УДК 343.98
DOI: 10.37635/jnalsu.28(4).2021.289-300

Віолетта Омелянівна Коновалова

Науково-дослідний інститут вивчення проблем злочинності
імені академіка В.В. Сташиса
Національної академії правових наук України
Харків, Україна

Василь Миколайович Стратонов

Кафедра галузевого права
Херсонський державний університет
Херсон, Україна

Ірина Валеріївна Савельєва

Кафедра професійних та спеціальних дисциплін
Херсонський факультет Одеського державного університету внутрішніх справ
Херсон, Україна

БІОМЕТРИЧНІ ПЕРСОНАЛЬНІ ДАНІ ТА ЇХ ВИКОРИСТАННЯ В РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

Анотація. *Стаття присвячена аналізу біометричних персональних даних, які пропонується розглядати як джерело інформації про особу та використовувати під час досудового розслідування кримінальних правопорушень. Актуальність теми дослідження полягає в необхідності розроблення оптимального механізму використання біометричних персональних даних в діяльності органів досудового розслідування. Метою наукової роботи є аналіз чинного міжнародного та національного законодавства щодо визначення місця біометричних персональних даних в системі криміналістичних обліків, здійснення їх класифікації та надання рекомендацій з використання державними органами та приватними особами. Задля досягнення поставленої мети в роботі використовувалися діалектичний, історико-правовий, формально-логічний, догматичний, структурно-системний та порівняльно-правовий методи. Доведено, що накопичені в системі криміналістичних обліків різноманітні види біометричних персональних даних можуть успішно використовуватися в процесі розслідування кримінальних правопорушень, а в окремих випадках й приватними особами в межах їх статутних повноважень. Звернуто увагу, що поряд з позитивними результатами такої діяльності є певні ризики, а саме наявність загрози витоку та отримання доступу до біометричних даних сторонніми особами, про що свідчить негативна судова практика окремих країн щодо незадовільного збирання, обробки, зберігання та використання біометричних персональних даних. З огляду на зазначене, констатовано, що збирання, обробка та використання біометричних персональних даних з метою їх використання в процесі розслідування кримінальних правопорушень, мають відповідати певним вимогам, а саме: володільцем бази біометричних персональних даних має бути тільки держава в особі спеціального державного органу. Відповідно держава має забезпечувати зберігання й захист біометричних персональних даних*

Ключові слова: *кримінальне провадження, досудове розслідування, відбитки пальців, генетичні ознаки людини, криміналістичні обліки, криміналістична реєстрація*

Violetta E. Konovalova

Academician Stashis Scientific Research
Institute for the Study of Crime Problems
National Academy of Law Sciences of Ukraine
Kharkiv, Ukraine

Vasyl M. Stratonov

Department of Industry Law
Kherson State University
Kherson, Ukraine

Iryna V. Savelieva

Department of Professional and Special Disciplines
Kherson Faculty of the Odesa State University of Internal Affairs
Kherson, Ukraine

BIOMETRIC PERSONAL DATA AND THEIR USE IN THE INVESTIGATION OF CRIMINAL OFFENCES

Abstract. *The article is devoted to the analysis of biometric personal data, which is proposed to be considered as a source of information about a person and used during pre-trial investigation of criminal offences. The relevance of the research topic lies in the need to develop an optimal mechanism for using biometric personal data in the activities of pre-trial investigation bodies. The purpose of the research is to analyse the current international and national legislation on determining the place of biometric personal data in the criminal record system, implement their classification and provide recommendations for use by state bodies and individuals. To achieve this goal, the work used dialectical, historical-legal, formal-logical, dogmatic, structural-system and comparative-legal methods. It is proved that various types of biometric personal data accumulated in the criminal record system can be successfully used in the process of investigating criminal offences, and in some cases by individuals within the limits of their statutory powers. It was noted that along with the positive results of such activities, there are certain risks, namely, the presence of a threat of leakage and access to biometric data by unauthorized persons, as evidenced by the negative judicial practice of individual countries regarding unsatisfactory collection, processing, storage and use of biometric personal data. Taking into account the above, it is stated that the collection, processing and use of biometric personal data for the purpose of their use in the investigation of criminal offences must meet certain requirements, namely: the owner of the database of biometric personal data should only be the state represented by a special state body. Accordingly, the state should ensure the storage and protection of biometric personal data*

Keywords: *criminal proceedings, pre-trial investigation, fingerprints, human genetic characteristics, forensic records, forensic registration*

INTRODUCTION

Respect for the rule of law and maintaining law and order in society remains one of the most important functions of a democratic state. The system of state bodies and private individuals take a wide variety of measures to prevent offences in various spheres of socio-economic and socio-political life, as well as to investigate criminal offences that have already been committed. The development of technical means and the spread of digitalisation logically leads to their use in law enforcement activities. The data about the person that is the basis for their identification – personal data – comes to the fore. However, such activities contain not only undoubted benefits, but also potential threats to human rights and freedoms. Therefore, it is necessary to develop a balanced mechanism for their use with maximum efficiency and minimisation of risks.

The relevance of the research topic is due to two aspects: first, active legislative activity in this direction in Ukraine and the world. In particular, over the past few years, amendments have been made to the Law of Ukraine "On the Unified State Demographic Register and Documents Certifying Citizenship of Ukraine, a Person's Identity or Special Status" [1] and the Law of Ukraine "On Personal Data Protection" [2]. In 2017, the Regulations on national system of biometric verification and identification of citizens of Ukraine, foreigners and stateless persons was adopted (approved by the resolution of the Cabinet of Ministers of Ukraine of 27.12.2017 No. 1073) [3], and in 2018 – Instructions on the procedure for recording biometric data (parameters) of foreigners and stateless persons by officials of the State Migration Service of Ukraine, its territorial bodies and territorial divisions (approved by the order of the Ministry of Internal Affairs of Ukraine

of 23.11.2018 No. 944) [4]. At the end of 2020, draft law No. 4265 "On State Registration of Human Genomic Information" was submitted and considered [5].

In Europe, the GDPR came into effect on May 25, 2018 (*The General Data Protection Regulation*, 2016). The GDPR specifically identifies biometric data as a "sensitive" category of personal information, ensuring reliable protection. The GDPR defines biometric data quite broadly, including physical (physical or physiological characteristics of a person: face, fingerprints, iris scans, etc.) and behavioural characteristics of the person. An important advantage of the GDPR is that the data subject has the right to withdraw their consent to their storage and processing at any time. It is also worth noting that in April of this year, the European Parliament approved the creation of one of the world's largest biometric databases – *Common Identity Repository* (CIR), which will be designed to combine the records of more than 350 million people.

In the United States, the CCPA came into force on January 01, 2020 (*California Consumer Privacy Act*, 2018). It is impossible not to mention that the largest biometric database in the world is located in India (*Unique Identification Authority of India* – UIDAI), which includes more than 90% of the country's population, and biometrics are used everywhere.

Secondly, the relevance of the study is determined by a large number of offences in the field of collecting, storing and processing personal data. During 2017-2020 alone, more than 20 large-scale leaks of personal data of millions of people were recorded [6; 7]. At the same time, the owners of personal data databases were both public institutions and private companies. New, modern technologies that attackers use to their advantage also contribute to the activation of committing offences in this area. So, in 2016, *Vkansee* researchers unlocked an iPhone using fingerprints collected with *Play-Doh*. This indicates that even advanced biometric systems can still be vulnerable to forgery. Consequently, the challenge is to protect them from unauthorised use.

General theoretical issues of using personal data are considered by S. Dobrianskiy [8], M. Rizak [9], V. Shvydenko [10] and et al. Certain issues of using biometric personal data in the process of investigating criminal offences were covered by scientists V. Bondar [11], R. Melnyk [12], O. Petryshyn [13], V. Prykhodko [14], M. Shepitko [15; 16], V. Shepitko [17] and other scientists. However, there are no comprehensive studies on this issue in Ukrainian legal Science, which makes it difficult to develop a balanced mechanism for using biometric personal data, in particular in the process of investigating criminal offences, taking into account national and international legislation.

Consequently, the need to develop an optimal mechanism for using biometric personal data in the activities of pre-trial investigation bodies is an urgent need of modern forensic science. Considering the above, *the purpose of the article* is a development and provision of recommendations for the implementation of optimal mechanisms for collecting, processing, storing, and using biometric personal data. *Tasks of the author's team* are to analyse international legal acts and the current legislation of individual states on regulating the use of biometric personal data in conducting forensic records, classify personal data, develop, and provide recommendations on the work of state bodies and individuals with biometric personal data.

1. MATERIALS AND METHODS

The work was based on the following materials: the Law of Ukraine "On Personal Data Protection", departmental regulatory documents: "Instruction on the operation of the fingerprint accounting of the expert service of the Ministry of Internal Affairs of Ukraine", "Instructions on the procedure for forming and using automated accounting of human genetic traits".

The methodological basis of the research was a system of techniques and methods of scientific knowledge, in particular, the dialectical method was included, which made it possible to comprehensively perceive and systematically study theoretical and regulatory provisions concerning the collection, storage and processing of personal data in the process of investigating criminal offences. The study also applied such general scientific methods as description, which made it possible to study and describe a person as a single biological and social dynamic system, biometric data as a set of data about a person collected on the basis of recording its characteristics, having sufficient stability and significantly different from similar parameters of other persons (biometric data, parameters – digitized signature of a person, digitized face image of a person, digitized fingerprints), the dogmatic method became the basis for the interpretation of concepts used in the field of psychology, linguistics and other branches of non-legal knowledge, finding out the content and meaning of the concepts and terms used, justification of the proposal to change and supplement them. The formal-logical method made it possible to define terminology related to the digitisation of all spheres of human life, the use of innovative digital technologies, and so on. A comparative legal method that has a number of advantages, namely comparison, classification in order to determine the legal categories that characterise personal data, which are diverse information in content and uniform in origin. The structural-system method is used

to study the ways, forms, concentration and systematisation of information that accumulates in the criminal record system as a subsystem of means of forensic registration, which differs in accounting data, the system of recorded data and the procedure for collecting, registering, systematising, storing and searching such data. Also, algorithms for recognising a wide variety of biometric indicators of a person, which in the future can be introduced as interrelated fingerprint and portrait identification, identification features for which are taken into account in various automated identification systems.

Among the special methods used: the historical and legal method made it possible to study the formation and implementation of informatisation on the basis of the Ministry of Internal Affairs of Ukraine and central executive authorities, the introduction of a unified information system, which over the past five years has been improved in order to ensure a high level of its reliability and trouble-free functioning. One of the most important areas of such activity was the development of automated public data banks based on the existing unified software and hardware complexes of the DIT divisions and the Expert Service of the Ministry of Internal Affairs of Ukraine. The integration of these information resources was supposed to create prospects for automating the information and search engine for identifying a person based on a face image. The formal legal method made it possible to study the norms of the Law of Ukraine "On Personal Data Protection", other laws of Ukraine, departmental regulatory documents, namely "Instruction on the operation of the fingerprint accounting of the expert service of the Ministry of Internal Affairs of Ukraine", "Instructions on the procedure for forming and using automated accounting of human genetic traits". Sociological and statistical methods made it possible to elicit the views of academics, investigators and experts in the context of the study.

2. RESULTS AND DISCUSSION

Personal data is diverse information in content and uniform in origin. All of them describe the individual as a single biological and social dynamic system. One of the subspecies of personal data is biometric. They are widely used for identity verification (identification) in order to provide access rights to gadgets, office and industrial premises, vehicles and information with restricted access, for making payments, for crossing state borders and receiving financial services. Therefore, the collection, use and processing of biometric data has long been part of the daily life of society.

International law classifies biometric personal data as "sensitive", that is, such that improper use of which leads to a violation of human rights and freedoms. Article 6 of the Council of Europe Convention No. 108 stipulates that such information should not be processed automatically if the national legislation does not provide for sufficient guarantees for its protection. The Regulation of the Council of Europe clarifies that the mentioned Article 6 of the convention does not contain an exhaustive list of "sensitive" personal data in general and biometric personal data in particular [18, p. 28]. However, despite the significant history of the formation and development of the protection of human rights and freedoms, there is no reason to call the EU human rights protection system a fully formed system without the need for further improvements [8, p. 57].

National Ukrainian legislation defines biometric data as a set of data about a person collected on the basis of recording its characteristics, which have sufficient stability and significantly differ from similar parameters of other persons (biometric data, parameters — digitized signature of a person, digitized image of a person's face, digitized fingerprints) [1]. Biometric data is characterised by biometric parameters, which are measurable physical characteristics or personality behavioural traits that are used to identify a person or verify the identification information provided about a person. In a narrow sense, biometric data includes a person's fingerprint, iris or retina, features of limbs, face, ear, tongue print, voice, location of veins, DNA, ECG, signature. In a broad sense, biometric data also includes human behaviour (in terms of features that can be distinguished): physical movements (the way of walking); the force/speed of pressing the screen, keyboard; the way an individual enters data (with their finger (which one), stylus), how the device is held (for example, the angle of inclination of the phone), etc. [9, p. 92]. The special status of biometric personal data is also determined by the inability to change them, unlike other personal data [19]. Yes, one can change their first and last name, passport details, residential address, and phone number. In some cases, even the date and place of birth and taxpayer identification number must be replaced. However, fingerprints, the location of veins, DNA, and voice cannot be changed. Therefore, it is biometric personal data that requires a special procedure for collecting, processing and storing it. Biometric personal data is a part of the persona, and it can be "read" and recorded, so there is no risk of forgetting or losing it. However, because they are unique, they cannot be replaced. Therefore, if biometric data has been compromised, it can lead to the destruction of an individual's social life.

Complete digitisation of all spheres of human life, the use of innovative digital technologies has a number of advantages: reducing costs, resources, time for information processing, fast analysis of large amounts of data, increasing labour productivity, more accurate forecasts in various spheres of life, etc. [20, p. 186].

The level of security of these biometric data is directly proportional to the level of security of their protection on the part of the database owner and manager. It is believed that the storage of biometric personal data by distributing it in different places, as well as a multi-level method of identity authentication to grant access rights, are necessary conditions for the security of such data. Our belief in the need to strengthen the level of protection of biometric personal data is based on examples of numerous large-scale leaks of personal data around the world over the past few years.

In particular in supermarket chains *Morrisons* (£10,500 fine), *British Airways* (£183 million fine), data leak of 500 million *Marriott* users in November 2018, *Nova Poshta* (in the spring of 2018, screenshots of the customer passport data database were leaked, an unscheduled inspection found no evidence), *Uber* in December 2017 (the company paid a ransom of $ 100,000 for non-disclosure of data) [21]. In 2017, a personal data leak occurred in the largest bank in Ukraine, and in 2018 – in the world's most popular social network, the most common taxi service and the largest delivery service in Ukraine [10]. In 2019, access to the Chinese Smart city database could be obtained *from* a web browser without a password. This database contained gigabytes of information, including facial recognition data from hundreds of people. The data was hosted on the cloud platform of the Chinese tech giant Alibaba [22]. The FBI has arrested 33-year-old programmer Paige Thompson. She is suspected of stealing the data of 106 million users of the American bank Capital One, mainly citizens of the United States and Canada [6].

Well-known companies from various sectors of the economy also become targets of hacker attacks with theft of personal data, such as *FacebookInc* (there are already many cases, in one of which the fine is $5 billion). It contained data from 133 million Facebook users from the United States, 18 million from the United Kingdom, and 50 million from Vietnam [7]. There were also leaks of personal data in *Toyota* and *Lexus* (hackers stole information about car owners in March 2019), *Suprema Biostar* (August 2019), *Mastercard* (August 2019), *Habr.com* (August 2019), *Yves Rocher* (September 2019), Darimax (Russian Federation, September 2019), *Novaestrat* (data leak on almost all residents of Ecuador, September 2019) and many others [21]. Therefore, the issue of storing and processing biometric personal data is particularly relevant.

In most cases, users of digital technology and the Internet protect personal information individually, using a variety of technologies [13, p. 19; 23]. However, the security of using biometric personal data in the process of investigating criminal offences should be ensured by the state, since such activities are one of the main tasks of the state. Judicial practice in cases of misuse of biometric personal data by private individuals confirms the need for the state to guarantee the security of storage and use of such data. In 2019, the owner of a fitness club in Kazan (Russian Federation) challenged in court the decision of Roskomnadzor to impose a fine of 10,000 RUB for using the PACS system to identify visitors from a photo when passing through a turnstile without their written consent. The court did not satisfy the complaint, referring to the fact that the photo is biometric personal data, and their use requires the written consent of the owner [24].

Decision of the Supreme Court of Illinois (USA) of 25.01.2019 in the case of the corporation *Rosenbach v. Six Flags Entertainment Corporation* confirmed the need for written consent to the collection and processing of biometric personal data [21]. In this case the parents of a minor child filed a lawsuit against the amusement park *Six Flags Great America*. They claimed that their child's biometric data was collected without consent and violated BIPA (performing biometric scanning at the turnstile to prevent fraud and provide access in case of ticket loss). The Illinois Supreme Court ruled that *Six Flags Entertainment Corporation* violated BIPA. The court's decision concluded that it is not necessary to prove the damage and it is enough that the collection was incorrect.

Biometric personal data is now widely used in the banking sector, in the field of providing financial services and making payments for services rendered. Thus, from 2015 to 2020, the Ladoshki project (Russian Federation) collected data on the structure of palm veins of tens of thousands of Russian children for use in the school food payment system [25]. Despite the 5-year period of the project's existence, there is still no consensus even among representatives of state bodies on the legality of all aspects of its activities. There are the first attempts to use fingerprints to register an employee's working hours in private companies. Thus, they try to maintain work discipline, because the fingerprint is not a card, it is impossible to transfer it to another person to register.

Banks are increasingly investing in new technologies: machine learning; real-time fraud reporting; voice, face, and fingerprint recognition (biometric data), as well as so-called behavioural biometrics, which include customer interaction profiles with their devices and online banking tools. Since 2018, the Central Bank (Russian Federation) has started collecting biometric personal data to identify individuals when providing financial services. This data is entered in a single biometric system and collected by many banking institutions. Since 2019, PrivatBank (Ukraine) has launched FacePay24 payment technology [26]. To counteract this,

cybercriminals have created a digital fingerprint market, and fraudsters have learned to record and reproduce customer voices using new technologies [27, p. 174].

Only a few states are gradually beginning to fill in large-scale regulatory gaps in regulating the use of biometric personal data by digital banks. It is very likely that in the near future, innovative technologies will radically change the structure of the economy, the labour market and the construction of society as a whole [28, p. 159]. Currently, the analysis of the current legislation of Ukraine suggests that the Ukrainian legislation protects the rights of Ukrainians much more closely than the CCPA, BIPA and GDPR, resulting in possible abuses. Violation of the Ukrainian national legislation on the rules for handling biometric personal data entails administrative and criminal liability. At the same time, an important achievement of the GDPR is the consolidation of the "right to erasure". According to it, the subject of biometric personal data has the right to withdraw their consent at any time. The consequence of revoking such consent under national law may be the "archiving" of such data without the possibility of further use, or deletion from the database. In April 2020, the European Parliament approved the creation of one of the world's largest biometric databases. It will be called the *Common Identity Repository* (CIR) and will contain records of more than 350 million people. The largest biometric database in the world is currently created in India (it includes data on more than 90% of the country's population, and biometrics are used everywhere) – UIDAI (*Unique Identification Authority of India*). Each person is assigned a unique personal number – AADHHAAR.

Biometric personal data is widely used in criminal proceedings. One of the most important and effective ways to achieve forensic tasks is forensic registration in general and maintaining forensic records in particular. Forensic registration (in the scientific literature, the term "criminal registration" is also often used) is a system of material objects (file cabinets, databases, collections and other information repositories) and a practical registration activity [12, p. 186]. It was the materialistic understanding of the world around us, the laws of dialectics and the theory of knowledge that became the basis for the development of the doctrine of forensic registration. Its development is closely connected with the teachings on the mechanism of trace formation and methods of committing criminal offences, on recording evidentiary information, and directly with the theory of forensic identification. Forensic registration also occupies a prominent place in the activities of Interpol. V. Shepitko emphasises the importance of creating and using judicial (international) records of Interpol as the most effective means of countering international crime [17, p. 184]. The doctrine of forensic registration is a scientific theoretical basis for a whole criminal record system, its development and designing of organisational forms and technical support. Biometric personal data is used to achieve the goals of forensic registration, namely:

1) accumulation of data that can be used to investigate and prevent criminal offences;
2) providing conditions for identifying objects whose attributes are accumulated in the credentials;
3) assistance in finding objects whose attributes are accumulated in their credentials;
4) providing reference and orientation information to operational-search and investigative units of law enforcement agencies and judicial bodies.

Accounting as a subsystem of forensic registration tools differs in record data, methods and forms of their concentration and systematisation. Accounting is both a system of recorded data and a procedure for collecting, registering, organising, storing and searching such data. According to incomplete information of R. Melnik, the modern system of forensic registration unites more than 30 types of objects of different origin and features [12, p. 185]. Forensic registration is conducted not only in Ukraine, but also in foreign countries. Thus, the model legislation establishing effective control over persons who have committed sexual offences is the legislation of the United Kingdom. The law on sexual offences, adopted in 2003, provides that persons who have committed sexual crimes are registered in a special database [15, p. 6], which contains, among other things, biometric personal data.

Biometric personal data contained in forensic records is used in the investigation of all types of criminal offences. Thus, M. Shepitko notes that during the investigation of judicial errors, investigators should search for and seize case materials and documents relevant to the case, namely recordings of the court session, audio and video recordings of the court session, a document confirming payment of the court fee, etc. [16, p. 136]. It is impossible to identify individuals on video and audio recordings of court sessions without using biometric personal data, in particular voice, speech and facial images. In 2016, the creation of a Unified Information System (hereinafter, UIS) of the Ministry of Internal Affairs began in the system of bodies subordinate to the MIA. During 2016-2020, implementing the concept of informatisation of the Ministry of Internal Affairs of Ukraine and central executive authorities, the implemented UIs was improved in order to ensure a high level of its reliability and trouble-free operation. One of the most important areas of such activity was the development of automated public data banks based on the existing unified software and hardware complexes of the DIT divisions and the Expert Service of the Ministry of Internal Affairs of Ukraine. The integration

of these information resources was supposed to create prospects for automating the information and search engine for identifying a person based on a face image. Also, since 2016, the provisions of the Law of Ukraine "On the Unified State Demographic Register and Documents Certifying Citizenship of Ukraine, a Person's Identity or Special Status" have been implemented, in particular, the registration of a passport of a citizen of Ukraine in the form of a card containing an electronic contactless chip with simultaneous fingerprint registration. Another element of the integrated automated system was the automated identification systems used by the Expert service of the Ministry of Internal Affairs of Ukraine (fingerprinting, signs of appearance).

Taking into account the capabilities of modern algorithms for recognising a wide variety of biometric indicators of a person, it is possible in the future to introduce interrelated fingerprint and portrait identification, the identification features for which are taken into account in various automated identification systems. According to V. Bondar, the functioning of such a system provides for a qualitatively new level – information-analytical processing of information arrays [11, p. 30]. Agreeing with him, we believe that the collection and processing of experimental data and computational forensic methods, as well as image analysis in forensic research, occupy a special place in analytical processing. Therefore, the essence of information and analytical support can be expressed by the formula "source information – the subject of forensic science – technology and technique of forensic science – the necessary information", which can be understood as the process of movement of forensic information from its receipt to processing by special subjects with the use of special knowledge and scientific and technical means and technologies in order to solve forensic problems [11, p. 31].

The provisions of the Law of Ukraine "On Personal Data Protection" apply to maintaining forensic records of biometric personal data. They provide for the processing of personal data, which is carried out using both automated and non-automated means, which are contained in the file cabinet, or will be entered in the file cabinet. Also, today there are instructions for regulating the procedure for the formation and functioning of certain types of forensic records, in particular instructions for organising the functioning of forensic records of the expert service of the Ministry of Internal Affairs [29], instructions on the procedure for the functioning of fingerprint records of the expert service of the Ministry of Internal Affairs of Ukraine [30], instructions on the procedure for the formation and use of automated accounting of human genetic traits [31]. The operation of these instructions provides legal regulation of each of the links of activities for conducting forensic records, which, for its part, creates conditions for relativity, reliability, and the possibility of verifying the information contained in this record [14, p. 92].

It is worth considering forensic records containing biometric personal data in more detail. According to paragraph 1.5. of the Instruction on the organisation of the functioning of criminal records of the Expert Service of the [29], among the criminal records that include biometric personal data, the following can be distinguished:

1) Dactyloscopic records;
2) records of persons on the basis of their physical appearance;
3) records of genetic traits of a person;
4) records of voices and speech records of persons.

Dactyloscopic record is leading among other types of criminal records, due to a large number of traces of human hands that remain during the commission of criminal offences. This type of record is one of the first record-keeping activities in the history of the development and refinement of state authorities in the investigation of crime. Dactyloscopic record is used to search for people who are missing; to establish the identity of a person behind an unidentified corpse; to confirm the identity of a previously fingerprinted person; to identify persons who left handprints at the scene; to establish the facts of leaving handprints by one person during the commission of various criminal offences. Elements of the dactyloscopic record subsystem are the handprint card index and the fingerprint card index. Both elements of the subsystem are interrelated, complement each other, and are used in four areas of verification: fingerprint card index-print, print-fingerprint card index, print-print, and fingerprint card index-fingerprint card index. Modern automated dactyloscopic information systems (ADIS) facilitate and speed up the processing of dactyloscopic information, as well as the search for necessary data about specific accounting objects and individuals among a large number of similar data. The structural divisions of the State Scientific Research Forensic Centre (SSRFC) of the Ministry of Internal Affairs of Ukraine use ADIS software and hardware complexes: "Sonda" and "Dakto 2000". Also, for the purpose of registering dactyloscopic objects, ADIS software and hardware complexes are used, which are equipped with colourless image input scanners, which scan fingerprints, fingerprints index card or a photograph of a footprint and display them on a monitor screen. Having entered fingerprint information into the computer, such systems are used to check and establish the coincidence or discrepancy of certain objects [32, p. 282].

Record persons on the basis of their physical appearance is intended, first of all, to ensure the achievement of operational search tasks of pre-trial investigation of criminal offences. At the regional and local levels, subjective portraits of persons suspected of committing criminal offences are subject to registration. At the written request of employees of operational units of the National Police of Ukraine, such subjective portraits are compiled. If a person who has been subjected to a subjective portrait is identified, their photo after being detained is transferred to an expert unit by an employee of the National Police of Ukraine – the initiator of the subjective portrait assignment.

Automated record of genetic traits is conducted at the central and regional levels. Its functioning is carried out using the AIRS "MC-Lab", the database of which stores DNA profiles of persons suspected or accused of committing criminal offences, taken into custody, convicted persons only in the case of their voluntary consent, as well as biological traces seized during the inspection of the scene, other investigative actions and operational search measures, unidentified corpses. The draft Law of Ukraine "On State Registration of Human Genomic Information" offers a slightly different list of tasks of such registration, namely prevention of criminal offences; identification of persons who have committed criminal offences; search for persons who are missing; identification of unidentified bodies (remains); identification of the face of a person who, due to their state of health or age, cannot provide information about themselves. In contrast to the current legislation, which provides for exclusively voluntary registration of genetic traits of persons suspected or accused of criminal offences, detained, convicted persons, the draft law of Ukraine rightly provides for mandatory registration of genomic information, including concerning persons prosecuted for intentional crimes against life, health, sexual freedom, sexual integrity of a person in respect of whom a measure of restraint has been chosen; persons who have committed socially dangerous acts against the life, health, sexual freedom or sexual inviolability of a person to whom compulsory measures of a medical nature have been ordered by a court; persons convicted of intentional crimes against life, health, sexual freedom and sexual integrity or a person; information established in biological material seized during investigative actions from places of commission of criminal offences committed in conditions of non-obviousness, or obtained during pre-trial investigation and not identified; unidentified corpses of people and their remains, information about the discovery of which is registered in the Single Register of Pre-Trial Investigations and an investigation has been initiated; missing persons, which, by court order, can be ascertained through molecular genetic examination (research) of previously taken biological samples or biological material taken from the missing person's personal effects.

After conducting expert studies of objects (their copies or images), the experts who conducted them draw up registration cards and add them to the operational search records. The object is checked in the criminal record system upon a written request of the established sample. The initiator is informed about the results of such verification by sending them a standard document of the established sample [32, p. 283].

Records of voices and speech covers the following types of collections:

1) the first type of collection includes audio recordings of voices and speech of individuals, as well as transmitting messages about threats to the safety of citizens and other socially dangerous acts anonymously;

2) the second type of collection includes audio recordings of voices and speech of identified persons who transmit messages about a threat to the safety of citizens and other socially dangerous acts.

Audio recordings of voices and speech of identified and unidentified persons are included in the collections in analog and digital format. Audio recordings of the voices and speech of identified persons are carried out by employees of the National Police of Ukraine, who conduct a pre-trial investigation, which involves a specialist in the recording process. Audio recordings of voices and speech of unidentified persons are carried out by duty units of territorial divisions of the state emergency service of Ukraine. Audio recordings attached to collections can be used for conducting expert research and investigative (search) actions.

Biometric personal data is also recorded in the system of the National Police of Ukraine. Units of the Department of Information and Analytical Support of the National Police of Ukraine (hereinafter – DIAS) are responsible for the functioning of forensic records of operational-investigative and reference-informational purposes. These subdivisions include territorial departments of information-analytical support of the National Police, sectors of information and analytical support, as well as individual information support workers of district police bodies. These forensic records are formed into an automated database, the arrays of which comprise the records of the objects of record within a separate automated information subsystem. The data on the objects of record are contained in electronic cards. In 2017, the "information Portal of the National Police of Ukraine" (hereinafter – IPNP) was created, which combined numerous previously available forensic records. As an information and telecommunications system, it is an integral part of the unified information system of the Ministry of Internal Affairs of Ukraine. The information portal of the National Police of Ukraine consists of the following subsystems: "Person", "Wanted", "Inquest", "License plates", "Administrative

practice", "Harpoon", "Delivered", "Unified accounting", "Criminal weapons", "Registered weapons", "Road accidents", "Wanted vehicles", "Cultural values", "Document", "House arrest", "corruption", "Atrium", "Dactyloscopic record".

It is important to take a closer look at the subsystems that include recording biometric personal data of individuals. The information subsystem "Person" takes into account information about persons involved in the commission of criminal offences, as well as in respect of whom employees of the National Police of Ukraine carry out preventive activities. The entire data array is divided into categories [33, p. 123]:

– "defendants" includes data on accused persons whose indictment has been sent to court;

– "previously convicted" – data on persons who were released from prison and served a sentence for an intentional crime and in respect of whom the criminal record has not been removed;

– "released from serving a sentence with probation" – data on persons given a non-custodial sentence;

– "administrative supervision" – data concerning previously convicted persons for whom administrative supervision has been established on the basis of a court ruling on the initiative of the police or in places of deprivation of liberty;

– "formal supervision" – data on previously convicted persons who have not been sentenced to imprisonment, as well as persons in respect of whom the term of administrative supervision has expired, and the criminal record has not yet been repaid (removed);

– "mentally ill" – data on persons with severe mental disorders and diseases and at the same time registered in health care facilities;

– "prostitutes" – data on persons who have been brought to administrative responsibility for prostitution;

– "Involved in ITN" – data on persons who have committed offences related to illicit trafficking in narcotic drugs and psychotropic substances;

– "delinquent child" – data on children who are on preventive registration and in respect of whom accounting and preventive cases are conducted;

– "domestic abuser" – data on persons who have committed domestic violence and against whom a formal warning has been issued that such violence is inadmissible.

The specified subsystem has a reference-informational purpose. The use of the data contained in it ensures the verification of information about individuals and the establishment of their location. Thus, law enforcement officers, if they find information about a person in a particular category of the "person" information subsystem, receive approximate information about them, which in turn contributes to the correct qualification of the event.

The information subsystem "Wanted" contains data on persons evading pre-trial investigation, trial, serving sentences, missing persons and other categories of persons wanted. By its purpose, this subsystem is operational-search and contains information about persons who have been or are subject to criminal liability, as well as missing persons. At the same time, the information subsystem "Inquest" contains data on persons hiding from the authorities, unidentified corpses, missing persons, persons who cannot provide any information about themselves due to their health or age. Data in the specified subsystem is formed by categories, for example, "unknown child", "unidentified corpse", "unknown patient".

The information subsystems "Wanted" and "Inquest" are interrelated due to the features of the objects of record. Thus, the same object can be in both information subsystems at the same time, e.g. a person evading serving a criminal sentence is counted in the IS "Wanted" and the same person as an unknown patient is counted in the IS "Inquest" (if in the process of evading serving the sentence, there was a traffic accident that resulted in the person being admitted to hospital without consciousness or identity documents). Therefore, in the process of entering information into these information subsystems, cross-validation of data is mandatory.

An electronic registration card is created for each registered person in the information subsystems "Person", "Wanted" and "Inquest". It records personal data of the person, citizenship, place of registration and actual residence, passport data, type and amount of the last sentence and articles of the Criminal Code of Ukraine under which such is assigned; date of release from the place of deprivation of liberty (if a penalty related to deprivation of liberty was imposed); category of registration and basis of registration of the person; date of registration of the person for preventive registration; registration number and date of material; type of offence and articles of the Criminal Code of Ukraine; brief plot (place, time and brief description of the circumstances of the offence, the nature of violent actions, motives, other information collected concerning the offence); additional information about the person, that directly characterise their lifestyle, and so on.

The information subsystem "Dactyloscopic record" contains data with dactyloscopic information and is an electronic array of fingerprint card indexes that are compiled in relation to persons detained on suspicion

of committing offences, unidentified corpses and persons who cannot provide any information about themselves due to illness or age. Thus, the data of the specified subsystem contains fingerprint card indexes of persons registered in other information subsystems.

Access to information contained in the information resources of the Information Portal of the National Police of Ukraine is limited. Authorised users may use such data within the limits of their functional responsibilities and the level of access provided to them. In total, there are four levels of access to IPNP data, which provide for searching or viewing information, and one level for entering information into information resources. Each user can only have one level of access to search or view.

Information from the information subsystems of the IPNP in the form of extracts is provided at the official requests of the prosecutor's office, pre-trial investigation, court, operational divisions of the National Police of other regions, officials of state authorities and law enforcement agencies of other states [33, p. 123].

CONCLUSIONS

The study found that biometric data is important in organising pre-trial investigations, as it facilitates the identification of an individual. At the same time, their active use also creates new threats to the security of both the state and the individual, and can also cause new organisational and legal problems, primarily regarding the collection and storage of biometric data and ensuring their confidentiality. It is indicated that biometric data should be divided into two groups, where the first group includes information related to body characteristics (physical or physiological features of a person), and the second – information related to human behaviour (any behavioural characteristics that are unique to a person and therefore can be identified). It is proved that the collection, processing and use of biometric personal data for use in the pre-trial investigation of criminal offences must meet the following requirements:

1) the owner of the database of biometric personal data should only be the state represented by a special state body. Accordingly, the state should ensure the storage and protection of biometric personal data;

2) physically, the media (servers) that store the database with biometric personal data must be located on the territory of the state, as this is a matter of national security;

3) the state may allow individuals to use a limited amount of biometric personal data to carry out their statutory activities only with the written consent of the persons who identify such data, and without the possibility of copying and accumulating them.

These types of biometric personal data are subject to state registration with the possibility of their use in the process of pre-trial investigation of criminal offences. It is concluded that the creation of a single automated information and analytical system of accounting for biometric personal data in the system of law enforcement and permitting authorities will create conditions for solving important tasks, namely:

1) to ensure the collection of complete information about objects with the formation of an "electronic profile" of potential offenders, identification and analysis of existing links with other objects and events of a criminal and illegal nature;

2) to record the social activity of persons who become involved in criminal proceedings, the emergence and change of their networks, and to analyse the degree of interest in them;

3) to improve the planning of investigative (search) actions and secret (search) actions, taking into account the complex set of numerous factors that affect the development of a particular investigative situation;

4) to form a set of methodological recommendations based on the analysis of a constantly updated array of all investigative situations and options for their development.

REFERENCES

[1] Law of Ukraine No. 5492-VI "About the Unified State Demographic Register and Documents Confirming the Citizenship of Ukraine, Identity or Special Status". (2012, November). Retrieved from https://zakon.rada.gov.ua/laws/show/5492-17#Text.

[2] Law of Ukraine No. 2297-VI "About Personal Data Protection". (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17#Text.

[3] Resolution of the Cabinet of Ministers of Ukraine No. 1073 "On Approval of the Regulation on the National System of Biometric Verification and Identification of Citizens of Ukraine, Foreigners and Stateless Persons". (2017, December). Retrieved from https://zakon.rada.gov.ua/laws/show/1073-2017-%D0%BF#Text.

[4] Order of the Ministry of Internal Affairs of Ukraine No. 944 "On Approval of the Instruction on the Procedure for Recording Biometric Data (Parameters) of Foreigners and Stateless Persons by Officials of the State Migration Service of Ukraine, its Territorial Bodies and Territorial Subdivisions". (2018, November). Retrieved from https://zakon.rada.gov.ua/laws/show/z1428-18#Text.

[5] Draft Law No. 4265 "On State Registration of Human Genomic Information". (2020, October). Retrieved from http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=70249.
[6] In the United States, the programmer is suspected of stealing data from 106 million people (2019). Retrieved from https://ms.detector.media/ kiberbezpeka/post/23263/2019-07-30-u-ssha-programistku-pidozryuyut-u-kradizhtsi-danikh-106-milioniv-osib/.
[7] The database with the numbers of 419 million Facebookusers in the public domain (2019). Retrieved from https://ms.detector. media/kiberbezpeka/post/23451/2019-09-05-baza-danikh-z-nomerami-419-mln-koristuvachiv-feisbuku-opinilasya-u-vidkritomu-dostupi/.
[8] Dobrianskiy, S. (2019). Legal security of human rights in the European Union: Current state and perspectives of development. *Journal of the National Academy of Legal Sciences of Ukraine*, 26(4), 55-72.
[9] Rizak, M. (2013). Classification of personal datas a necessary element of the introduction of effective communication in society. *Scientific Bulletin of the International Humanities University. Series: Jurisprudence*, 6-3(1), 91-95.
[10] Shvydchenko, V. (2018). *Painful protection of personal data: New problems of Ukrainian business to changes in EU rules*. Retrieved from https://www.eurointegration.com.ua/experts/2018/05/31/7082338/.
[11] Bondar, V.S. (2017). Ways to improve the information-analytical processing of information arrays of forensic records. *Current Problems of State and Law,* 78, 28-33.
[12] Melnyk, R.V., & Holdynskyi, I. (2016). Organization and practical use of forensic records in the detection and investigation of crimes. *Law and Society*, 2(3), 184-189.
[13] Petryshyn, O., & Hyliaka, O. (2021). Human rights in the digital age: Challenges, threats and prospects. *Journal of the National Academy of Legal Sciences of Ukraine*, 28(1),15-23.
[14] Prykhodko, V. (2018). The normative and legal provision of criminalistics databases of the Ministry of Internal Affairs of Ukraine. *Scientific Bulletin of the International Humanities University. Series: Jurisprudence*, 34, 90-93.
[15] Shepitko, V., Tishchenko, V., Shepitko, M., Marysiuk, K., & Sychova, V. (2019). Some aspects of foreign experience in combating human trafficking. *Journal of Legal, Ethical and Regulatory Issues*, 22(5), 1-8.
[16] Shepitko, M.(2020) Criminal legislation trends in Ukraine (evidence from crimes against justice). *Journal of the National Academy of Legal Sciences of Ukraine*, 27(2), 131-141.
[17] Shepitko, V., & Shepitko, M. (2021). The role of forensic science and forensic examination in international cooperation in the investigation of crimes. *Journal of the National Academy of Legal Sciences of Ukraine*, 28(1), 179-186.
[18] Guide to European law in the field of personal data protection. (2015). Retrieved from https://rm.coe.int/168044e84e.
[19] Clarification of the main provisions of the Procedure for notifying the Commissioner to determine the processing of personal data that poses a special risk to the rights and freedoms of personal data subjects. (2014, January). Retrieved from https://zakon.rada.gov.ua/laws/show/n0003715-14#Text.
[20] Velykanova, M. (2020). Artificial intelligence: Legal problems and risks. *Journal of the National Academy of Legal Sciences of Ukraine*, 27(4), 185-198.
[21] Bryhynets, S. (2019). *Biometric data: Collection and protection in Europe, USA and Ukraine*. Retrieved from https://yur-gazeta.com/publications/practice/inshe/biometrichni-dani-zbir-i-zahist-u-evropi-ssha-ta-ukrayini.html.
[22] Security lapse exposed a Chinese smart city surveillance system. (2019, May). Retrieved from https://techcrunch.com/2019/05/03/china-smart-city-exposed/.
[23] Carrillo, E., & Sequera, M. (2020). Personal data in the social security institute: Exploratory analysis on some personal data protection practices in the social security system of the paraguayan state. *Revista de Direito, Estado e Telecomunicacoes*, 12(2), 14-37.
[24] Belyaeva, Yu. (2020). *3 topical questions about personal data processing: We are looking for answers in fresh explanations of the regulator and court cases*. Retrieved from http://www.garant.ru/ia/opinion/author/belyaeva/ 1402489/#ixzz6cFW6QFjV.
[25] Operation "Children's palms". Why does Sberbank collect biometric data from schoolchildren? (2020). Retrieved from https://thebell.io/operatsiya-detskie-ladoshki-zachem-sber-sobiraet-biometricheskie-dannye-shkolnikov.
[26] PrivatBank has launched the technology of payment by face. (2019). Retrieved from https://ms.detector.media/kiberbezpeka/post/23493/2019-09-12-privatbank-zapustiv-tekhnologiyu-oplati-za-dopomogoyu-oblichchya/.
[27] Bem, M.V., Horodiskyi, I.M., Sutton, H., & Rodionenko, O.M. (2015). *Personal data protection: Legal regulation and practical aspects*. Kyiv: K.I.S.
[28] Stefanchuk, O., Muzyka-Stefanchuk, O., & Stefanchuk, M. (2021). Prospects of legal regulation of relations in the field of artificial intelligence. *Journal of the National Academy of Legal Sciences of Ukraine*, 28(1), 157-168.

[29] Order of the Ministry of Internal Affairs of Ukraine No. 390 "About the Statement of the Instruction on the Organization of Functioning of Criminalistic Records of Expert Service of the Ministry of Internal Affairs". (2009, September). Retrieved from https://zakon.rada.gov.ua/laws/show/z0963-09#Text.
[30] Order of the Ministry of Internal Affairs of Ukraine No. 785 "On Approval of the Instruction on the Procedure for Functioning of Dactyloscopic Accounting of the Expert Service of the Ministry of Internal Affairs of Ukraine". (2001, September). Retrieved from https://zakon.rada.gov.ua/laws/show/z1066-01#Text.
[31] Order of DNDEKC of the Ministry of Internal Affairs of Ukraine No. 19/50-227н "Instruction on the Procedure for Forming and Using an Automated Human Genetic Trait". (2013, September).
[32] Prykhodko, V.O. (2018). Forensic records of search purpose of the Expert Service of the Ministry of Internal Affairs of Ukraine – sources of forensic-significant information. *Comparative and Analytical Law,* 3, 281-284.
[33] Prykhodko, V.O. (2018). Forensic records of the Department of information and analytical support of the National Police of Ukraine. *National Law Journal: Theory and Practice*, 4-2(32), 122-128.

Violetta O. Konovalova

Doctor of Law, Professor
Full Member (Academician) of the National Academy of Legal Sciences Ukraine,
Chief Researcher
Institute for the Study of Crime Problems
National Academy of Law Sciences of Ukraine
61024, 49 Pushkinska Str., Kharkiv, Ukraine

Vasyl M. Stratonov

Doctor of Law, Professor
Professor of the Department of Industry Law
Kherson State University
73003, 27 Universytetska Str., Kherson, Ukraine

Iryna V. Savelieva

Doctor of Philosophy (Program Subject Area – 081 Law)
Associate Professor of the Department of Professional and Special Disciplines
Kherson Faculty of the Odesa State University of Internal Affairs
73034, 1 Fonvizin Str., Kherson, Ukraine

Suggested Citation: Konovalova, V.O., Stratonov, V.M., & Savelieva, I.V. (2021). Biometric personal data and their use in the investigation of criminal offences. *Journal of the National Academy of Legal Sciences of Ukraine,* 28(4), 289-300.

Submitted: 02.09.2021
Revised: 14.11.2021
Accepted: 03.12.2021