DOI 10.52468/2542-1514.2022.6(3).120-133

DIGITAL INNOVATION AND HUMAN RIGHTS: DILEMMAS IN INTERNATIONAL LAW ENFORCEMENT PRACTICE

Mikhail A. Mikhailov, Tatiana A. Kokodey
Sevastopol State University, Sevastopol, Russia

Article info
Received –
2022 February 14
Accepted –
2022 June 20
Available online –
2022 September 20

Keywords
Digitalization, information and communication trends, protection, personal data, digital technologies, international law enforcement practice, identification, biometric data

The subject of the study is the legal nature of personal data, as well as a set of legal norms governing relations in the field of their processing and circulation in the Russian Federation and foreign countries. The article uses a comparative method, a system analysis method, as well as a forecasting method.

The purpose of the article is to confirm or refute the hypotheses about the further strengthening of the contradictions between the emergence and implementation of new technologies for processing personal data versus ensuring the protection of human rights, as well as the expediency and possibility of using foreign legislative experience in domestic practice to counter these threats and reduce the risks arising from this and damage.

Main results, scope. The article examines the legislative experience of legal regulation of the types, scope, and nature of personal data in the People's Republic of China, the United States of America, the Republic of Belarus, and the Russian Federation. At the same time, Chinese legislation most quickly responds to the challenges of the criminal use of biometric technologies, American legal norms are less acceptable for our practice due to the peculiarities of case law, and Belarusian law has only recently entered into force, opening the era of legal regulation in this area. The facts of the use of new technologies (such as deepfake) for the processing of biometric information for criminal purposes and the problems of law enforcement in this area, as well as legal disputes of citizens who have suffered damage from the use of these technologies, are analyzed. It is predicted that it will be impossible to fully ensure the protection of human rights in the context of the emergence of new technologies for processing personal data. The importance of the desire to predict threats to the protection of personal information at the stage of emergence of new technologies for processing personal data in order to neutralize them in a timely manner is indicated.

Conclusion. An analysis of the legislation of foreign countries will make it possible to give preference to the Chinese experience, which promptly counteracts the risks of using new technologies for criminal purposes. An analysis of domestic and global law enforcement practice will make it possible to predict the spread of new ways of committing crimes, the misuse of personal data, and vulnerabilities in their storage and protection. At the same time, excessive restrictions on access to data, their processing and their circulation can make it difficult for law enforcement agencies to solve the tasks of ensuring state security and the protection of public order. It requires constant monitoring of threats and risks and timely technical and legal response to their manifestation. The purpose of the study has been achieved, ways to improve legislation in order to protect human rights in the context of the introduction of digital innovations in all spheres of human activity are proposed. Security, combating crime.

ISSN 2658-4050 (Online)

1.Introduction

Scientific and technological progress, which has affected all spheres of human activity, has become the cause of contradictions that a few years ago did not cause particular concern among society and the state. We are talking about the turnover of personal data of a person, their volume and nature, collection, storage, distribution and the need for protection in the context of the manifestation of digital innovative methods of their processing.

Modern technologies make it possible to generate, receive, store and process significant amounts of such information, thus tracking all the circumstances that make up the behavior and condition of a particular person, as well as analyze law-abiding and moral qualities, and predict further actions. With the development of the global Internet, such information has been uncontrolled and is at the disposal of intruders.

Thus, the noble goals of introducing these technologies have been discredited by the risks of violating the human right to privacy, which has slowed down their implementation. At the same time, countering crime, and above all such a dangerous manifestation of it as terrorism, does not allow ignoring effective digital tools for identifying and neutralizing criminals, minimizing the damage caused by them.

The problem of the contradiction of the spread of modern information and communication technologies with the requirements of human rights has recently become the object of attention of domestic authors, primarily from the field of information and constitutional law, as well as criminal, administrative and civil law. In particular, the authors E. V. Vinogradova, T. A. Polyakova and A. V. Minbaleev, M. Hildebrant, V. V. Blazheeva, A. K. Zharova consider the phenomenon of the digital profile and the legal regulation of relations in the field of digital profiling [1; 2, p. 55; 3; 4; 5]. The legal regulation of artificial intelligence in general is devoted to the works of V. B. Naumov and K. Y. Nikolskaya [6; 7; 8].

Certain aspects of the problem are also considered in the publications of specialists in criminal procedure and forensics. Thus, the legal and ethical aspects of the use of subject identification systems by electronic face recognition, as well as the aesthetic problems of fingerprint registration of the population were considered by one of the authors of this article [9; 10; 11]. In many ways, the global Covid-19 pandemic contributed to the aggravation of the problem under consideration [12-15].

The need for legislative regulation of the definition of the volume and nature of personal data, mechanisms for their protection during receipt, and processing and circulation, is implemented differently in some countries of the world, depending on the type of legal system, the level of development of information technology, and the efficiency of legislative response. The latter is especially important in the context of the emergence of new technologies related to face recognition, synthesis of voice, photo, and video images of appearance and so forth. For example, deepfake (translated from English. "deep learning" and "fake" [16; 17; 18; 19]. Another innovative biometric authentication technology is the combination of biometric modalities such as fingerprints and electroencephalograms [20; 21].

The legislative experience presented above is subject to careful study in order to take into account mistakes and successes and to prevent risks in domestic practice and predict their further development, while respecting the constitutional requirements for the protection of human rights.

2. Legal Regulation of Personal Data Protection in China

The beginning of 2022 put an end to the uncontrolled receipt of information from databases in China with actively emerging legislation on the protection of personal data, in connection with the entry into force of the Law of 1.11.2021. (Personal Information Protection Law) [22; 23; 24]. This law expanded the requirements of the previous law, focusing on the protection of information that allows personal identification of a citizen of China. As indicated in the Art. 1, the mission of the law is to "protect the rights and interests of individuals", "regulate the processing of personal data" and "ensure the reasonable use of personal

ISSN 2542-1514 (Print)

information". At the same time, the Legislation does not extend the law to residents of such regions as Hong Kong, Macau and Taiwan [25].

According to experts, the law will protect ordinary citizens, and optimize the regulation of the Internet economy, protecting the interests of Internet users by eliminating violations caused by the uncontrolled collection of personal information, including personal and biometric data of users.

For example, in recent years, facial recognition technology has been developing a lot, starting in private companies and for commercial purposes. Most companies managing real estate in China began to require owners and tenants of premises to undergo mandatory biometric scanning at the entrance to residential complexes. Then the ubiquity of this practice led to the fact that the first lawsuits appeared (for example, a certain Gou Bing became the first plaintiff in the China to bring a claim to the zoo for using facial recognition technology).2021 r

At the beginning of the Covid-19 pandemic, this technology was introduced in many public places to combat the illness. This reduced the burden on security, including the thermometry of customers. However, the main reason that caused the widespread use of personal identification technologies is the possibility of extracting super-profits by applying it, for targeted marketing impact on specific customers.

To that end, Chinese electric car maker XPeng Motors illegally collected 430,000 images of the faces of visitors to its stores over a period of six months, but it was subsequently forced to remove the database. The population also believes that such technologies should be used only by law enforcement agencies and special services, and not by private organizations.

These technologies are increasingly being developed in the world and disseminated in most countries. There is not only legal regulation of such activities for the private sector, but also state policy in this area.

At the moment, there is a need to establish a certain balance between the introduction of these technologies, which, of course, are useful especially in the areas of combating crime, protecting public order, state security, and measures to protect personal data, protecting human rights and freedoms. The problem has long grown from an ethical one to a legal one for most countries in the world.

China's response to this challenge was the Personal Information Protection Law. This was the first legislative act of the country which focuses on the systematization of measures to protect the personal information of citizens. It is verified in accordance with the principle of informed consent, that is, as a basic rule of protection of personal information, it gives citizens the right to know and the right to make decisions regarding their personal information.

With the comprehensive application of this Law, the Cyber Security Law and the Data Security Law, a comprehensive legal framework for information protection, compliance with corporate data requirements and the digital economy of China is being created.

Article 4 of the Law defines the concept of personal data as all types of information recorded by electronic or other means relating to identified or identifiable natural persons, without including information obtained after the processing of anonymized data.

The processing of personal data includes the collection, storage, use, processing, transfer, provision, disclosure, and deletion of personal information.

The law prohibits excessive collection of personal information (Art. 6) and price discrimination using large databases against customers. When marketing business to individuals through automated decision-making, processors of personal information must provide options that do not target personal characteristics, or offer methods of refusal.

When handling personal information, the principles of openness and transparency, disclosure of the rules for handling personal information and a clear indication of the purpose, method and scope of processing must be observed.

Art. 13 of the Law lists the conditions that allow the processing of personal information without the consent of the subject:

ISSN 2658-4050 (Online)

– When concluding and executing contracts in which an individual is an interested party, including labor contracts.

– If necessary, in order to fulfill statutory obligations and bring to justice for their violation;

– Respond to sudden public health threats as necessary or protect the life and health of individuals or the safety of their property in emergency conditions;

– The processing of personal information is allowed within reasonable limits for the presentation of news, observation of public opinion and other similar actions in the public interest;

– When processing personal information disclosed by the persons themselves or otherwise already disclosed legally, within reasonable limits in accordance with the provisions of this Law.

– As well as in circumstances provided for by other laws and by-laws.

The required consent of users must be obtained for the processing by online services of such personal information as biometric, medical data, health data, financial accounts and location.

The law also requires the suspension or termination of the provision of services for applications that illegally process personal data. With about one billion internet users in China today, there are more than four million websites and three million apps.

The law requires that Internet giants that possess the personal information of a large number of users create independent structures, mainly from external observers who control the processing of information.

As the Law is implemented, entrepreneurs, shareholders and investors of major Chinese technology companies should understand that the "golden era" of generating solid profits through invasion of user privacy and excessive data collection is a thing of the past. The use of personal data must comply with international standards.

In accordance with Art. 26 of the Law, the installation of equipment for the collection of images or identity recognition in public places must be carried out in accordance with the requirements of public safety and compliance with relevant state regulations, and clear signs indicating this must be installed. The personal images and personal identification information collected may only be used for the purpose of protecting public safety; they may not be used for other purposes, except in cases where the separate consent of individuals has been obtained.

This Law also introduces the concept of confidential personal data (Article 28). This is personal information that, in the event of leakage or illegal use, can cause harm to the honor and dignity of an individual, or significant harm to personal or property security, including information about biometric characteristics, religious beliefs, special status, health, financial accounts, individual location, and so forth, as well as personal information of minors under the age of 14. Only if there is a specific purpose and necessity, as well as subject to strict protection measures, it is allowed to process confidential personal data, for which it is necessary to obtain the separate consent of a natural person.

The introduction of the above legislative requirements at the beginning of 2022 led to contradictions between the development of innovative digital technologies in the country and legal restrictions on their use [26]. The Cyberspace Administration of China is currently considering the introduction of rules for the use of deep synthesis technology to protect the legitimate rights and interests of citizens in the country within the framework of the legal act "Regulation on the administration of deep synthesis of Information services of the Internet (Internet Information Service Deep Synthesis Management Provisions)" [27]. Deep synthesis is a typical application of artificial intelligence technology. In the past, this technology was known as "deep-fake" because it could be used to create non-existent video and audio content, which creates potential problems for policing, crime control, and national security. However, the technology in question also has many public benefits. Applications, in such areas as film and television production, assistance to patients with speech impairment might provide social benefits. We think that's why the neutral term "deep synthesis" is more acceptable.

Article 2 of the Regulations lists the areas of application of this technology:

ISSN 2542-1514 (Print)

1. Technologies for generating or editing text content (text generation, transformation of writing style, dialogues in the form of questions and answers);

2. Technologies for creating or editing voice content (text-to-speech, voice conversion and editing of voice characteristics);

3. Technologies for creating or editing non-vocal sound content (creating music and editing environmental sounds);

4. Technologies for creating or editing a person's face in images or videos (creating faces, replacing faces, editing appearance features, changing facial expressions and body movements);

5. Technologies for editing non-biological characteristics of images or videos (image enhancement and restoration);

6. Technologies for creating or editing virtual settings (transformation of two-dimensional models into three-dimensional ones).

In March 2021, the state regulatory authorities of China demanded that 11 influential Chinese Internet companies, including Tencent, Xiaomi and Kuaishou, strengthen the security assessment of voice software and new Internet technologies and applications using deepfake synthesis technology.

The latest unsafe manifestation of it was the application "Avatarify", which uses artificial intelligence that allows the user to replace their own faces with the faces of other people when creating photo and video products. According to media reports, the application became very common (viral) on “TikTok”, a service for viewing short videos in February 2021 and has already been downloaded more than 1.5 million times. However, at the request of the authorities on March 2, the application was removed from the Chinese Apple's app store due to concerns about invasion of privacy.

In March 2021, police in Zhengzhou, Central China, warned that the use of face-altering software carries with it certain security risks, such as leakage of personal information, and that such technologies are often used for criminal purposes, and videos created after that are often pornography. This is another reason for strengthening the protection of personal data in China.

Article 6 of the Regulation introduces a new concept of "portrait rights": no organization or individual can use the services of "Deep Synthesis" to participate in activities that violate the rights of other people to protection from misuse of their images, protection of reputation, privacy, portrait rights and other content protected by law.

Art. 9 instructs service providers of the Deep Synthesis technology to authenticate the real identification information of users of their service and prohibits the publication of this information.

Where a Deep Synthesis service provider offers features that include substantial processing of biometric information, such as a face and a human voice, the service user should obtain the subject's individual consent for the personal information being edited before editing the information. Except in cases provided for by law and administrative regulations.

Thus, the purpose of the document is to direct this technology on the path of healthy development, prevent risks and increase its positive role in technical terms.

3. Mechanisms for regulating relations in the field of personal data protection in the Republic of Belarus

The legislative consolidation of the regulation of personal data in the Republic of Belarus is implemented in the main provisions of the Law of the Republic of Belarus dated May 7, 2021 No. 99-Z "On the Protection of Personal Data", which entered into force on November 15, 2021 after its five-year development [28; 29]. Prior to the introduction of this law, Belarus remained one of the last countries in the world where there was practically no protection of personal data. Designed to facilitate the implementation by operators of the provisions of the above law, is a set of rights of individuals as subjects of personal data, allowing them to control and influence the processing of personal information.

As for the concept of personal data, the law provides for their broad interpretation, involving the inclusion of IP and email addresses of individuals. That is, according to Art. 1, personal data is any information relating to an identified natural person or an individual who can be identified. Additionally, this article introduces the following concepts:

ISSN 2658-4050 (Online)

- genetic personal data, which are information relating to the inherited or acquired genetic characteristics of a person, which contains unique data on his physiology or health and can be identified, in particular, in the study of his biological sample;

- special personal data – personal data relating to race or nationality, political opinions, membership in trade unions, religious or other beliefs, health or sexual life, administrative or criminal liability, as well as biometric and genetic personal data;

- processing of personal data - any action or set of actions performed with personal data, including collection, systematization, storage, modification, use, depersonalization, blocking, distribution, provision, or deletion of personal data;

The processing of personal data is regulated by Chapter 2 of this law. The processing of personal data is carried out with the consent of the subject of personal data, except for cases provided for by this Law and other legislative acts. In general, consent to the processing of personal data by law has three properties: awareness, freedom and specificity.

Art. 6 defines the conditions under which the processing of personal data can be carried out without the consent of a natural person, including consent to the processing of personal data (excluding special personal data) is not required:

- for the purposes of conducting administrative and (or) criminal proceedings, carrying out operational and investigative activities

- for the administration of justice, the execution of court decisions and other executive documents;

- for the purpose of exercising control (supervision) in accordance with legislative acts;

- in the implementation of the norms of legislation in the field of national security, the fight against corruption, the prevention of the legalization of proceeds from crime , the financing of terrorist activities and the financing of the proliferation of weapons of mass destruction

- to protect the life, health or other vital interests of the subject of personal data or other persons, if obtaining the consent of the subject of personal data is impossible, etc.

Art. 8 defines the procedure for the processing of special personal data, including the conditions under which the consent of a natural person is not required:

- when processing by public associations, political parties, trade unions, religious organizations of personal data of their founders (members) in order to achieve statutory goals, provided that these data are not subject to dissemination without the consent of the subject of personal data;

- for the purpose of organizing the provision of medical care, provided that such personal data are processed by a medical, pharmaceutical or other health care worker who is responsible for ensuring the protection of personal data and, in accordance with the law, is subject to the obligation to maintain medical confidentiality;

- for the administration of justice, the execution of court decisions and other executive documents, the execution of an executive inscription, the registration of inheritance rights;

- for the purposes of conducting administrative and (or) criminal proceedings, carrying out operational-search activities;

- In order to ensure the functioning of the unified State system of registration and registration of offenses;

- For the purpose of maintaining forensic records;

- In cases provided for by penal enforcement legislation, legislation in the field of national security, defense, combating corruption, combating terrorism and countering extremism, preventing the legalization of proceeds from crime, financing terrorist activities and financing the proliferation of weapons of mass destruction, etc.

In accordance with the considered law, (Chapter 4), an authorized body for the protection of the rights of personal data subjects (the National Center for personal data protection of the Republic of Belarus [30]) was also created, the main functions of which include: control over the processing of personal data by operators, consideration of complaints of personal data subjects on the processing of personal data; preparation of draft acts of legislation on personal data, etc.

ISSN 2542-1514 (Print)

4. Law Enforcement Practices in the Field of Personal Data Protection in the United States

s

The U.S. national legal system, which operates on the principles of the Anglo-Saxon legal family, does not provide for any federal legal acts for the protection of personal data, unlike most leading countries in the world. In case of violation of these rights, the practice of case law, as well as the provisions of the Constitution, are mainly applied.

The main legal acts in force in the field of personal data processing are the Privacy Act of 1974 and the Privacy Protection Act of 1980, which regulate the activities of public authorities in this area.

The Privacy Act of 1974 protects personal information in the possession of the Federal Government by preventing its unauthorized dissemination. Individuals also have the right to receive this information, as well as the right to be informed about their changes and such information is transferred to someone.

It is obvious that the above regulations, adopted about half a century ago, do not fully meet the requirements of the modern digital era and require a radical update.

In 2010, the NIST Special Publication Act 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) [31] came into force, the purpose of which was to legally regulate the activities of state bodies and federal agencies for the protection of personal data of citizens. However, this Law contains only general recommendations for the protection of personal data without detailing the mechanism for fulfilling its requirements, and definitions of basic concepts.

In the U.S., personal information refers to any information about an individual held by an agency, including (1) information that can be used to identify or spy on an individual, such as name, social security number, date and place of birth, mother's maiden name, or biometric parameters; and (2) any other information that is or may be associated with an individual, for example, medical, educational, financial and employment information.

This Law defines the principles for handling personal data, including:

- Restriction of the procedure for obtaining these data, that is, the use of only legal means for this, and, if necessary, obtaining the consent of the subject of personal data to collect such information.

- Personal data must correspond in content to the purposes for which they will be used. It is necessary that they are accurate, complete and constantly updated.

- Personal data should not be distributed, transferred to anyone specifically or otherwise used for purposes other than those stated, except with the consent of the data subject or by virtue of law, etc. This indicates that in the United States there is no unified mechanism regulating the processing and protection of personal data.

At the same time, the current legal norms contain mainly definitions of the relevant concepts and general recommendations, which are addressed mainly to state bodies. At the same time, there is no current control over personal data operators, and responsibility comes only after the leakage of confidential information. After identifying such cases, it is often possible to identify such cases. There are problems with the qualification of the crime. Thus, the personal information of individuals is very vulnerable.

For example, in March 2021, a resident of Pennsylvania, Raffaela Spone, was accused of using distorted images and videos created using Deepfake technology to discredit several members of the team of cheerleaders who competed with her daughter. On the falsified content, her daughter's rivals appeared to be drinkers and smokers of electronic cigarettes. The prosecutor qualified the actions only as cyberbullying, precisely because of the lack of a sufficient legal framework for the protection of personal data [32].

5. Comparative analysis of the legal regulation of personal data protection in the Russian Federation and foreign countries

When developing legislation on personal data, our country used the key principles of the leading countries of the world, taking into account the previously formed domestic approaches to ensuring information security. The Russian Federation in the field of personal data protection ratified the

ISSN 2658-4050 (Online)

Convention of the Council of Europe "On the Protection of Individuals with Regard to Automated Processing of Personal Data" (ETS No. 108, 1981), according to which, in order to: ensuring the protection of the rights and freedoms of a person and a citizen when processing his personal data, Federal Law No. 152 "On Personal Data" FL-152 of 27.07.2006 [33] was adopted. Subsequently, Federal Law No. 261 "On Amendments to the Federal Law "On Personal Data"" FL-261 of 25.07.2011 was adopted. Then Federal Law No. 519 "On Amendments to the Federal Law "On Personal Data"" was adopted again" FL-519 of 30.12.2020, at the same time, these latest amendments came into force on 1.03.2021, toughening responsibility for the leakage of personal data.

In this law (Part 1 of Article 3), personal data in a broad sense means "any information relating directly or indirectly to a specific or identifiable natural person (subject of personal data)";

At the same time, the processing of personal data is understood (clause 2 of Article 3) "any action (operation) or a set of actions (operations) performed with the use of automation tools or without the use of such means with personal data, including collection, recording, systematization, accumulation, storage, refinement (updating, modification), extraction, use, transfer (distribution, provision, access), depersonalization, blocking, deletion, nullification of personal data"..

Article 9 states that the subject of personal data decides on the provision of his personal data and consents to their processing freely, of his own free will and in his interest.

Art. 11 defines the procedure for the use of biometric personal data, which are understood as "information that characterizes the physiological and biological characteristics of a person, on the basis of which it is possible to establish his identity (biometric personal data) and which are used by the operator to establish the identity of the subject of personal data, can be processed only with the written consent of the subject of personal data." An exception, when the consent of the subject is not required, are the cases provided for in part 2 of Article 11: "in connection with the implementation of international treaties of the Russian Federation on readmission, in connection with the administration of justice and the execution of judicial acts, as well as in cases provided for by the legislation of the Russian Federation on defense, on security, on countering terrorism, on transport security, on combating corruption, on operational and search activities, on the civil service, the penal enforcement legislation of the Russian Federation, the legislation of the Russian Federation on the procedure for leaving the Russian Federation and entering the Russian Federation".

Comparing the approaches to the protection of personal data in Russia and the legislation of other countries discussed above, we can draw the following conclusions:

1. In the Russian Federation, there is a single mechanism that includes the powers of all participants: operators, subjects and state authorized bodies, while this mechanism is based on the condition of mandatory protection of personal data. Russian regulatory documents regulate specific measures to protect personal data and responsibility for their leakage. Practically similar is the Belarusian legislation in this area, which actually repeats the Russian regulatory framework. It can be noted that the legislation of both countries is of a preventive nature and is aimed at preventing violations.
2. In the United States, there is no single mechanism that would regulate the processing and protection of personal data, while the regulations are in the nature of general recommendations. Also, in the United States, the practice of case law is actively used, that is, the responsibility of operators comes only after the actual leakage of confidential information, which prevents the formation of an effective system for protecting the private information of citizens. This way of ensuring the protection of personal data radically different from the path of most European countries.
3. The Republic of Belarus is just beginning to feel the consequences of threats in the field of personal data protection and at the same time has its own vision to ensure the right to privacy. However, her experience as a newcomer in this field, only forming legislation, can also be useful for our country, given the proximity of our countries and the mentality of peoples.

ISSN 2542-1514 (Print)

4. The country with the most actively developing digital technologies and, in this regard, an equally rapidly emerging legislation on the protection of personal data is the People's Republic of China. At the same time, its first legislative and subordinate acts on the protection of personal data largely systematize general recommendations for the protection of personal information and rules for the use of innovative technologies for its collection and processing. This circumstance should be the reason for the close attention of the domestic legislator to the experience of this country, both in connection with the emergence of new threats caused by the development of scientific and technological progress, and with the successes of our neighbors in neutralizing and overcoming them.

6. Conclusion

This study is aimed at solving the urgent problem of ensuring adequate protection of personal data in the Russian Federation in the context of rapid digitalization of all spheres of society, without infringing on human rights to privacy.

Based on the analysis, it should be noted that the development of information and communication technologies inevitably leads to situations that threaten the implementation of human rights. Neither technical, nor legislative, nor ethical obstacles can completely eliminate this problem.

On the other hand, excessive restrictions on the receipt, storage and processing of these data by judicial and law enforcement agencies can significantly complicate the provision of state security, countering crime and such dangerous manifestations as terrorism, as well as protecting public order.

It is difficult to explain, difficult to control, and therefore ineffective requirements for obtaining consent from the subject to the processing of his personal data, in particular the image of the face, his voice, etc., which he voluntarily posts on the global Internet (in social networks, on video hosting, etc.).

As a few years ago with the advent of digital photography, we are on the verge of another qualitative leap in the development of technologies that allow us to change virtual images of a person, the audiogram of his voice and forge them for another specific person. This will inevitably lead to the emergence of new ways of committing offenses, the counteraction of which must be prepared now, both technically and legislatively.

Operational monitoring of law enforcement practice, both domestic and foreign, will allow, if not to minimize, then at least to reduce the damage from such manifestations. Studying the experience of legislators of foreign countries (primarily China) and its adaptation to domestic specifics will also contribute to solving these problems.

The main directions for improving domestic legislation in the field of personal data protection should be considered:

- mandatory adjustment of the volume and type of personal data requiring special protection;
- determination of the type of personal data, the processing of which is possible only with the consent of the subject;
- legal response to the emergence of new threats due to the emergence of previously unknown technologies (on the example of the global synthesis of biometric information of a person - deepfake);
- strengthening and differentiation of civil, administrative and criminal liability for improper protection of personal data, violation of human rights.

We hope that the topic of respect for human rights in the use of personal data processing technologies will be in the focus of constant attention of specialists in this field, scientists and practitioners, which will effectively counteract criminal manifestations in this area.

REFERENCES

1. Vinogradova E.V., Polyakova T.A., Minbaleev A.V. Digital profile: concept, regulation mechanisms and implementation problems. *Pravoprimenenie = Law Enforcement Review*, 2021, Vol. 5, no. 4, pp. 5–19. DOI: 10.52468/2542-1514.2021.5(4).5-19. (In Russ.).

2. Mochalov A.N. Digital profile: main risks for constitutional human rights in the face of legal uncertainty. *Lex russica*, 2021, vol. 74, no. 9 (178), pp. 88–101. DOI: 10.17803/1729-5920.2021.178.9.088-101. (In Russ.).

3. Blazheev V.V., Egorova M. A. (eds.). *Digital law*, Textbook. Moscow, Prospekt Publ., 2020. 640 p. (In Russ.).

4. Minbaleev A.V. (ed.). *Mechanisms and models of regulation of digital technologies*, Monograph. Moscow, Prospekt Publ., 2020. 264 p.

5. Talapina E.V. Protection of personal data in the digital age: Russian law in the European context. *Trudy Instituta gosudarstva i prava Rossiiskoi akademii nauk = Proceedings of the Institute of State and Law of the Russian Academy of Sciences*, 2018, vol. 13, no. 5, pp. 117–150. (In Russ.).

6. Zharova A.K. Issues of ensuring the security of a person's digital profile. *Yurist = Lawyer*, 2020, no. 3, pp. 55–61. (In Russ.).

7. Nikolskaia K., Naumov V. Artificial Intelligence in Law, in: *2020 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon)*, Vladivostok, 2020, pp. 1–4. DOI: 10.1109/FarEastCon50210.2020.9271095.

8. Nikolskaia K., Naumov V. Ethical and Legal Principles of Publishing Open Source Dual-Purpose Machine Learning Algorithms, in: *2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, Yaroslavl, 2020, pp. 56–58. DOI: 10.1109/ITQMIS51053. 2020.9322897.

9. Naumov V.B. (ed.). *Legal and ethical aspects related to the development and application of artificial intelligence systems and robotics: history, current state and development prospects*, Monograph. St. Petersburg, NP-Print Publ., 2020. 258 p. (In Russ.).

10. Volynsky A.F. On the issue of creating a unified state system for registering citizens: problems, ways to solve them. *Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia*, 2011, no. 9, pp. 56–58. (In Russ.).

11. Maksimov N.V. Legal issues of fingerprinting the civilian population, in: *Kazanskie ugolovno-protsessual'nye i kriminalisticheskie chteniya*, Materials of the International scientific-practical conference, Kazan, 2022, pp. 193–196. (In Russ.).

12. Bugaev K.V. Human rights and terms of storage of fingerprint information: Russian experience. *Uchenye zapiski Tavricheskogo natsional'nogo universiteta imeni V.I. Vernadskogo. Seriya: Yuridicheskie nauki = Scientific notes of the Taurida National University named after V.I. Vernadsky. Series: Legal Sciences*, 2008, vol. 21, no. 1 (60), pp. 211–216. (In Russ.).

13. Mikhailov M.A. Ethical problems of fingerprint registration of the population, in: *Sovershenstvovanie sistemy daktiloskopicheskoi registratsii*, a collection of materials of the International scientific and practical conferences (October 8, 2015), Moscow, Yurlitinform Publ., 2016, pp. 153–160. (In Russ.).

14. Mikhailov M.A. Biometrics: A new word in personal identification, in: Baev O.Ya. (ed.). *Voronezhskie kriminalisticheskie chteniya*, collection of scientific works, iss. ll, Voronezh, Voronezh State University Publ., 2009, pp. 267–280. (In Russ.).

15. Mikhailov M.A. Legal and ethical aspects of the distribution and use of human identification systems by electronic face recognition, in: Mikhailov M.A. (ed.). *Problemy polucheniya i ispol'zovaniya dokazatel'stvennoi i kriminalisticheski znachimoi informatsii*, materials of the International Scientific and Practical Conference, Simferopol, Arial Publ., 2019, pp. 79–82. (In Russ.).

16. Williams C.C., Kayaoglu A. The coronavirus pandemic and Europe's undeclared economy: impacts and a policy proposal. *South East European Journal of Economics and Business*, 2020, vol. 15, iss. 1, pp. 80–92. DOI: 10.2478/jeb-2020-0007.

17. Lungu E.V. Pandemic COVID-19. A new challenge to constitutional relations. *Pravoprimenenie = Law Enforcement Review*, 2020, vol. 4, no. 3, pp. 69–75. DOI: 10.24147/2542-1514.2020.4(3).69-75. (In Russ.).

18. Blazheev V.V., Egorov M.A. (eds.). *Legal regulation of artificial intelligence in a pandemic and infodemic*. Moscow, Prospekt Publ., 2020. 240 p. (In Russ.).

19. Egorova M.A., Minbaleev A.V., Kozhevina O.V., Duflo A. The main directions of legal regulation of the use of artificial intelligence in a pandemic. *Vestnik Sankt-Peterburgskogo gosudarstvennogo universiteta. Pravo = Bulle-*

ISSN 2542-1514 (Print)

tin of St. Petersburg University. Law, 2021, vol. 12, no. 2. pp. 250–262. DOI: 10.21638/spbu14.2021.201. (In Russ.).

20. Anisimov V.A., Sagitov A.M., Khusnutdinova E.K., Lutsenko V.I., Chemeris A.V., Aminev F.G. Genomic registration of the entire population and ethical issues of the formation and use of relevant databases, in: *Aktual'nye problemy sudebno-ekspertnoi deyatel'nosti v ugolovnom, grazhdanskom, arbitrazhnom protsesse i po delam ob administrativnykh pravonarusheniyakh*, Materials of the VII International Scientific and Practical Conference, November 9, 2018, Ufa, Bashkir State University Publ., 2018, pp. 16–22. (In Russ.).

21. Matveev Yu.N. Technologies for biometric identification of a person by voice and other modalities. *Vestnik Moskovskogo gosudarstvennogo tekhnicheskogo universiteta im. N.E. Baumana = Bulletin of Bauman Moscow State Technical University*, 2012, no. 3 (3), p. 5. DOI: 10.18698/2308-6033-2012-3-91. (In Russ.).

22. Westerlund M. The Emergence of Deepfake Technology: A Review. *Technology innovation management review*, 2019, vol. 9, iss. 11, pp. 39–52.

23. Fitzgerald A. Our Deepfake Future. *Virginia Quarterly Review*, 2020, vol. 96, no. 1, pp. 8–13.

24. Zendran M., Rusiecki A. Swapping Face Images with Generative Neural Networks for Deepfake Technology – Ex-perimental Study. *Procedia computer science*, 2021, vol. 192, pp. 834–843.

25. Qunjian Wu, Ying Zeng, Chi Zhang, Li Tong, Bin Yan. An EEG-Based Person Authentication System with Open-Set Capability Combining Eye Blinking Signals. *Sensors (Basel)*, 2018, vol. 18, iss. 2, art. 335. DOI: 10.3390/s18020335.

26. Hui-Ling Chan, Po-Chih Kuo, Chia-Yi Cheng, Yong-Sheng Chen. Challenges and Future Perspectives on Electroencephalogram-Based Biometrics in Person Recognition. *Frontiers in Neuroinformatics*, 2018, vol. 12, art. 66. DOI: 10.3389/fninf.2018.00066.

27. Ushmaev O.S. Biometric Iris Identification: Current State and Prospects, in: *Grafikon'2011*, 21st International Conference on Computer Graphics and Machine Vision, Moscow, MAKS Press Publ., 2011, pp. 192–194. (In Russ.).

28. Barsukov S.S. Forensic identification by the iris and retina: Modern possibilities and problems of application. *Yurist-Pravoved = Lawyer-Pravoved*, 2021, no. 1 (96), pp. 170–175. (In Russ.).

29. Eremenko Yu.I., Olyunina Yu.S. On the identification of users' keyboard handwriting. *Prospects for the development of information technologies*, 2016, no. 28, pp. 145–151. (In Russ.).

30. Uvarova A.V., Veshchev E.A. Identification by keyboard handwriting, in: *Integratsiya nauki i obrazovaniya*, Collection of articles based on the materials of the international scientific-practical conference, Irkutsk, Apeks publ., 2017, pp. 27–30. (In Russ.).

31. Razumov E.A. Digital dictatorship: features of the social credit system in China. *Trudy instituta istorii, arkheologii i etnografii DVO RAN = Proceedings of the Institute of History, Archeology and Ethnography of the Far Eastern Branch of the Russian Academy of Sciences*, 2019, no. 24, pp. 94–95. (In Russ.).

32. Pinkevich T.V., Nesterenko A.V. Violation of privacy when using big data technology. *Yuridicheskaya nauka i praktika: Vestnik Nizhegorodskoi akademii MVD Rossii = Legal Science and Practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 2019, no. 3 (47), pp. 143–147. (In Russ.).

INFORMATION ABOUT AUTHORS

Mikhail A. Mikhailov – PhD in Law, Associate Professor; Associate Professor, Department of Criminal Law and Procedure
Sevastopol State University
33, Universitetskaya ul., Sevastopol, 299011, Russia
E-mail: mmikh1@ya.ru
RSCI SPIN-code: 7307-3426; AuthorID: 189185

Tatiana A. Kokodey – Doctor of Economics, Associate Professor; Professor (Head), Department of Pedagogy and Psychology of Creative Development
Sevastopol State University
33, Universitetskaya ul., Sevastopol, 299011, Russia
E-mail: tanya.kokodey@gmail.com
RSCI SPIN-code: 4665-9541; AuthorID: 840438

BIBLIOGRAPHIC DESCRIPTION

Law Enforcement Review
2022, vol. 6, no. 3, pp. 120–133

ISSN 2658-4050 (Online)

Mikhailov M.A., Kokodey T.A. Digital innovation and human rights: dilemmas in international law enforcement practice. *Pravoprimenenie = Law Enforcement Review*, 2022, vol. 6, no. 3, pp. 120–133. DOI: 10.52468/2542-1514.2022.6(2).120-133. (In Russ.).