion, is a study that will identify ways to minimize these risks from the use of biometric technologies.

References:

1. Talianchuk L. Kryminalistichne doslidzhennia dokumentiv, shcho posvidchuiut osobu pry peretyni derzhavnoho kordonu Ukrayny: dis. ... kand. yuryd. nauk. 12.00.09. K.: NAVS, 2016. 249 s.
 2. Volevodz A. Udostoverayushchiye lichnost' dokumenty s biometricheskimi personal'nymi dannymi: mezhdunarodnyye standarty, inostrannyy opyt, otechestvennoye pravovoye regulirovaniye i yego problemy. Uchenyye zapiski SPb filiala RTA. 2015. № 1(53). S. 87–117.
 3. Felson M. Routine Activity approach. Environmental criminology and crime analysis. Willan. 2013. P. 92–99.
 4. Lambert R. Routine Activity and Rational Choice. New York. Routledge. 2017. 428 p.
 5. Filippov S. Information support for counteraction to cross-border crime. Visegrad Journal on Human Rights. 2018. № 4(2). S. 107–112.
 6. Strateyhia derzhavnoi mihratsiinoi polityky Ukrayny na period do 2025 roku, skhvaleno rozpor. KMU vid 12 lypnia 2017 roku № 482-r. URL: <http://zakon.rada.gov.ua/laws/show/482-2017-%D1%80#n10/>
 7. Polozhennia pro natsionalnu systemu biometrychnoi verifikatsii ta identyfikatsii gromadian Ukrayny, inozemtsiv ta osib bez hromadianstva, zatverdzheno postanovou KMU vid 27 hrudnia 2017 roku № 1073. URL: <http://zakon.rada.gov.ua/laws/show/1073-2017-p>
 8. Doc 9303. Mashinoschityvayemyye proyezdnyye dokumenty. Chast' 3. Spetsifikatsii, obshchiye dlya vsekh MSPD. IKAO. URL: https://www.icao.int/publications/Documents/9303_p3_cons_ru.pdf
 9. ICAO. Security and Facilitation. Facilitation Programme. PKD. ePassport. Basics. URL: <https://www.icao.int/Security/FAL/PKD/Pages/ePassportBasics.aspx>
 10. Filippov S. The Borders Barrier Properties vs Cross-Border Criminality. Law Rev. Kyiv, 2017. № 2. P. 245–250.
 11. Aviaperelety skoro mozhno budet sovershat' bez pasporta. 23.06.2017. URL:http://www.biometrics.ru/news/aviapereleti_skoro_mozhno_budet_sovershat_bezi_pasporta/
 12. Resolution 2396 (2017). Adopted by the Security Council at its 8148-th meeting, on 21 December 2017. URL: https://digitallibrary.un.org/record/1327675/files/S_RES_2396%282017%29-EN.pdf