Personal data protection in Kazakhstan and the EU: Comparative-legal analysis

by *Yernar Ye. Yerbolatov*[*], *Serik K. Zhetpisov*[**], *Aleksey V. Boretsky*[***], *Gulnar A. Alibayeva*[****], *Yuriy Yu. Kolesnikov*[*****]

Abstract

The rapid development of information technology, which penetrates all spheres of public life, has contributed to the emergence of new legal relations regarding personal information protection. In the conditions of the information society formation, the right to inviolability of person's private life acquires a special value. The purpose of the study is to analyze the issues of the personal data protection legal regulation in foreign countries and to develop scientifically based proposals for the improvement and systematization of the regulatory framework of the Republic of Kazakhstan, ensuring personal data confidentiality. The methodological basis of the research constitutes general scientific methods (in particular, philosophical, dialectical, synergetic, inductive, deductive, analysis, synthesis, formalization, analogy, materialistic and empirical methods) in order to ensure the integrity and balance of the research. The legislation of the CIS member states in the field of personal data is not developing as dynamically as in European countries. The regulatory provisions analysis showed that in the Republic of Kazakhstan a number of aspects stipulated by European legislation are not applied. Nowadays, in the legal regulation of the personal data circulation and protection, various problems need resolving in order to guarantee the right to the citizens' personal data protection. Improving and amending the legislation of the Republic of Kazakhstan in the field of personal data should place it on the leading states level.

[*] Department of Law - Faculty of Business, Education and Law – Innovative Eurasian – University – 140000, 45 Lomova Str., Pavlodar, Republic of Kazakhstan.
[**] Department of Law – Faculty of Business, Education and Law – Innovative Eurasian University – 140000, 45 Lomova Str., Pavlodar, Republic of Kazakhstan.
[***] Department of Law – Faculty of Business, Education and Law – Innovative Eurasian University – 140000, 45 Lomova Str., Pavlodar, Republic of Kazakhstan.
[****] Department of Constitutional, International and Customs Law – Eurasian Law Academy named after D. A. Kunaeva – 050000, 107 Kurmangazy Str., Almaty, Republic of Kazakhstan.
[*****] Department of Jurisprudence – Faculty of Economics and Law – Toraigyrov University – 140000, 65 Lomova Str., Pavlodar, Republic of Kazakhstan.

Rivista di Studi sulla Sostenibilità, (ISSN 2239-1959, ISSNe 2239-7221), 2022, 1

Doi: 10.3280/RISS2022-001005

Key words: personal information; confidential information; public figures; the right to privacy; protection of personal data.

First submission: 24 December 2021; *accepted*: 31 May 2022

1. Introduction

In the XX century with the advent of the computer, the penetration into all spheres of human activity, society and state information by computer technologies and telecommunication networks began. This process has two aspects. On the one hand, new technologies and means of communication allow to "compress" time and "reduce" distances and to economize the labor force. They also have political, technological and other advantages, regarding interests of the individual, groups of people, the country, regions and the world community. On the other hand, the problem of illegal actions involving the use of the means of electronic information environment (e-environment) is exacerbated. Activities concerning the databases formation, processing and dissemination of information about persons without their knowledge have led to the global problem of information security of the individual, the society and the state. The international cooperation in legal, economic, financial, banking, cultural and law enforcement spheres provides for the free movement of information on goods, capital and services, increases personal data flows and maintains the state sovereignity using information technologies and telecommunication networks. Therefore, these aspects determine the objective need to protect personal data.

Technological progress presupposes a wider range of needs and opportunities for the collection and processing of personal data. In its turn, personal data are increasingly used in a variety of areas, for example, in business and politics. Besides, their use is developing into a multifaceted activity. Thus, they can serve as a tool to violate human rights and freedoms, including the right to privacy. In this regard, the development of personal data protection is one of the most pressing challenges of the democratic society today. The personal data protection and its improvement are not only the responsibility of the state and the subject of state and legal regulations but also must be considered in connection with the protection of human rights and freedoms, including the right to respect for private life. In addition, the creation of an effective system of personal data protection is one of the international obligations related to the European integration of Kazakhstan. In addition to the legal instruments governing such a system, its effectiveness

is now ensured by the highly professional activities of authorized bodies, which have already achieved a significant success in implementing the international and European standards of personal data protection. However, another important factor is the level of awareness of citizens and public actors about the ways and possibilities of using these tools.

Many academic works by such scholars as Bachilo (2019), Abdullin (2017), Lozovaya (2015), Byrum (2017), Shevchuk (2018) are dedicated to the problems of practical application of ECtHR decisions in the law enforcement. The purpose of this study is to compare the legal regulations of personal data protection in foreign countries and develop scientifically substantiated proposals for the development, improvement and amendment to the legislation of the Republic of Kazakhstan, regarding personal data confidentiality. The scientific novelty of the obtained results is that this paper presents a comprehensive study of the constitutional protection of personal information in a comparative legal aspect. A number of conceptual concepts, theoretical positions and conclusions are substantiated for carrying out the comparative legal analysis of personal data protection in the European Union and in Kazakhstan.

2. Materials and methods

The methodological basis of this study is a scope of techniques and methods of scientific knowledge. It is aimed to ensure the integrity and balance of the research using general scientific methods (philosophical, dialectical, synergetic, inductive, deductive, analysis, synthesis, formalization, analogy, materialistic and empirical methods) as well as to render a rigorous analysis of the personal data protection system in foreign countries and Kazakhstan. The use of a general scientific dialectical method helped to analyze the issue of personal information legal protection, considering its interdependence, integrity, comprehensiveness and dynamics. The subject of the study implied the use of the following methods. A comparative analysis was used in order to compare the legal regulations of personal information protection and their application in European countries and Kazakhstan. Structural and functional methods served to identify and study factors that affect the personal information protection. A historical method was applied to analyze the history of the right to privacy (in particular, in the field of information protection), its normative consolidation and the history of the development of the legislation on personal information legal protection in the European Union and

Kazakhstan. A systemic method was used in order to consider personal information in combination with other legal phenomena related to its protection, especially from the standpoint of balancing the right to privacy and freedom of expression. A formal-logical method helped define the concepts of personal data; formal and legal as well as interprete the current legislation and case law of the European Union and Kazakhstan.

In order to clarify the historical development of the personal data protection institution, a historical method was applied. A systemic method is used to apreciate a specific object as part of a system consisting of interconnected elements. However, a structural-functional method consists of the interpretation of the society as a social system that has its own structure and the mechanisms of interaction of its structural elements performing their own individual functions. Using the systemic and structural-functional methods, the main mechanisms for protecting personal data in the European Union and Kazakhstan were determined. The important place in the research methods system was occupied by the method of legal analysis of normative legal acts of international and European institutions in order to improve the existing personal data protection system in the Republic of Kazakhstan. In the course of the study, the following sources were analyzed: The Constitution of the Republic of Kazakhstan, international legal acts, constitutional, administrative, civil, criminal legislation, by-laws, and other legal and technical material of the CIS and EU countries.

3. Results

The society has become increasingly digital. In light of these changes, on a daily basis everyone is affected in different ways by the pace of technological development and the ways of personal data processing. Effective personal data protection in the EU (European Union) is ensured through a comprehensive mechanism consisting of the following elements:

pan-European regulations, national legislation governing personal data protection and the limits of their protection, which determine the conditions for the transfer of personal data to third countries;

basic principles of law on personal data protection with legal clarity;

European advisory and supervisory bodies for personal data protection;

special legal status, fundamental rights, freedoms and responsibilities of data subjects, controllers, operators and third parties (Avramenko, 2019).

The EU's reforms in the field of personal data protection are large-scale and complex. They have a significant impact on individuals and business

giving them many benefits. Nowadays, among the most important legal documents of the European Union on legal circulation and personal data protection, the following ones can be singled out:

Convention for the Protection of Individuals with Respect to Automatic Processing of Personal Data (Convention 108), which is one of the few international treaties that enshrines a person's right to privacy of personal information that is binding on its signatories (Council of Europe, 1981).

Directive 95/46/EC "On the protection of the rights of individuals with regard to the processing of personal data and on the free circulation of such data", which laid the foundations for a pan-European system for the protection of personal data (European Parliament, 1995).

Regulation No. 45/2001 "On the protection of individuals in the processing of personal data carried out by institutions and bodies of the Union and on the free circulation of such data", according to which institutions and public authorities should preserve the protection of citizens' fundamental rights and freedoms and most importantly the right to privacy of personal data (European Parliament, 2000).

Directive 2002/58/EC concerning the processing of personal data and the protection of confidentiality in the electronic communication sector (European Parliament, 2002).

Regulation (EU) 2016/679 "On the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)" (European Parliament, 2016).

Throughout the entire period of the European Union existence, its legislation has been formed in relation to the circulation and protection of personal data. Legal regulation of the circulation of personal data and their protection in the rapidly developing digital environment requires regular improvement and harmonization. Each of the adopted documents has its own characteristics that respond to the challenges, risks and threats that have taken place. Various reasons of social, economic, political, technological nature have become the basis for their development and adoption. Such a thorough legal regulation of the issue under consideration gives grounds to assert that in the conditions of modern global information space, personal data protection is one of the basic human needs (Reding, 2011).

Directive 95/46/EC of the European Parliament and the Council on the protection of individuals in the processing of personal data and on the free movement of such data "enshrined eight basic principles of personal data protection, according to which data controllers must act". The Directive anal-

ysis shows that these basic principles are the following: the principle of persocentrism (the system of personal data protection is formed primarily for human service), the principle of extraterritoriality (personal data owners (controllers) regardless of the individuals' nationality or place of residence must respect their fundamental rights and freedoms); subsidiarity principle for the rights and freedoms of data subjects (Bu-Pasha, 2017).

The document also sets out a mechanism to link the right to protection of personal data with the right to privacy. The level of individuals' rights and freedoms protection with regard to the processing of such data must be the same in all Member States in order to eliminate obstacles to the personal data transfer. Moreover, particular attention is paid to the principles of personal data processing (legality, clarity, fairness, and accessibility). Data protection of individuals should be applied to both automated and manual data processing; and the extent of such protection should not depend on the methods used. Derogating from the ban on the processing of confidential data categories may be justified by the public interest in such areas as public healthcare, social protection, research and government statistics (Brązkiewicz, 2019).

In addition to universal international treaties, the relevant norms are contained in regional international treaties in the field of human rights protection. Thus, the provisions on the protection of the right to privacy are embraced in Art. 7 of the Charter of Fundamental Rights of the European Union (European Parliament, 2012). Art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms of 1950 states: "Everyone has the right to respect for his private and family life, his home and his correspondence" (Council of Europe, 1950). This document became the source of the personal data protection system. It should be noted that the Charter of Fundamental Rights (Charter) enshrines not only the right to protection of personal data of a person and a citizen but also regulates the support of values and principles related to this right. This document preserves the need for honesty in the personal data processing and the implementation of this process with the person's consent and only on legal grounds established by the applicable law. In addition, all subjects should be given the right to correct errors in their personal data. These principles must be upheld by the competent authority. Individuals should also have the right to access their data (Gonzalez, 2016).

All necessary measures to ensure the right to respect for private life and personal data protection of the citizen must be taken by the state. The right to protection of personal data may be applied to any transaction related to personal data processing and will be subject to the rules on protection. When an employer enters data on the employees' names and salaries, there is no

violation of their right to personal data protection. At the same time, if the employer transfers the employees' personal data to third parties, it falls under the scope of the relulation on the right to protection of personal data. Recording information about employees is considered personal data processing, so employers must follow the rules of personal data protection (Hoofnagle, 2019).

In order to create an effective mechanism for monitoring the activities of national institutions, the independent institute of the European Data Protection Officer was established in 2000. It was established in accordance with Article 41 of Regulation 45/2001 of the European Parliament (2000) and the Council of 18 December 2000 on the protection of the rights of individuals with regard to the processing of personal data by EU bodies and institutions and on the free movement of such data.

This institution functions are similar to those of an ombudsman, but it is specialized in personal data protection. The appointment to this position is based on the results of a candidates' public competition. The main criterion of the European Data Protection Officer's activity is its independence from other EU institutions, which is ensured by a special mechanism laid down in the Regulation. Its main task is to ensure the respect for the right to privacy and personal data protection by all federal bodies and institutions, providing advisory clarifications on its own initiative and at the request of interested bodies. It is also important to hightlight that, according to Article 24 of Regulation (EC) 45/2001, along with the position of the Commissioner each EU body appoints at least one person as an officer (hereinafter – the Officer) for personal data protection. The officer must serve a term of two to five years (Custers et al., 2018).

The EU General Data Protection Regulation (GDPR), developed and adopted back in 2016, came into force on May 25, 2018 (European Parliament, 2016). Improving the principles laid down in previous documents on the protection of personal data and privacy, it aims to strengthen the most important individual rights in the digital age. In addition, it eliminates the fragmentation of the EU Member States legislation, unifying it and removing administrative barriers. The key importance is given to the issue of cross-border data exchange in order to strengthen the control over confidentiality and introduce the international standards of personal data protection.

It is noteworthy that with a view to protect the effectiveness of principles, the Regulation also provides for technical aspects of personal data protection. In particular, the Regulation controls the mandatory use of such procedures as anonymization, pseudonymization and data encryption by data processing organizations. The anonymization implies removing personal identifiers

from data arrays, while the pseudonymization is the replacement of personal data identifiers with identifiers. The use of such procedures obliges the controller to consider the processing purposes, the risks of threats to the rights and freedoms of individuals, the processing volume and nature as well as the implementation cost. However, the Regulation does not specify what risks are significant, what processing purposes and tasks should be taken into account, etc. It is advisable for the controller or the processor association to develop codes of conduct approved by the appropriate supervisory authority. They will allow to independently regulate their activities, even considering the control of the authorized bodies. These documents are especially important when transmitting personal data to a third country or an international organization, which should involve an additional guarantee of their protection (Granger & Irion, 2018).

European law sets strict limits on the collection and the use of personal data and requires each EU country to establish a national independent body to protect such data. For example, in France, the National Commission for Informatics and Freedoms is such an independent administrative authority. Its independence is ensured by its formation conditions (from various bodies and the civil society), the term of office (5 years), the prohibition of conflicts of interest, and the lack of prior financial control over the commission costs (such costs are controlled only by the Accounting Chamber) (Dei et al., 2020).

Furthermore, sensitive personal data also includes certain information related to the relationships between the employer and the employee. The European Community pays considerable attention to this issue. Thus, in the interests of information security the German government established a federal agency for security in the field of information technology in 1993. The competence of this department includes the technical information protection, consultations of citizens on technical information protection and security equipment certification and standardization. In addition, this agency encourages the protection of business information.

It is also worth noting that in the labor legislation of France and Italy, the concept of employee's personal data is defined as information required by the employer related to a particular employee and his professional qualifications and professional qualities. This information also applies to the requirements that may be imposed on the employee due to the nature of the work. In this case, the French law of December 31, 1992 on the protection of personal dignity of the employee during employment and during the employment contract gives the employer the right to request information when hiring solely to determine the employee's professional qualifications. It should

not concern his moral account, the nature and peculiarities of his personal and family life (Guiwan, 2019).

Some countries, while not prohibiting or preventing the collection of employee's data from third-party sources, restrict this data processing by the employer. For example, in Austria there is a guaranteed right to receive information about the employee from his former employer. This is explained by the fact that the so-called certificate of employment must relate to the employment duration and the services type. Besides, any statement or phrase that hinder the employee's future career is prohibited. In particular, the information may not be provided to the next employer if it concerns the reason for the employee's dismissal, negative assessment of his work or his engagement in activities provided by a member of the works council or a labor union. The same applies to oral communications of (former) employers. A similar legal situation exists in Belgium.

In some European countries, special regulations were adopted in the field of employees' personal data protection. For example, in Poland there is a Regulation on general data protection, which entered into force on May 25, 2018. It regulates, inter alia, the collection and processing of employee's personal data, including biometric data. According to this Regulation, the employer has the right to request a list of certain personal data from candidates/employees. It is important to underline that the employer also has the right to collect other work-related data if the employee gives his consent and the processing of such data is in his interests. At the same time, the Regulation also sets restrictions on video surveillance of employees at the workplace, as well as special requirements for the personal data storage. Thus, video surveillance will be possible if it is necessary to ensure the safety of workers, protect property, control production or preserve confidential information. Each employer is obliged to indicate the goals, scope and method of monitoring the employee's personal data in the collective or employment agreement or work instructions (Kutsin, 2018).

In Croatia and the Czech Republic, employers have to inform their employees about the e-mail observation and monitoring. In other countries, such as Bulgaria and Poland, this is not required by law, but, in practice, employers include relevant conditions and rules in the work instructions or the collective agreement in order to implement a transparency policy. Employees also receive information on possible monitoring of their emails and internet access. In particular, the employer determines the following issues: whether it is possible for employees to use private e-mails during working hours; terms and conditions of e-mail for private purposes; the procedure for opening an employee's e-mail in case of his long absence; whether the employees

can access the Internet during working hours; and technical and organizational measures to protect personal data.

Thus, it is common in many European countries for an employer, as the owner of a computer system, to obtain the right to monitor an employee's e-mails. However, such monitoring may only be carried out with the employee's knowledge. At the same time, in almost all European countries there is a special institution, whose functions include monitoring of the compliance with procedures of personal data protection. For example, in the Czech Republic it is the Office for Personal Data Protection, in Croatia this role is performed by the Agency for Personal Data Protection, in Bulgaria it is withing the competence of the Commission for Personal Data Protection. The most characteristic prerogatives of these institutions are to supervise personal data protection, detect violations during the personal data collection and the application of sanctions, monitor the legislation on personal data protection, consider and resolve complaints, etc. (Martinez, 2018).

It has already been pointed out that the European Union legislation developed and effectively applies legal mechanisms to mediate the processing and protection of certain personal data categories. Therefore, much attention is paid to the sensitive personal information protection, for example, in the law enforcement activities. It can be illustrated by the Recommendation No. R (87) 15 of the Committee of Ministers of the Council of Europe (1987), which regulates the use of personal data in the police. According to this document, data processing activities "for police purposes" mean all the problems that can be solved by the police in order to prevent or stop criminal offenses and establish public order. The basic principles of this Recommendation are based on the data processing solely for legitimate purposes. Consequently, it should be limited to the extent necessary to avert a real danger or to put an end to a criminal offense.

Any exception to this provision should be subject to the special national legislation. If a person's data were collected and stored without his or her knowledge and if data were not destroyed, he or she should be informed that information about him or her is being kept. Data collection by technical or other automated means may be carried out only in accordance with the personal consent. Moreover, the personal data collection only on the grounds of a certain racial origin, religious beliefs, sexual behavior, political views or belonging to movements or organizations that are not outlawed should be prohibited. The data collection concerning these issues may be realized only in case of an exceptional need to achieve the maximum legality and openness of a specific investigation (Tikkinen-Piri et al., 2018).

The transition to the information society in the Republic of Kazakhstan took place at the end of the 20th century when almost all spheres of life were reformed. By the beginning of the twenty-first century, the information revolution affected almost all aspects of social reality, including the economic, socio-political, cultural and spiritual development of the society. Information and communication technologies also penetrated into management activities. The relatively recent legislation of the Republic of Kazakhstan consolidated the provisions on personal data protection. At the same time, the state has not accumulated a lot of law enforcement experience in this area, unlike most democratic states. Today, the Republic of Kazakhstan passed a natural stage of development determined by the "information society".

In the Republic of Kazakhstan, the collection, processing and protection of personal data is regulated by the Law "On Personal Data and Protection" (Parliament of the Republic of Kazakhstan, 2013). Peculiarities of this process may be regulated not only by Article 3 of this Law but also by other laws and the acts of the President of the Republic of Kazakhstan. The laws governing personal data include the following ones: the Code of the Republic of Kazakhstan of July 7, 2020 No. 360-VI "On human health and the health care system" (Parliament of the Republic of Kazakhstan, 2020); Labor Code of the Republic of Kazakhstan dated November 23, 2015 No. 414-V (Parliament of the Republic of Kazakhstan, 2015).

A special procedure for processing personal data is provided by the legislation of the Republic of Kazakhstan to ensure their protection. There is a unique legal regime of processing by special authorized bodies that have the appropriate competency under the current legislation. It includes obligations of subjects, the principles and conditions of this processing, control measures and responsibility for violations of the legislation. In addition, the protection of all individuals' personal data included in electronic databases are enshrined in the Resolution of the Government of the Republic of Kazakhstan (Alyamkin, 2016).

Apart from that, it is prohibited for owners and operators of mobile communication companies to dissemine personal data without legal grounds or consent of the subject or its legal representative, in accordance with the current Law of the Republic of Kazakhstan "On personal data and their protection" (clause 1 of Article 11 of the Law "On personal data and their protection"). This norm can be regarded an important part of the integral mechanism for protecting personal data. After all, the violation of personal data confidentiality by the owner and operator can cause significant moral or material damage to an individual. Therefore, the level of personal confidence in information resources largely depends on how effectively the personal data

confidentiality is ensured during their collection, storage and use and contributes to their involvement in the informatization (Shevchuk, 2018).

The depersonalization procedure is an important factor in guaranteeing the personal data security. The current legislation of the Republic of Kazakhstan enshrines the provisions on the personal data depersonalization used for statistical, sociological or scientific research by operators or state-authorized bodies. The legislation also regulates the termination of the obligations of the owner, the operator and the third party to protect personal data from the moment of their depersonalization. That is, if personal data was anonymized, the legal confidentiality regime in relation to them ceases to apply, since it becomes impossible to identify personal data and their holder (Bachilo, 2019).

The analysis of the national legislation of the Republic of Kazakhstan reveals an important aspect of the mechanism for ensuring the personal data confidentiality that needs improvement. Despite the fact that the Law of the Republic of Kazakhstan "On personal data and their protection" stipulates that restricted personal data is confidential, the procedure for ensuring confidentiality is regulated superficially. However, it is worth mentioning that in solving this issue, the experience of the EU countries is remarkable. For example, the legislative acts on personal data protection in Sweden do not contain a specific regulatory indication of the personal data confidentiality. Despite this, the procedure for ensuring their security is very carefully detailed. The Swedish legislation provides special criteria for technical and organizational measures to protect personal data during their processing. These measures are aimed at maintaining the required personal data security level, considering the available technical facilities, the relevant measures costs, special risks associated with personal data processing, and the processed data sensitivity degree (Abdullin, 2017).

The requirements in the field of information security and information and communication technologies were adopted in accordance with the decree of the Government of the Republic of Kazakhstan in 2016. They are mandatory for state bodies, local executive bodies, state legal entities, quasi-public sector entities, owners of private information systems integrated with the state information systems or intended for the formation of state electronic information resources and owners of critical information and communication infrastructure facilities (Telina, 2016).

It is necessary to add that in many European countries, such issues are regulated by legislation. The importance of ensuring personal data protection, it is considered expedient to implement the organizational and technical regulation by law. Having analyzed the legislation that governs operational-

search activities in Kazakhstan, significant shortcomings that result in violation of the human right to personal data protection can be identified. First of all, this concerns the access to information and its storage, which is collected during operational search activities (Zhatkanbaeva, 2009).

Clause 3 of Art. 5 of the Law of the Republic of Kazakhstan "On operational-search activity", establishes that "a person whose guilt in the preparation or commission of a crime has not been proven, has the right to demand from the body carrying out operational-search activity the information that served as the basis for its verification and the nature of the available information regarding him" (Parliament of the Republic of Kazakhstan, 1994).

This provision was somewhat concretized with the introduction of the "right to informational self-determination" by the Federal Constitutional Court in 1983, which could be limited to a dominant public interest. It implies that the state or by third parties can conduct an operational-search activity without notifying the individuals whose personal data were used. However, such interference should not violate the principle of proportionality, that is, it should not be longer in duration than determined by the legislator and also not be used for a purpose other than that provided by the law. In accordance with the provisions of the German Federal Data Protection Act, the right of the data holder to access his personal information may be limited if this could harm public safety and order (para. 4 §19). Besides, the French law "On Informatics, Card Index and Freedom" establishes restrictions on a person's access to personal data if they are of interest for the state security, national defense, and public order. Moreover, free access to administrative documents containing information not of personal nature but affecting an individual's interests also allows for the exceptions to the general rules (Article 19) (Lozovaya, 2015).

Finally, the Law of the Republic of Kazakhstan "On Personal Data and Their Protection" establishes general requirements for the personal data protection, but they require more considerable control by the state. The downside of these requirements implementation is the fact that in this area many issues are not regulated by law at all. Currently in the Republic of Kazakhstan, there is no legislation body on the circulation and protection of personal data. However, it is at the initial stage of its development and should be similar to the European countries' personal data protection agency. It will deal with the issue of creating a register of all personal data operators in Kazakhstan, monitoring the information systems owners and the state of personal data protection.

4. Discussion

The lack of an authorized body in the field of personal data protection of the Republic citizens is a significant problem, but it is being resolved. Deputy Chairman of the Committee on Information Security of the Ministry of Digital Development, Defense and Aerospace Industry said that "A prototype of the Data Protection Agency will appear in Kazakhstan being the only center responsible for the security of Kazakhstan citizens' personal data. The personal data collection and processing is entrusted to the state bodies where these processes take place, until a new authorized body is established" (Yurchenko, 2016).

In this study, special attention is drawn to the progressive nature of the European experience in the personal data legal regulation. While creating the authorized body in the field of personal data, this experience is worth borrowing. Its peculiarity is that the authorized bodies of the European Union and the supervisory authorities for data protection of the Member States are endowed with an independent status. Accordingly, in the Republic of Kazakhstan, the created authorized body should be independent, not accountable to any ministry and endowed with necessary functional powers and material resources. The status of the independent body will make it possible to identify violations at all levels of public authorities, in quasi-public and private sectors (Khuzhina, 2015).

The amendments to the conceptual and terminological framework of the Law of the Republic of Kazakhstan "On personal data and their protection" require special attention from public authorities. The extension of terminology should include the disclosure of all actions related to personal data protection. Moreover, such important aspects of personal data as their modification and addition also remained unresolved. The importance of the definition of these terms to provide their unambiguous understanding and additional guarantees of compliance with the rule of law in the law enforcement practice, it should be considered appropriate to supplement Article 1 of the Law of the Republic of Kazakhstan "On Personal Data and Their Protection" with the following definitions: "Changes in personal data are actions aimed to correct and clarify personal data contained in the database. Supplementing personal data is actions aimed to enter new personal data that were not previously introduced into the database" (Byrum, 2017).

When reforming the legislation of the Republic of Kazakhstan in the field of personal data protection, another important factor within the European Regulation on Personal Data Protection is General Data Protection Regulation (GDPR). Apart from that, the introduction of "confidential personal data" in domestic law is also worth paying attention to. The "sensitivity"

criterion is very valuable in identifying personal data. Consequently, increased security measures are required when establishing guarantees for data processing and choosing an appropriate legal and practical mechanism for regulating and protecting personal data (Radkevich, 2014).

An important step in shaping legislation on personal data protection is reforming the EU legislation. After all, current European legislation forms a large set of legal norms on personal data protection. It is necessary to take into consideration this reform results in the sphere of personal data circulation and protection in such integration organizations as the Commonwealth of Independent States and the Eurasian Economic Union. European law principles and standards have become fundamental in the law formation in other non-European countries. Accordingly, the EU norms are not only universal but they also analyze the accumulated European practical experience in applying the principles enshrined in current international instruments. Today, many countries are borrowing the European experience in this area and trying to implement it into national law. Thus, this practice should also be introduced by the Republic of Kazakhstan to ensure personal data protection in the state and international cooperation.

The legislation of the CIS member states on personal data protection is not developing as dynamically as in European countries. In addition, it does not detail many procedures as it is done in European legal documents. Thus, the regulatory provisions analysis showed, a number of aspects embraced by European legislation are not applied in the Republic of Kazakhstan. For instance, there is no right to be forgotten and to data portability. The improvement of the legislation of the Republic of Kazakhstan on personal data should placed on the leading states legislation level. If the state pretends to be integrated into the global information space, it must be ready to ensure the maximum protection level for its citizens, especially in such an important area as personal data protection.

Personal data protection in the Republic of Kazakhstan is preserved in the current legislation. It enshrines the rights and obligations of the subjects of these legal relations and provides the mechanism for regulating the use of personal data and liability for violation of an individual's right to confidentiality. The need for international legal regulation of personal data protection should be rejected. The Republic of Kazakhstan should organize its own legislation in accordance with the norms and principles of the European Union law.

Finally, the development of personal data protection legal regulation in the Republic of Kazakhstan lags behind European realities, according to the analysis of the current national legislation. Nevertheless, the personal data

protection level through the implementation of the best practices is improving. For example, Kazakhstan and the European Union signed the Enlarged Partnership and Cooperation Agreement in 2015, which prescribes the parties to ensure high personal data management requirements.

5. Conclusions

The globalization, informatization and new technologies development require new understanding of the problems of protecting human rights and freedoms, achieving a balance of the interests of the individual, the society and the state, and modernizing the legal framework. The current state of legal regulation on personal data circulation and protection in the Republic of Kazakhstan has need for its harmonization with the international standards by adopting appropriate amendments and additions to the national legislation. At the same time, it is important to take into account the progressive international and European experience in personal data protection. The legislation on personal data circulation and protection has been of considerable importance throughout the European Union's existence. However, in the rapidly evolving digital environment, the legal regulation of personal data circulation and protection needs to be regularly improved and harmonized. Each adopted document has its own characteristics, which respond to the challenges, risks and threats that have occurred Apart from that, it contains the basis for the legislation development due to various reasons of social, economic, political and technological nature. The comprehensive analysis of the legal mechanisms for personal data protection in the EU demonstrates the formation of the legal institution for the personal data protection in the EU. However, the role of technological progress and globalization, the information technology development, automated data processing methods, the global information systems formation raises the problem of a continuous improvement of legal and technical regulation of personal data protection.

The national legislation of the Republic of Kazakhstan lags behind the European and the world experience, as proved by the current national legislation analysis. It is worth noting that in 2015, Kazakhstan and the European Union signed the Agreement on Enhanced Partnership and Cooperation, which addresses the need to ensure a high level of personal data protection by the experience and knowledge exchange. The negative aspect of the national legislation in the Republic of Kazakhstan is that there is still no authorized body for personal data protection that would be similar to the

agencies for personal data protection in European countries. However, its creation has already begun. This body should be independent as it should protect the citizens' human rights. Furthermore, the normative regulation of personal data protection of the Republic of Kazakhstan does not provide adequate protection and needs improving in order to increase the level of compliance with the international and European standards.

In order to effectively ensure the right to protection of personal data, a number of issues should be addressed within the legal regulation of personal data. Accordingly, improving the legislation on personal data should raise it to the leading countries legislation level, promote its integration into the global information space and ensure its citizens' protection. Despite the lack of experience in personal data legal protection in Kazakhstan, this study is of practical importance and constitutes the basis for the development of personal data protection mechanisms. In addition, it is made up of democratic values and ideas borrowed from the rich positive experience accumulated by European states. The extreme urgency of the outlined problems caused the need for the analysis and understanding of the legal science possibilities to ensure the personal data protection. The proposals aimed at improving legislation in this area are distinguished by their novelty.

The practical significance of the obtained results lies in the fact that the main conclusions, formulated in the course of the research, can be used in the following law-making activities: the development and improvement of the international legal norms, European legal acts and Kazakhstani legislation on the protection of the individuals' rights and freedoms when using their personal data; in law enforcement activities related to the individuals' personal data protection in the European Union and in the Republic of Kazakhstan; when training specialists whose activities are directly connected to the use (collection, processing, storage, transfer, etc.) of personal data; the boost of awareness and legal literacy regarding the protection of the rights and freedoms in personal data processing by entrepreneurs, representatives of federal government bodies and executive authorities and local government bodies of the Republic of Kazakhstan. This research is a fundamental analysis of the existing legal norms of the European Union concerning the individuals' personal data protection. Therefore, the theoretical significance of this study results is that they can be used for further further research in the sphere of protecting human rights and freedoms and contribute to resolving the problems of personal data protection.

References

Abdullin A.I. (2017). *European law: textbook and workshop for academic bachelor's degree.* Yurayt Publishing House.

Alyamkin S.N. (2016). Personal data as an object of legal regulation: the concept and methods of protection. *World of Science and Education*, 4(8): 84-89.

Avramenko A.V. (2019). Best international experience in protecting employees' personal data. *Scientific Legal Journal*, 7: 59-64.

Bachilo I.L. (2019). *Information law: textbook for academic bachelor's degree*. Yurayt Publishing House.

Brązkiewicz D. (2019). The security of personal data in European Union since 2018. *Rozprawy Spoleczne*, 12(4): 39-45.

Bu-Pasha S. (2017). Cross-border issues under EU data protection law with regards to personal data protection. *Information & Communications Technology Law*, 26(3): 213-228. Doi: 10.1080/13600834.2017.1330740.

Byrum K. (2017). The European right to be forgotten: A challenge to the United States Constitution's First Amendment and to professional public relations ethics. *Public Relations Review*, 43(1): 102-111. Doi: 10.1016/ j.pubrev.2016.10.010.

Committee of Ministers of the Council of Europe (1987). Recommendation No. R (87)15 of the Committee of Ministers to member states regulating the use of personal data in the police sector. Rm.Coe.Int. -- https://rm.coe.int/168062dfd4.

Council of Europe (1950). Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols No. 11 and 14. Eods. -- https://www.eods.eu/library/CoE_European%20Convention%20for%20the%20Protection%20of%20Human%20Rights%20and%20Fundamental%20Freedoms_1950_EN.pdf.

Council of Europe (1981). Convention for the Protection of Individuals with regard to Automated processing personal data. Hrlibrary. Umn. Edu. -- http://hrlibrary.umn.edu/euro/Rets108.html.

Custers B., Dechesne F., Sears A.M., Tani T., & Hof S. (2018). A comparison of data protection legislation and policies across the EU. *Computer Law & Security Review, 3*(2): 234-243. Doi: 10.1016/j.clsr.2017.09.001.

Dei M., Rudenko O. & Lunov V. (Ed.) (2020). *Association agreement: driving integrational changes*. Accent Graphics Communications & Publishing.

European Parliament (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Eur-Lex.Europa. -- https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046.

European Parliament (2000). Regulation (EO) No. 45/2001 for the European Parliament and for the Council of 18 December 2000 is relatively protected against a person against processing against personal data from an institution and organization of the Community and for free movement on such a basis. Eur-Lex. Europa. -- https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=celex%3A32001R0045.

European Parliament (2002). Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Eur-Lex. Europa. -- https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058.

European Parliament (2012). Charter of Fundamental Rights of the European Union. Eur-Lex. Europa. -- https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012P%2FTXT.

European Parliament (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Eur-Lex. Europa. -- https://eur-lex.europa.eu/eli/reg/2016/679/oj.

Gonzalez S.M. (2016).The automatic exchange of tax information and the protection of personal data in the European Union: Reflections on the latest jurisprudential and normative advances. *EC Tax Review*, 25(3): 201-213.

Guiwan P.D. (2019). Regulation of personal data protection in acts of international law. *Scientific Bulletin of the International Humanities University*, 42(2): 130-133.

Hoofnagle C.J. (2019). The European Union general data protection regulation: what it is and what it means, Bart van der Sloot, Frederik Zuiderveen Borgesius. *Information & Communications Technology Law*, 28(1): 65-98. Doi. 10.1080/13600834.2019.1573501.

Granger M-P., & Irion K. (2018). The right to protection of personal data: The new posterchild of European Union citizenship?. In: S. de Vries, H. de Waele, & M-P. Granger (Eds.). *Civil Rights and EU Citizenship: Challenges at the Crossroads of the European, National and Private Spheres (Interdisciplinary Perspectives on EU Citizenship).* (pp. 279-302). Edward Elgar. Doi: 10.4337/9781788113441.00019.

Khuzhina A.V. (2015). The legal nature of the Internet: regulatory issues. *Bulletin of the South Ural State University. Series "Right"*, 15(1): 101-107.

Kutsin J.M. (2018). Possibilities of the Parliament of Ukraine to improve the mechanisms of personal data protection: a comparative legal study. *Scientific Bulletin of Uzhhorod National University*, 1(49): 79-84.

Lozovaya O.V. (2015). Legislation of the Republic of Kazakhstan in the field of personal data protection: a comparative analysis with the law of the European Union. *Bulletin of the Institute of Legislation and Legal Information*, 1(37): 28-133.

Martinez D.F. (2018). Unification of personal data protection in the European Union: Challenges and implications. *Profesional de la Informacion*, 27(1): 185-194. Doi: 10.3145/epi.2018.ene.17.

Parliament of the Republic of Kazakhstan (1994). Law No. 154-XIII "On operational-search activities". Adilet. Zan. Kz. -- https://online.zakon.kz/Document/?doc_id=1003158#pos=121;-53.

Parliament of the Republic of Kazakhstan (2013). Law No. 94-V “On personal data and their protection”. Adilet. Zan. Kz. -- https://online.zakon.kz/Document/?doc_id=31396226.
Parliament of the Republic of Kazakhstan (2015). Labor Code of the Republic of Kazakhstan No. 414-V. Adilet. Zan. Kz. -- http://adilet.zan.kz/rus/docs/K1500000414.
Parliament of the Republic of Kazakhstan (2020). Code of the Republic of Kazakhstan No. 360-VI “On people’s health and the health care system”. Adilet. Zan. Kz. -- http://adilet.zan.kz/rus/docs/K090000193_.
Radkevich O.P. (2014). *Civil law protection and protection of personal information on the Internet.* National Academy of Internal Affairs.
Reding V. (2011). The upcoming data protection reform for the European Union. *International Data Privacy Law, 1*(1): 3-5. Doi: 10.1093/idpl/ipq007.
Shevchuk A.A. (2018). *Legal regulation of personal data protection in the European Union*. Nauka.
Telina Yu.S. (2016). *The constitutional right of a citizen to privacy, personal and family secrets when processing personal data in Russia and foreign countries.* Academy of the Prosecutor General’s Office of the Russian Federation.
Tikkinen-Piri C., Rohunen A., & Markkula J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review, 34*(1): 134-153. Doi: 10.1016/j.clsr.2017.05.015.
Yurchenko I.A. (2016). *Violation of privacy. Legal research at the Department of Criminal Law of the All-Union Law Institute.* Nauka.
Zhatkanbaeva A.E. (2009). *Theoretical problems of constitutional and legal support of information security in the Republic of Kazakhstan.* Al-Farabi Kazakh National university.