

Formation of common legal framework for biometric data security based on contradictions in international legislation

S S Sokolov, N B Glebov, A P Nyrkov, Z V Boriev

Admiral Makarov State University of Maritime and Inland Shipping, 5/7 Dvinskaya St., Saint-Petersburg, 198035, Russia

E-mail: sergiiblack@mail.ru

Abstract. The article analyzes the personal data security issue. The authors have given historical examples of personal data security in different countries of the world, as well as the classification of personal data types. The separate considered issue is the legal regulation of the biometric personal data protection, first of all, the issue of compliance of the Federal legislation of the Russian Federation with international treaties and conventions. Based on the analysis results, the authors provide recommendations on formation of the common legal framework for internal security of the international community.

1. Introduction

The technologies with use of biometric data are increasingly becoming a part of our everyday life year by year. This is due to the ever-growing threat of physical and cyber security. Biometric systems are used for the subject authentication by such static and dynamic parameters as a fingerprint, facial geometry, retina, handwriting, voice, etc. The listed parameters are an integral part of everyone, and when they are used in authentication systems, they become biometric personal data automatically.

The first normative document regulating the biometric personal data security is the Convention No. 108 "For the Protection of Individuals with regard to Automatic Processing of Personal Data" in 1981, accepted by the Council of Europe in Strasbourg. The purpose of this Convention is to secure in the territory of each country of the European Union for every individual, whatever his nationality or residence is, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him [1].

2. The regular focus on the personal data

A little bit later, most of the states that were part of the European Union adopted the Directive 95/46/EC of 24.10.1995 "On the Protection of Individuals With regard to the Processing of Personal Data and on the Free Movement of Such Data". The main subject of this document was also the provision on the protection of the fundamental rights and freedoms of individuals, and, in particular, their right to privacy with regard to automatic processing of personal data by EU member states. The second main item of the directive was the freedom of personal data handling between EU member states on the security-related grounds provided under the preceding item [2].

The regular focus on the personal data issue in view of the emergence of the need for their frequent use necessitated a division into two categories depending on the degree of sensitiveness - normal and special. Further, such division was accepted by many countries of the world and began to be used in



the national laws and regulations.

The reasons for consolidation of the special category in the personal data legislation are different. The list of information relating to this data type largely coincides with Art. 14 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (1950): race, religion, political and other beliefs, national origin [3]. At first, the main purpose of inclusion of such information into the sensitive personal data list was to provide citizens with supplementary guarantees from discrimination in the conditions of use of information technologies in the information processing. This was often caused by the negative experience of using such data for personal purposes in totalitarian states. With the information technology development, there is a partial rethinking of this information type. Except for the prohibition of impairment of rights on the basis of personal data, the information confidentiality, when an access to special data of third parties without the consent of the data subject is equivalent to a substantial violation of his rights, also assumes a greater importance.

3. Biometric technologies

The biometric data can be used for discrimination purposes even more easily. For example, the data contained in the DNA allow determining the liability of an individual to special diseases, which can be used for the purposes of employment, life and health insurance, etc. in the future. Such regulation is applied in the automated processing of the information about a person's race, and, regardless of the fact that the biometric technologies can be used in such situation, the processing of these data will also refer to the data security provisions relating to the special personal data category.

In this regard, the Russian Federation was one of the first countries which has introduced the separate biometric personal data definition into the legislation. According to the Federal Law of 27.07.2006 No. 152-FZ "On Personal Data", the personal data is divided into the following categories: normal, special and biometric [4]. The expediency of this procedure is determined by the biometric data specifics. If the data of insurance, place of residence or passport can be changed over time, then the authentication subject's fingerprints or a form of his external ear remain unchanged. There are two opinions on this issue in the European Union countries: someone considers that the security level of all personal data should be on the same level, while others insist on increase in the level of protection of citizens' rights in the biometric data processing field. The consequence of different ideas on the required biometric parameter protection degree was the disagreement in the legal regulation of such personal data protection.

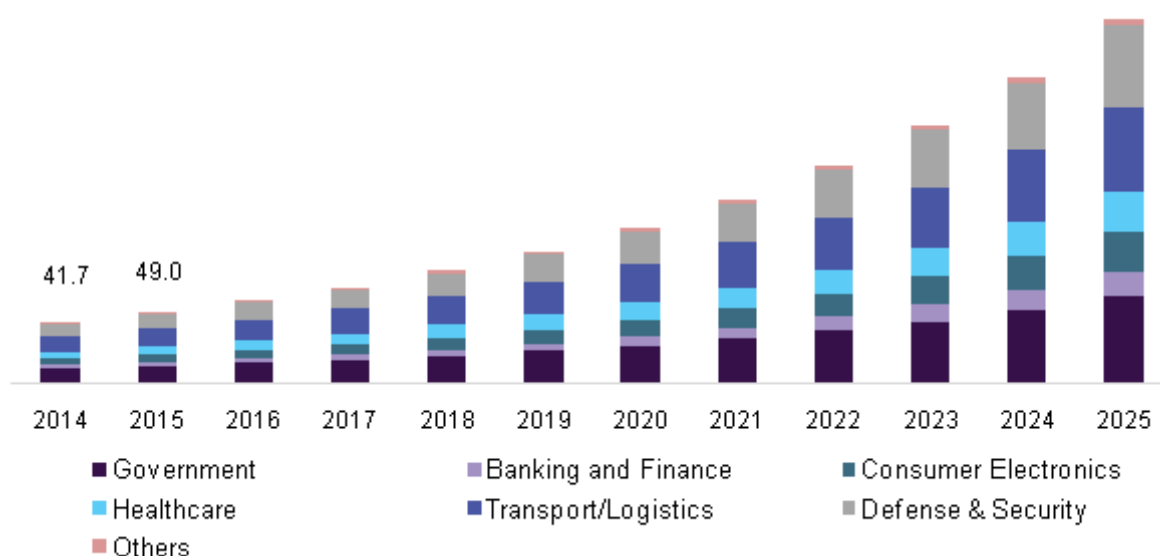


Figure 1. Development of biometric indicators.

Disagreements in the legal framework of regulation of the biometric data protection arise on the

ground of formation of the common internal security area of the international community. Different states have developed different ways for ensuring citizens' security by means of modern technical solutions and approaches, one of which was toughening of the requirements for identification means.

First of all, the development of the personal authentication direction touched upon the areas where the identification is a regular procedure. These areas include transport, customs and migration services. Decades of experience of these systems have shown that the information contained in the identity carriers is often subject to a forgery or falsification. Documents containing biometric information became the modern solution of this issue. One of such examples is a biometric passport.

Since 2002, the USA and some European countries have recognized facial biometrics as the basic identification technology for passports that was the beginning of wide use of biometric technologies. Since 2006, the Russian Federation has gone on the mass issuance of biometric foreign passports. Despite the general tendency of improvement in the biometric authentication processes, the issue of security of the transferred personality parameters was considered of secondary importance. By way of example, we will continue to examine this issue on the biometric passport.

The main difference between such passport and passport of the old sample is a contactless chip in a plastic cover, which is a microelectronic processor. A couple of years earlier, having a smartphone with a chip reader with a short-range wireless data transfer technology, it was possible to get a full name, photo and other information, which is contained in the passport, for a couple of minutes and absolutely free.

It is said in the Article 9 of the Federal Law "On the Procedure for Departure from the Russian Federation and Entry into the Russian Federation" that the biometric data of hands remain only on electronic media, and it is removed from the information systems of the organization, which has issued a document, upon receipt of the passport [5]. Unfortunately, such working conditions with biometric parameters place the information security of citizens' personal data under a threat [6]. There is an explicit threat of theft or forgery of personal data, including of biometric parameters, which almost do not change over time. In the engineering industry, biometrics processes have been widely used [9-12].

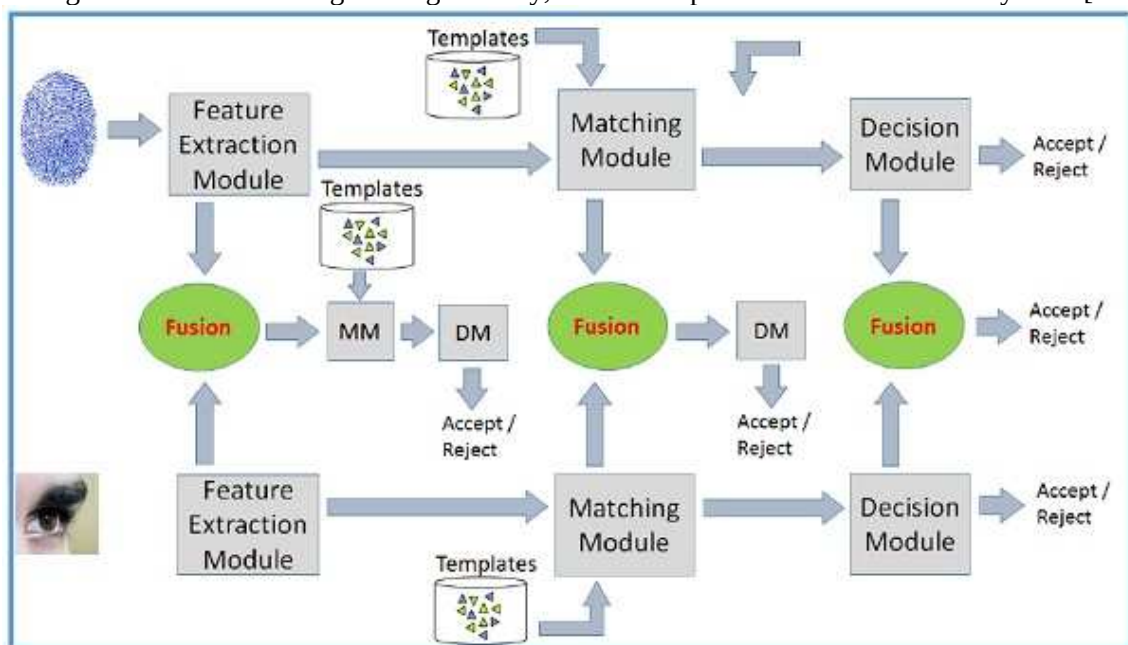


Figure 2. Algorithm of biometric indicators.

Analyzing the experience of Western specialists, it was found that, in order to avoid such situations, the International Civil Aviation Organization (ICAO) points out in its Convention on International Civil Aviation, part 1, volume 2, item 12.2 "On Machine Readable Travel Documents" [7] that if the issuing state decides to provide fingerprint data in their electronic passports, then the

fingerprint image storage is obligatory for ensuring global interoperability between classes. On the one hand, we have an example of solution of the problem of the source information protection against forgery. But there is an obvious legal conflict at the same time. Thanks to Article 15 of the Constitution of the Russian Federation, the norms adopted by ICAO are applied, since the international treaty of the Russian Federation establishes other rules different from the law of the Russian Federation [8].

It may be concluded that use of biometric technologies in the personal identification provides a high-grade personal data security, higher information processing rate and automatic identification of an owner's identity, provides information security that successfully contributes to the fight against illegal migration, transportation and unauthorized access [1,5,9,13]. Despite the introduction of these technologies by analogy with the western tendency, it should be noted that the Russian Federation uses this experience, projecting on its own features of legal regulation, territorial structure and ethnic composition. The achievements in organization of the visa regime in the Schengen area showed in real terms that the Russian Federation is ready to discuss and organize a single international legal framework. It is to be hoped that the current political confrontations won't affect cooperation in ensuring of the security of citizens and formation of the internal security space.

4. Conclusion

This article provides a clear illustration of the contradiction between normative legal acts regulating the same issues of the biometric data security. Collisions arise against the background of formation of the necessary common internal security space of the international community. Today, the world community needs to reduce the personal data types and standards for their processing to the general (international) classification, and also to explore the issue of the legal regulation of the biometric data security in more detail. The organization of such uniform environment is necessary for creation of the single standard for the legal regulation for use of biometric parameters that is very important against the intensively growing integration processes.

References

- [1] The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.01.1981, ConsultantPlus
- [2] The Directive No. 95/46/EC of the European Parliament and Council of the European Union (Adopted in Luxembourg, 24.10.1995)
- [3] The European Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 04.11.1950
- [4] On Personal Data: Federal Law No. 152-FZ of 27.07.2006 (as amended on 29.07.2017)
- [5] On the Procedure for Departure from the Russian Federation and Entry into the Russian Federation: Federal Law No. 114-FZ of 15.08.1996
- [6] Vasilyeva A A, Sutyagin S A, Polyakova E N, Moskvina V V 2016 The problems of citizens' personal data security when submitting electronic appeals to the government authorities *Bulletin of the Ural Federal District* **4(22)** 31-34
- [7] URL: <http://www.icao.int/Security/mrtd/>
- [8] The Constitution of the Russian Federation
- [9] Chernyi S and Zhilenkov A 2015 Modeling of complex structures for the ship's power complex using XILINX system. *Transport and Telecommunication* **16 (1)** 73–82
- [10] Chernyi S 2016 Use of Information Intelligent Components for the Analysis of Complex Processes of Marine Energy Systems. *Transport and Telecommunication Journal* **17 (3)** 202–211
- [11] Chernyi S 2016 Analysis of the energy reliability component for offshore drilling platforms within the Black Sea. *Neftyanoe Khozyaystvo - Oil Industry* **2** 106-110
- [12] Sokolov S, Zhilenkov A, Nyrkov A and Chernyi S 2017 The Use Robotics for Underwater Research Complex Objects *Advances in Intelligent Systems and Computing* 421-427

- [13] Horev, A.A., Bykov, A.I., Sokolov, A.N. Design and research of characteristics of the analog acoustic noise generator 2016 *2nd International Conference on Industrial Engineering; Applications and Manufacturing; ICIEAM 2016 – Proceedings* 7911563