Protection of privacy in information technologies in the context of COVID-19: A comparative legal analysis of the Republic of Kazakhstan and the European Union

by *Gizat Kubenov*[*], *Serik K. Zhetpisov*[**], *Gulnar A. Alibayeva*[***], *Yuriy Yu. Kolesnikov*[****], *Ainash K. Kydralinova*[*****]

Abstract

Today, the world community faces the arduous and responsible task of preventing the spread of the coronavirus disease COVID-19, which objectively requires the adoption of a complex of anti-epidemic (organizational, medical, administrative, and other) measures to prevent the spread of COVID-19 and to contain and eliminate this epidemic. At the same time, to a large extent, such measures are embodied in various forms of restrictions on the realization of civil, political, and other rights, freedoms, and legitimate interests of a person and a citizen, as well as to a certain extent there are encroachments on the inviolability of a person's private life. The purpose of the scientific article is to study the state mechanisms of Kazakhstan and the European Union on legal support and security of personal data on the Internet, particularly during the COVID-19 pandemic, and to determine possible ways for their development and improvement. The research used dialectical, historical-legal, formal-logical, comparative-legal, and special-legal research methods, and systemic-structural research methods, as well as the method of systemic analysis. The theoretical significance of the study lies in the fact that it develops new scientific provisions, proposals, and recommendations that deepen the theoretical and practical foundations in the field of legal regulation of personal data protection in information

[*] Specialized Interdistrict Economic Court of Pavlodar Region 140000, 104 General Dyusenov 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.
[*****] Department of Law – Faculty of Business, Education and Law Innovative Eurasian University 140000, 45 Lomova Str., Pavlodar, Republic of Kazakhstan.

Rivista di Studi sulla Sostenibilità, (ISSN 2239-1959, ISSNe 2239-7221), 2023, 1

Doi: 10.3280/RISS2023-001004

technologies during the pandemic in the European Union in general and in the Republic of Kazakhstan in particular.

Key words: privacy, COVID-19, privacy protection, privacy on the internet, European Union.

First submission: 31 March 2023; *accepted*: 31 May 2023

1. Introduction

International norms on the legal rights and freedoms of a person guarantee everyone the possibility of the highest level of health, obliging the state to take measures to prevent threats to the health of the population and to provide medical assistance to those who need it. International standards in the field of human rights also provide that in situations of serious threats to the health of the population and states of emergency that threaten the life of the nation, limitations of certain rights and freedoms are permissible, if such limitations are introduced legally, are necessary and scientifically justified, and also if their application is not arbitrary or discriminatory and limited in time, if human dignity is respected, in addition, such restrictions are subject to control and corresponding to the pursued goal.

Modern states are trying to form a regulatory framework and fill in the legal gaps in the regulation of the Internet space, which indicates a shift in the focus of a person's real-life to the virtual world. This was also facilitated by the COVID-19 pandemic that unfolded in 2020 when restrictive measures introduced everywhere had a significant impact on the development of the technology industry. For example, only one of the companies in Kazakhstan providing services in this area reported an increase in the number of Internet subscribers in the first half of 2020 by 6.1%. This indicates that the pandemic is accelerating the introduction of digitalization in many countries and the life and activities of modern man are gradually moving to the Internet space.

With the spread of the coronavirus disease COVID-19, many countries have begun to use mobile technologies to overcome this global problem. State methods vary. If in Asia, smartphones and geolocation are mostly used to determine and inform people whether they have crossed paths with carriers of the coronavirus, then in the participants of the European Union (EU) such technologies are used to check whether citizens adhere to the self-isolation regime or have not had direct contact with patients with coronavirus disease. EU countries actively signed agreements with communication operators on

the collection of anonymous location data and emphasized the development of a single mobile application that would help track and prevent the spread of the coronavirus. However, with the spread of such technologies, there are more and more doubts about how to maintain the fine line between privacy rights and protection of life and health of an individual.

The Republic of Kazakhstan, developing in line with modern trends of globalization and informatization, as well as the COVID-19 pandemic, has faced the emergence of new challenges regarding the provision and protection of privacy. However, the study of these problems has not yet been adequately reflected in Kazakhstan's legal science and practice, despite their relevance. This is explained by the fact that there is no legal tradition of ensuring privacy in Kazakhstan, which dictates the need to turn to the richest progressive experience of the legal protection of this right in Europe, which could be useful to domestic legislators. Therefore, it is important to ensure the reflection of the process of protection of the right to privacy at the European level, where new human rights, defined as information rights, appear, with the aim of further integration of European experience into the legislation of the Republic of Kazakhstan.

Many scientific works are devoted to the problems of legal regulation of the right to privacy in the age of digital technologies, in particular, such scientists as M.S. Ablameyko (2018), M. Goddard (2017), M.A. Gracheva (2017), S.Yu. Kashkin (2018), S. Malgieri (2019). The study is aimed at identifying the main patterns of development and regulation of the right to privacy in the process of obtaining personal information in the digital era in the European Union as a whole and the Republic of Kazakhstan in particular, given the modern challenges associated with the COVID-19 pandemic. The provisions, conclusions, recommendations, and proposals formulated in the study complement the potential of legal sciences and can be used as a basis for further research in the field of implementation and defense of the personal information in the European Union and the Republic of Kazakhstan.

2. Materials and methods

The choice of research methodology is determined by scientific and applied expediency. Scientific activity is based on scientific methods and principles inherent in both the general theory of law and the science of international law with its specific features. The research used dialectical, formal-logical, comparative-legal, and special-legal research methods, and systemic-structural research methods, as well as the method of systemic analy-

sis. Dialectics, which studies not specific forms and types of development, but general moments, connections, and regularities of any changes, is not only a general theory of development but also a universal method of learning about developing objects. Dialectical thinking is usually characterized as a flexible non-standard creative understanding of the world. Thus, the dialectical method was used to study the development of the human right to privacy and establish the connection between this right and other legal phenomena and rights.

The main task solved by the legal comparative method is to obtain new knowledge by comparing the legal sources and practices of the European Union and the Republic of Kazakhstan. This method is used for the doctrinal characterization of the right to privacy in the European legal field and the Republic of Kazakhstan. The formal-logical method is used for the formation of new concepts, their classification, typology of the studied phenomena; elimination of inaccuracies and contradictions, etc. This method involves the application of logical laws and rules (they are also called methods, techniques, or logical methods): descent from the abstract to the concrete, abstraction, analysis and synthesis, induction and deduction, modeling, and others. It ensures logical consistency and consistency in the presentation of legal norms; the presence of the necessary internal elements in the formulation of concepts, as well as the derivation of logical consequences. In this study, the legal regulation of the right to privacy in the aspect of modern technologies was analyzed using the formal-logical method. Special legal methods – clarified the relationship between the legislation of Kazakhstan and international legal documents on the human right to privacy. The essence of this method of knowledge is that it is used for external legal processing of legal material – the so-called "dogma of law". System-structural method – to clarify the role of privacy protection in the human rights system and to study other problems related to this right; method of system analysis – to determine the effectiveness of norms aimed at protecting the right to privacy in the age of digital technologies.

A number of articles related to the research topic were also analysed, such "Legal regulation of personal data taking into account the introduction of ID cards and biometric passports" (Ablameyko, 2018), "Legal positions of the Constitutional Court of Russia and the European Court of Human Rights: genesis and mutual influence" (Chernyshev, 2010), "A comparison of data protection legislation and policies across the EU Bart Custers" (Dechesne et al., 2018), "The EU General Data Protection Regulation (GDPR): European regulation that has a global impact" (Goddard, 2017), "Features of the interpretation of the right to inviolability of private and family life, home and

correspondence in European legal systems" (Gracheva, 2017), "Recommendations for ensuring confidentiality on the Internet" (Ilyubaev et al., 2021), "European Union Law: Textbook for Academic Bachelor's Degree" (Kashkin, 2018), "Legal responsibility for violation of the legislation on personal data in the Russian Federation and the Republic of Kazakhstan" (Komarov & Mytskaya, 2018), "Legislation of the Republic of Kazakhstan in the sphere of personal data protection: a comparative analysis with the law of the European Union" (Lozovaya, 2015), "From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation" (Macenaite, 2017), "Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations" (Malgieri, 2019), "The EU's General Data Protection Regulation (GDPR) in a research context" (Mondschein & Monda, 2019), "The right to privacy: some current trends in the practice of the Strasbourg court" (Pankevich, 2018), "Towards a global data privacy standard" (Rustad & Koenig, 2019), "Global data privacy: The EU way" (Schwartz, 2019), "Legal regulation of personal data protection in the European Union: genesis and development prospects" (Shadrin, 2019), Experience of criminal law protection of personal data of Kazakhstan and Germany" (Vabyshevich, 2020), "Data retention and its implications for the fundamental right to privacy: A European perspective" (Vedaschi & Lubello, 2015), "Place of personal data in the system of information of limited access" (Volchinskaya, 2014).

3. Results

3.1. General provisions for the defense of the personal information in the age of digital technology

The experience of European countries, as well as European legislation, is a signpost to true democracy, which almost all countries in the world emulate. European Union (EU) countries have come a long way in ensuring and privacy protection. Because in Europe of the 20th century, liberal thought combined the freedom and individualism of the individual, who now tried to be independent and no longer tolerated interference in his private sphere. Since then, the main goal of European states is not to control, but to ensure the privacy of a person.

The right to private life, referred to as EU respect for private life, first appeared in the Universal Declaration of Human Rights (UDHR) (United Na-

tions General Assembly, 1948), an international human rights instrument, as one of the fundamental rights protected. Article 17 of the International Covenant on Civil and Political Rights (United Nations General Assembly, 1966) states: "No one shall interfere arbitrarily or unlawfully with his private life, family, home or correspondence, or with his property, honour and calling".

Europe also reaffirmed this right in the European Convention on Human Rights (ECHR) of 1950 (Council of Europe, 1950) shortly after the adoption of the Universal Declaration of Human Rights. Art. Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms states that "everyone has the right to respect for his private and family life, home and correspondence". Article 10 of the Covenant states: "Everyone has the right to freedom of expression." This right includes freedom to express personal opinions and to receive and impart information and ideas without interference by public authorities and regardless of frontiers (Pankevich, 2018).

Modern law enforcement practices in EU countries and major systemic changes in information technology have driven reforms in EU data protection legislation. In 2009, discussions began on the need to modernize EU data protection rules and a public consultation on the future legal framework for implementing fundamental privacy rights. As a result of long-term negotiations between the European Parliament and the Council of the European Union, Regulation (European Parliament and Council of the European Union, 2016) No. 2016/679 on the processing of personal data and on the free movement of such data (GDPR). The GDPR establishes rules for the protection of natural persons concerning the processing of personal data by competent authorities for the prevention, investigation, detection or prosecution of criminal offences or criminal sanctions, which each EU member state implements on its territory and must apply from May 6, 2018.

The General Data Protection Regulation provides for the right to delete information; the right to appeal (according to which a person may not agree to the processing of his data); the right to transfer data; and fines for data breaches. This act has played an important role among many others in ensuring the protection of the privacy rights (Goddard, 2017).

The adoption of the General Data Protection Regulation modernized EU data protection legislation and made the protection of basic rights acceptable in the context of the economic and challenges in the social sphere of the digital age. The GDPR preserves and develops the fundamental principles and rights of the data subject. By EU legislation, the provisions of the Regulation are directly applicable and there is no need to enshrine them at the national level. Thus, the general data protection regulation provides a single set of

data protection rules for all countries of the European Union. This creates a coherent system of protection across the EU (Rustad & Koenig, 2019).

Although Kazakhstan is not a member state of the EU, it has a large number of projects with the EU and uses information products made in the EU. In this context, an analysis of Article 8 of the European Convention on Human Rights seems appropriate. Article 8 of the ECHR states that all people have a number of rights related to privacy and family life. Public authorities shall not interfere with the implementation of this right, besides as required by law and necessary for the sake of national and public safety or the economic well-being of the country in a democratic society, to prevent civil unrest or crime, to protect health or morals, or to protect the rights and freedoms of others.

From the point of view of the user of Internet resources, the issue of protecting his data, the terms of their use and distribution, as well as mechanisms for protecting his rights in case of violation remains important. The state is obliged to guarantee such persons proper conditions for safe use of the Internet and placement of their data on it. According to Recommendation CM/Rec (2016) 5 (1) of the Committee of Ministers of Member States on Internet Freedom, Council of Europe member states have both positive and negative obligations (Council of Europe Committee of Ministers, 2016).

This document draws the attention of member states to the fact that any state intervention in the exercise of human rights and fundamental freedoms on the Internet must meet the requirements of the Convention. In addition, the state is obliged to timely and properly provide the public with information about restrictions directly related to the possibility of disseminating confidential information, taking into account the relevant legal framework that is directly related to this. Laws must ensure that all private information is protected by the ECHR.

Control over the protection and use of private information in the World Wide Web must be implemented by the state. Thus, in the practice of international law-making and law enforcement, the owner and manager of data must not allow the disclosure of personal data that became known to him in connection with the performance of professional or official, or labor duties. This confidentiality obligation is a key element in respecting data subject rights. At the same time, the owner of personal data must determine what measures must be taken to ensure their protection. However, the control of such activities, legal regulations and other legal actions to monitor the legal use of personal data on the Internet is the responsibility of the state (Schwartz, 2019).

State intervention in the right to privacy on the Internet requires compliance with the requirements of legality, legitimacy, and proportionality provided for in Article 8 of the Convention, i.e. the use of the so-called "three-pronged test". Thus, there is a provision for such interference in the limitation of rights that would be justified under specific circumstances. In general, according to the practice of the European Court of Human Rights, the state retains certain freedom of action in balancing public and private interests in the context of protecting the right to privacy in the modern world. At the same time, this freedom depends on the nature and importance of legitimate interests, as well as on the degree of necessary intervention (Volchinskaya, 2014).

Kazakhstan is a party to the 1966 Covenant on Civil and Political Rights (General Assembly, 1966), article 17 of which guarantees everyone protection from arbitrary or unlawful interference in his personal and family life, attacks on the inviolability of his home, secrecy of correspondence, honor, and reputation. It is noteworthy that the national legislation, namely Article 18 of the Constitution (Parliament of the Republic of Kazakhstan, 1995) proclaims the human right to inviolability of life in the private sphere, personal and family secrets, and protection of honor and dignity. The term "immunity" seems to be even more strict than the term "respect" used by the ECPL. It should be considered how these norms are implemented in practice in the Republic of Kazakhstan and how this practice is consistent with the European approach.

Traditional means of "satisfaction" of the victim (refutation, compensation for moral damage, liability for defamation) are often powerless against Internet technologies due to the lightning speed of information dissemination in a virtual environment. This, in turn, not only gives the right but also imposes an obligation on states to take specific measures to combat offenses on the Internet.

Thus, in the case of K.U. v. Finland, The European Court of Human Rights (ECtHR) has faced the state's unwillingness and inability to reveal the identity of the perpetrator to bring him to justice. The fact that the development of Internet technologies is ahead of the development of legislation cannot be taken into account when the state is obliged to protect the so clearly violated privacy of its citizens. As far as freedom of expression and confidentiality of communications are concerned, in the opinion of the court, despite their importance in a democratic society, the guarantees they provide cannot be considered absolute. The right to anonymity and freedom of speech should not a priori dominate such legitimate requirements as the protection of public order and the legitimate interests of others. Accordingly, the ECtHR unanimously concluded that there had been a violation of Article 8 of the European Convention in the present case. And it was expressed in the

fact that the Finnish law, protecting the confidentiality of communications, did not provide for an effective mechanism for protecting the rights of third parties violated by anonymous authors.

If we consider this problem in the aspect of Kazakhstan, then in practice it is very difficult for Kazakhstanis to prosecute anonymous authors who publish offensive materials against individuals. Meanwhile, almost every user of the World Wide Web has encountered similar cases at least once in their life. The Republic of Kazakhstan needs to develop legislation on the protection of privacy from virtual encroachments in two directions at the same time.

The first is the inclusion in the agenda of consideration of the issue of total deanonymization of Internet users, following the example of China. Even from the point of view of formal logic, the right to anonymity (as well as the opportunity to have free speech and express one's views enshrined in law, and indeed any right) can only belong to a certain subject of law. Before using any constitutional guarantees, he must somehow identify himself so that the state knows whose rights it protects. If a person is not going to use the possibilities of the Internet contrary to the law, he has nothing to fear that, under certain conditions, his identity may be revealed.

The second is the creation of a reliable system of guarantees against state arbitrariness and illegal use of personal data. As evidenced by the judicial practice of the same European Court of Human Rights, in a modern state, any intrusion of the authorities into private life must meet three conditions: be prescribed by law, pursue a proportionate goal, and be subject to impartial judicial control. In other words, whenever the police or someone else wants to know who is hiding behind a faceless avatar, they must convince the judge concerning a specific rule of law that this is necessary to protect citizens and society. It is important to understand that strengthening control over Internet activity is not necessary to combat dissent and not to build a police state. It is necessary to protect the constitutional rights of citizens. And if judicial practice interprets legislative innovations in this way, it will be the most reliable response to the challenges posed by the latest information technologies (Kazakh truth, 2017).

3.2. Increasing the need to protect personal data in the context of COVID-19

COVID-19 has become the first pandemic of the digital era – right now, the latest digitization tools can be massively used to combat the disease: smartphones, as well as the data generated as a result of their use. For exam-

ple, most popular applications collect information about our location through GPS data, WiFi points, and Bluetooth use – and we permit them to do this by confirming consent to use the next function from our smartphone, for example, to put geolocation in the next post in social networks Or mobile operators can track the movement of subscribers through the communication towers that provide mobile communication. And although such data are mostly stored by the companies themselves and used for marketing, the state can gain access to them. Usually, such access can be obtained to investigate crimes or counter-terrorist activity – and usually by court order.

In the context of countering the pandemic, state governments mentioned the possibility of using digital assets for their benefit and the introduction of preventive measures, and also mentioned the technological giants and the huge arrays of data they possess. From the practice of the European Court of Human Rights (the decision in the case of Uzun v Germany), it can also be concluded that the tracking of a person's movements by the state is an interference with his privacy, but this can be justified only if the possibility of tracking is provided for by law and is necessary to achieve a socially important goal.

Such a goal as countering the COVID-19 pandemic falls under the goal of protecting public health. However, other criteria for restrictions on human rights must also be met: first of all, the restriction of privacy must be established by law and not based on the undefined discretionary powers of law enforcement or executive authorities. It is also important to pay attention to the standards for compliance with human rights (and in particular privacy) by technology companies that are not subjects of international law and do not have to directly comply with these standards.

Paragraphs 11-12 of the UN Guiding Principles on Business and Human Rights (UN Security Council, 2011) state that companies must avoid violations of human rights guaranteed by International Covenants (which, as discussed above, include the right to privacy) and must eliminate the adverse impact of their activities on such rights. In addition, the Council of Europe, in its recommendation on the roles and responsibilities of Internet intermediaries CM/Rec(2018)2 (Council of Europe, 2018), emphasized the need for intermediaries to obtain consent for data aggregation, as well as the fact that technologies for digital tracking of individuals must not violate the right to privacy and meet privacy standards when transferring data to third parties. Therefore, technology companies should also make every effort to respect the right to privacy in their work. And no matter how tempting such companies are to hand over all collected data about users to the state and the temptation of the state to force tech companies to show them all the social contacts

of patients (for the benefit of countering the pandemic), this will not be legitimate (Dechesne et al., 2018).

If we refer to the practices of European countries, then Poland developed its application. Its installation is mandatory, the app tracks the location of sick and quarantined people, and requires you to take a selfie within 20 minutes of receiving a push notification to confirm your location. This should prevent police visits to check people are at home – however, police visits continue. In addition, data from this application will be stored for 6 years. Norway is starting to test such an application, which will collect data on the movement of people, and in case of detection of the virus, it will send a notification to all users who were at a distance of fewer than 2 meters from the patient for more than 15 minutes – to prevent the spread of COVID-19. Germany, Canada, and Ireland are thinking about developing and implementing their applications. There are also calls for the development of the application at the level of the European Union, taking into account the requirements of EU legislation regarding the regulation of private information and GDPR. Most of the world's countries have not yet introduced mandatory tracking of coronavirus patients – except for states known for their neglect of individual human rights. For the most part, the data received using applications will be stored only during the quarantine.

But there are valid concerns that such collection of sensitive data about people could be another step toward mass surveillance. Therefore, states must use the received data strictly in proportion to the purpose of their processing and delete them immediately after the purpose of processing has been achieved. In particular, human rights defenders stress that the use of digital technologies to track and monitor individuals and the population must be carried out in strict accordance with human rights standards and include elements of accountability and safeguards against abuse (Gracheva, 2017).

Scaling up mobile tracking programs in response to COVID-19 could be scientifically redundant and risk human rights violations if not accompanied by effective privacy safeguards. Years of experience in implementing emergency measures such as electronic surveillance to combat terrorism show that they often go too far, do not provide the desired results, and, once introduced, often remain in force after the initial reason for the introduction disappears.

International human rights law provides that even when a state restricts rights and freedoms in the interests of public health during a state of emergency, such restrictions must be lawful, necessary, and proportionate. The state of emergency must be limited in time, and any restrictions on human

rights must take into account the disproportionate consequences for certain categories of the population or marginalized groups.

Notably, international legal instruments such as the Personal Protection Convention Relating to Automatic Processing of Personal Data (Convention No. 108) (Council of Europe, 1981) and the modernized Convention No. 108+ (Council of Europe, 2018b) For the purposes of and the European Parliament and of the Council (EU) Regulation 2016/679 (European Parliament, 2016) on the protection of natural persons in relation to the processing of personal data, on the free movement of such data and repealing Directive 95/46/EU (GDPR) (European Parliament, 1995) guarantees high standards in the field of protection of personal data. At the same time, it can be noted that the specified documents as a whole are unlikely to be incompatible with the temporary application of restrictive measures aimed at saving lives and fighting the pandemic.

In particular, in a joint statement by Alexandra Pierucci, Chair of the Convention 108 Committee, and Jean-Philippe Walter, Commissioner for Data Protection of the Council of Europe, dated March 30, 2020, it is noted that the Modernized Convention 108+ recognizes the need to allow certain exceptions and limitations for urgent purposes, which are vital and of public interest. However, such restrictions must meet clear requirements to ensure uninterrupted observance of the rule of law. Exclusions must have a legal basis, not contradict fundamental rights and freedoms, be necessary and proportional in a democratic society – this is established by the Modernized Convention 108+. Such restrictive measures should be applied: exclusively temporarily (during a certain period, clearly limited by the duration of the state of emergency); subject to the establishment of guarantees (for example, coding of data with keys, mandatory awareness of the subject regarding the processing of data related to him, conducting an assessment of the impact of processing directly before it begins, etc.); subject to the reversibility of restrictive measures (this means that after the cessation of the circumstances that became the basis for the introduction of restrictive measures and the achievement of the specified goals, the normal regime of privacy protection must be restored in full with the cancellation of exceptions and restrictions that were applied during the state of emergency) (Kashkin, 2018).

These principles also apply to the Covid-19 response using mobile user location data. The collection and analysis of such data may reveal information about the identity, movements, and contacts of users, which is fraught with the infringement of the privacy protection. Article 17 of the International Covenant on Civil and Political Rights, based on Article 12 of the Universal Declaration of Human Rights, states that unlawful interference with

private life is prohibited,ë arbitrary or unlawful interference with the inviolability of his home or the secrecy of his correspondence. The Human Rights Committee, in its general comment on this article, states that there can be no interference with the right to privacy at all, except as provided by law. At the same time, restrictions should be proportionate to the desired goal and necessary, taking into account the severity of the situation.

Mobile tracking poses significant and well-proven privacy risks. Mobile user location data may contain sensitive and non-public information about a person's identity, place of residence, behavior, connections, and activities. The use of these mobile networks gives the authorities targeted and real-time opportunities that can be used to enforce quarantine, discrimination, or persecution of citizens for other reasons. In the hands of an unscrupulous government that already practices intrusive surveillance methods, this can lead to more repression.

The mobile tracking programs described above raise concerns that governments may be collecting, using, and storing data for more than legitimate and targeted disease monitoring efforts. The lack of transparency in many such initiatives, as in Ecuador and Ethiopia, prevents the public from assessing whether there are reasonable limits on the personal information that is expected to be collected, used, aggregated, and stored and whether tracking and data collection will stop when the pandemic subsides. This is especially true for countries such as China, and Ethiopia, where the practice of mass surveillance has already developed (Macenaite, 2017).

Other problematic aspects include restriction of freedom of movement based on arbitrary and non-transparent application algorithms, as in China; no need to obtain consent to use data, as in Armenia, Israel, and South Korea; linking mobile tracking with other technologies, including face recognition. Nearly all location-based initiatives to fight the coronavirus are putting massive amounts of data in the hands of governments, many of which have a history of repression and discrimination against marginalized populations such as religious minorities and political dissidents.

Years of experience in the introduction of emergency measures show that they often go too far, do not achieve the desired goals, and, once adopted, last longer than necessary. Regardless of the severity of the situation, states and private actors should strive to ensure that emergency measures do not go beyond the limits of legal restrictions on individual rights.

This means that governments, in their fight against Covid-19, can use or authorize mobile tracking technologies only if they are proven necessary and proportionate from an anti-epidemic point of view, and if their use is accompanied by sufficient guarantees that exclude the violation of rights and free-

doms. An answer must be given to the fundamental question of whether such technologies are capable of containing the spread of the coronavirus, or in reality, they can distort the perception of the risk of infection of a particular person or mislead society as a whole. The state must evaluate other means at its disposal that would be less intrusive to human rights such as privacy and freedom of movement. The limits of restriction of these rights are regulated by the international legal standard, which establishes the following requirements (Malgieri, 2019).

Restrictions must be lawful, that is, not arbitrary or discriminatory in nature and application, and imposed based on a law that would ensure that people clearly understand the restrictions imposed on them and provide clear limits to the discretionary powers of the authorities. Restrictions must be necessary, effective, based on scientific facts, and infringe on rights and freedoms to the minimum possible extent. Restrictions must be proportionate to the risks to public health and must not in any way affect the substance of the rights being restricted. Restrictions must pursue a legitimate aim: in this case, the protection of public health (but not a xenophobic or discriminatory agenda). The effect of restrictive measures should be limited in time to a period of emergency. The technology used and authorized users must respect human dignity. The applied technologies should be transparent and should be subject to verification and oversight; remedies should be provided for violations of human rights.

Human Rights Watch and over 100 other non-governmental organizations recently urged governments to respect privacy and human rights when using digital technologies to contain the pandemic. In our opinion, at least the following conditions must be met: must be lawful, necessary, proportionate, transparent, and justified in terms of a legitimate public health goal; should be limited in time and only be valid for the period necessary to combat the pandemic; should be limited in scope and adopted solely to combat the pandemic; must adequately protect private information; must take into account the risks of discrimination and other human rights violations against marginalized populations; should ensure transparency of any data-sharing arrangements with other public and private actors; should include safeguards to prevent undue surveillance and ensure access to effective remedies; should include mechanisms for the free, active and meaningful participation of stakeholders (Vedaschi & Lubello, 2015).

By the GDPR, the legal grounds for processing personal data when issuing code certificates are: Article 6(1)(c) of the GDPR – processing is carried out in the public interest or to fulfill the powers of state authorities; Article 9(2)(g) GDPR – processing is socially necessary and must comply with the

current legislation of EU members; is carried out in compliance with the principles of proportionality to the stated purpose, respect for the right to the protection of personal data and ensuring the basic rights and freedoms of the data subject.

The EU government also follows the provisions of the Convention for the Protection of the Individual on automatic processing of personal data (Convention 108+) when determining the process of checking the vaccination status of its citizens. Regarding the challenges of the pandemic, Council of Europe Convention No. 108 acknowledged the need to restrict the right to protection of private information, but stressed the importance of carefully assessing the proportionality and effectiveness of any such restrictions.

Therefore, the development of an algorithm for checking the vaccination status of citizens in the EU does not pose an insurmountable problem either for business entities that may need such information from their visitors (restaurants, shopping centers, etc.) or for employers. When solving this issue, EU countries lean towards digital solutions for information collection and are guided by the following aspects of personal data protection. Time limitation: the period of storage of personal data collected must be reasonably limited. Legally justified purpose: the purpose of data processing must be clearly defined and based on a certain legal norm. Proportionality of measures and continuous assessment of their effectiveness: proportionality is determined by effectiveness and means the ability to stop applying a certain measure in cases where there is no evidence of effectiveness. Transparency and comprehensibility of data processing operations: to the greatest extent, this aspect concerns several requirements for the use of automatic means of reading information. Accountability of data controllers and impact assessment of the effectiveness of private information protection measures.

The experience of Italy has become indicative. The political debate on the introduction of “green certificates” in this country ended with the victory of the imperative of certificates as a necessary condition for the admission of all workers to the employer’s premises. The law entered into force in September of this year, and the new procedure has worked both in the Italian public and private sector. The risks of disclosure of personal data were minimized: the QR code generated by the mobile application contains information limited to a minimum (the name of the person and the validity period of the certificate). This approach was also applied by Luxembourg. The Covid Check application, which has been used in this country since October to confirm the fact of vaccination, works in a way that reduces all risks of processing personal data to zero. Since the operation of scanning the QR

code is not accompanied by the storage of any information about the person, it cannot be considered as processing of personal data.

Not all countries have yet managed to implement an effective procedure for checking vaccination status. The political interests of the opponents of quarantine measures, who do not want to move along the path of legal development, usually stand in the way. Poland is demonstrating such results today. Her government has faced accusations of improper disclosure of vaccination information. For several months, the Ministry of Health of this country was engaged in the legal settlement of this issue, and then stopped work on the corresponding law due to public opposition. Community opinion on this issue is divided: employers, worried about the prospect of losing their companies due to the impossibility of ensuring proper working conditions, speak about the need to check vaccination status; trade unions and some workers claim discrimination and segregation.

This concise analysis is an illustration of the decisive strategy of countering the coronavirus and the innovative tactics of rulemaking of some EU countries in the conditions of the COVID-19 pandemic. When developing legislation, most European countries proceed from public interests as a justified goal of restricting some individual rights. It turns out that even the strict GDPR cannot stand in the way of limiting the rights to protect personal data when it comes to the urgent need to adapt legislation to the requirements of the times.

3.3. The state of private information protection in the aspect of the development of digital technologies and the pandemic in the Republic of Kazakhstan

In the Republic of Kazakhstan, the situation with the recognition and consolidation of human rights received a new impetus with the adoption of the 1995 Constitution (Parliament of the Republic of Kazakhstan, 1995), which laid new foundations for the regulation of relations between the individual, society and the state. A person, his life, rights, and freedoms are declared the highest value of the state. In addition, according to the Constitution of the Republic of Kazakhstan, today a rights and obligations are fixed by law, including the right to inviolability of private life, opens up significant opportunities for individual self-realization not only for its citizens but also for the person as a whole.

The Constitution of the Republic of Kazakhstan since its adoption in 1995 is legally correct and through the market socio-economic and new political

relations in Kazakhstan society forms and consolidates the rights and freedoms of man and citizen. In this connection, there is a need to overcome the existing ambiguous understanding of privacy. However, the concept of "private life" has not yet been developed in the current legislation of the Republic of Kazakhstan. This is an important task facing the legislator, and its solution determines the legal limits of privacy restrictions and the creation of an adequate protection mechanism. Developing in the direction of democratic transformations, after gaining independence, the Republic of Kazakhstan dynamically and consistently fulfills practical tasks related to the formation of a legal state and civil society. In this regard, the constitutional consolidation of a wide range of political, civil, economic, and social rights of citizens provided for by the Universal Declaration of Human Rights (UN General Assembly, 1948) is an organic inclusion in the Constitution of the Republic of Kazakhstan.

The Constitution of the Republic of Kazakhstan defines the main, fundamental issues related to the protection of human rights. Normative acts adopted in the process of legal reform are based on the principles of legality, justice, equality of citizens before the law, humanism, etc. The declaration in the Constitution of the Republic of Kazakhstan of the rights and freedoms of a person and a citizen, his life as the highest value, sets specific requirements for the activities of state authorities. The state and society must make every effort to ensure that legal acts that establish the rights and freedoms of the individual operate automatically, regardless of the will or arbitrary subjective understanding, regardless of which political forces are in power and the state system of the country (Ilyubaev et al., 2021).

The Republic of Kazakhstan almost recently joined the process of information globalization, which gave rise to many different problems and led to the need to develop legal measures to solve them. And above all, the goal of the development of information technologies and the transition to the informatization of society was the private life of a person. Thus, modern Kazakhstani society and the state face new challenges in terms of ensuring privacy, and it is necessary to offer conceptual and acceptable solutions to these problems. Undoubtedly, the process of impact of new information technologies on the right to privacy is extremely complex, its analysis shows that the evolutionary period that separates the introduction of new technologies and their regulation is very slow.

In the program documents of the Republic of Kazakhstan, attention is paid to the problems of ensuring confidentiality and protection of private information, as well as achieving a balance of the interests of the individual, society, and the state. For example, the concept of cyber security is one of the key issues: “Ignoring security considerations when using Internet re-

sources and social networks increases the risk of confidentiality, unauthorized use or modification of publicly available personal data, as well as disclosure of restricted personal data. or extraterritorially accessible. for criminal communities or special services when they are stored in other states" (Volchinskaya, 2014).

In the Republic of Kazakhstan, the private information protection is regulated by the current legislation and laws, which contain the rights and obligations of the subject of legal relations in the field of circulation and private information protection, as well as responsibility for their illegal processing. The need to protect the interests of individuals, society and the state has led to the emergence of a fairly large number of legal structures that provide for restrictions on access to information. For example, the Law of the Republic of Kazakhstan dated May 21, 2013 No. 94-V "On personal data and their protection" (Parliament of the Republic of Kazakhstan, 2013), established the division of personal data into public and restricted access. (Article 6 of the Law of the Republic of Kazakhstan "On Personal Data and Their Protection"). According to the Law of the Republic of Kazakhstan "On Access to Information", information with limited access is information that constitutes a state secret, personal, family, medical, banking, commercial, and other secrets protected by law, as well as official information marked "For official use" (Parliament of the Republic of Kazakhstan, 2015a).

In Kazakhstan, issues and problems regarded to the private information protection are becoming increasingly important, especially in the context of countering the COVID-19 pandemic. On the one hand, despite the existence of the Law on Personal Data, many of its elements are stalling in practice, and there is also no strategic vision of moving toward the adoption of the key principles of the European General Data Protection Regulation (GDPR). On the other hand, recent cases of large-scale leaks of the personal data of Kazakhstanis in 2019 from state databases cast doubt on the ability and obligation of the state to protect personal data by the Law on Personal Data (Komarov & Mytskaya, 2018).

At the same time, the results of a study on personal data in Kazakhstan conducted in 2019 indicate the critical need to raise awareness and understanding of the importance of promoting a culture of personal data protection among Kazakhstanis to build a nationwide system of cybersecurity and cyber resilience. Today, in the context of the large-scale introduction of face recognition technologies, artificial intelligence algorithms, and the collection of fingerprints of Kazakhstanis in the coming years, on the one hand, and the implementation of ambitious tasks within the framework of the Digital Kazakhstan state program to ensure national security and create an information

society, on the other, it is important to ensure the secure collection, processing, and storage of personal data by the principles of the GDPR. Moreover, the importance and necessity of large-scale digitalization must be accompanied by observance of the main freedoms and rights, avoiding the manipulation of technology to digitally spy on citizens (especially activists) and excessive collection of personal data at the time of emergency and quarantine due to COVID-2019.

The emergence of e-government in Kazakhstan has contributed to a significant change in the relationship between society and the state to promote democratization and effective public administration. The other side of this process is the widespread introduction of technological solutions, massive data collection, and digital surveillance (surveillance). In the context of Kazakhstan's transition to a digital society, many opportunities, difficulties, and limitations have arisen. The ministries of health and internal affairs of Kazakhstan have partially turned to technological solutions to combat the COVID-19 outbreak (Lozovaya, 2015).

For example, about 8,000 Kazakhs in Almaty and Nur-Sultan under mandatory quarantine have been ordered to use the SmartAstana tracking app, which helps ensure that people remain in isolation. To do this, you must turn on your location, Wi-Fi, and Bluetooth settings so that you can track and ensure that people move no more than 30 meters from their designated location. If a person's phone is inactive for four hours, or if the Ministry of Health is notified that they have gone too far, the person receives a video call to clarify. In addition to tracking, the SmartAstana application also allows you to use some government services and services.

However, along with the obvious benefits of these measures, other equally important questions arise. In particular, who processes the collected personal data, who has access to it, how data depersonalization is ensured, how long this data will be stored on servers, how to prevent unauthorized access and leaks, and what protocols are developed for these and other crises, like the Protection Agency data, will oversee all these initiatives and monitor their compliance with the law and the observance of the digital rights of Kazakhstanis and many other issues, the answers to which have not yet been answered. In addition, primary technological solutions, caused by the need to prevent the deterioration of the epidemiological situation in individual cities and the country, today continue to change and transform into long-term mechanisms for collecting, processing, and storing the personal data of millions of Kazakhstanis.

Since the beginning of the COVID-19 pandemic in Kazakhstan, the situation with the private information protection has worsened, despite the crea-

tion of a specialized agency. Firstly, the entire ordinary routine life of most people automatically switched to digital rails: citizens began to use online services more often – trade, banking, etc. Secondly, despite the obvious digital and technological shift that catalyzed large-scale digitalization of various sectors by shock the personal data of the first cases were not properly protected, however, as well as basic human rights and freedoms, such as the privacy protection right, freedom of movement, the right to access information, etc. (Vabyshevich, 2020).

For Kazakhstan, the development of its regulations for the private information protection in the aspect of COVID-19 is becoming even more relevant and important. Of course, the pandemic has made adjustments to the implementation of the plans for the mass digitalization of the country and the promotion of ideas for the private information protection. The creation of an authorized body was the first step toward monitoring the situation and the state of affairs, as well as helping to ensure that the legislation in the field of personal data protection is strictly observed by all – both officials and active citizens – in each specific case without exception (Ablameyko, 2018).

The relevant Agency has significantly limited control over the application of laws on the private information protection and compliance with the requirements for the protection of private information – no one was held responsible for data leaks in the Damumed system and from other government databases. All this does not allow solving systemic problems, postponing the solution of the most important problems to a later date – training personnel, creating a legal and information culture, first of all, at home (that is, in the entire state apparatus). Dismissal cannot remain a method of punishment for violation of the law, because it defines clear mechanisms for holding accountable. Since personal data is subject to protection and the state acts as its guarantor, this means that everyone, without exception, must comply with the developed technical and legal parameters.

Initiatives to introduce artificial intelligence technology, facial recognition systems, and other technological solutions must take into account the risks associated with the provision, collection, analysis, and storage of personal data. The transparency of such processes will significantly minimize potential vulnerabilities, adequately respond to crises and enhance the cyber resilience of the Kazakhstani system.

The profile agency needs to develop a regulation on data leakage incidents and unauthorized access to personal data. These cases should be reported by organizations where similar crises occur, not by anyone else. This is a normal standard protocol, a set of tools and practices not only present in the European GDPR but all companies in the world. The introduction of

transparent risk management protocols will not only strengthen the system and personal data protection component but also reduce the existing gray areas that can be used for corruption and espionage purposes. These practices should be massively implemented in all government agencies working with databases, not to mention private businesses.

4. Discussion

The countries of the European Union were among the first to face the issues of data transfer and processing within the framework of international cooperation and were faced with the need to take comprehensive coordinated measures for their protection. Accordingly, they were the first to modernize the legislation and improve the human rights protection mechanism, taking into account the emergence of new technologies and awareness of new security challenges and risks. In recent decades, several international organizations have adopted several legal documents that develop basic information rights in connection with the use of modern information technologies and the spread of the COVID-19 pandemic in the world.

The creation of a more effective mechanism for the human rights protection in Europe is undoubtedly beneficial for citizens. Privacy law works for the benefit of EU citizens. Actions of the European Union to approximate the legislation of the EU member states will lead to the establishment of general rules on the protection of the right to privacy, which is necessary to give additional impetus to the more effective functioning of the European human rights mechanism. The new approach to the harmonization of the legislation of the member states of the European Union is based on the principle of full harmonization of the legislation through the approximation of the national laws of the member states and allows them to minimize the diversification of legal regulation. The most complete harmonization of legislation in integration entities often causes controversy, as it is necessary to take into account the interests of all involved parties. This is a rather complicated procedure since the states of the integration association are in different conditions of economic, social, political, cultural, and legal development. However, in the case of such an integration entity as the European Union, which proved the possibility of full integration of legislation taking into account the positions of the individual, society, and the state, achieving a balance of their interests, the uniqueness of the procedure can be noted (Mondschein & Monda, 2019).

In general, it is possible to propose two main ways at the international level of improving the modern system of privacy protection thanks to the

development of information technologies – normative and institutional. Thus, the regulation of the right to privacy on the Internet at the international level should be recognized as insufficiently developed. The issues of the right to be forgotten, responsibility for violations of the order of storage, transmission, distribution, deletion of information containing personal data, the inviolability of the consumer's private life, and the lawful behavior of e-commerce companies now require thorough research and consolidation. It can be either a single act or a combination of them, taking into account various aspects of the protection of the right to privacy. In this context, it is important that this regulation acts not only at the level of declarations and recommendations, which are sources of "soft law", but also obliges states after their ratification to include relevant provisions in national legislation and ensure their implementation (Chernyshev, 2010).

At the level of the Council of Europe, in 2012, the Committee of Experts on the Rights of Internet Users (MSI-DUI) was established to study the possibility of adapting rights for their use on the Internet. This committee was active from July 6, 2012, to December 31, 2013. Therefore, in our opinion, the activity of specially authorized institutions in the field of privacy on the Internet is necessary. Therefore, in our opinion, a possible option is the creation of an international institution (at the level of the Council of Europe in the context of regional protection of the human right to privacy), with powers to control private information, processing, and distribution, creation and improvement of personal data, improvement of modern legislation on privacy in the Internet, control over the activities of states. It is possible to empower this body to consider individual complaints about violations in this area. To increase the effectiveness and influence of this body, it is necessary to create its branches and representative offices at the level of member states (Shadrin, 2019).

Therefore, the task of the European Union is to take into account the views of all parties involved throughout the EU to establish standards that do not conflict with the expectations of the majority of member states, excluding violations of their rights and legitimate interests. In addition, the European Union must regularly engage in cooperation between all states, monitoring changes in social relations, and in the field of privacy, which must be reflected in legal regulation. The problematic nature of this process is that the European Union plays a supranational role and it is practically impossible to satisfy the needs and interests of all stakeholders involved in the privacy and protection mechanism. At the current stage of the development of European society, the process of making significant changes and additions to regulatory documents aimed at protecting private life was adopted earlier. This process is associated with high rates of scientific and technical progress, the in-

troduction of information technologies in all spheres of life, as well as the globalization of the information space, and therefore the development of society as a whole.

5. Conclusions

The global epidemic and related pandemic of COVID-19, caused by the SARS-CoV-2 coronavirus, which rapidly spread throughout the world, has given rise to the continuous work of the best scientists in the field of medicine and virology on vital questions – the nature of the virus and effective ways to overcome it. At the same time, in addition to medical issues and problems, the situation that has developed has revealed several legal problems that are related to the peculiarities of the implementation of several human rights in the conditions of an emergency. Thus, the most discussed and debatable issues are related to the provision of human rights at the constitutional level, in particular, the right to free movement and choice of place of residence, the right to a family (to enter into and dissolve a marriage), the right to education, etc. But there is one generally important and perhaps the most discussed problem in the legal sphere of today – the problem of personal data protection. The vital need to collect and process personal data of sick persons to ensure control, isolation, contact tracing, and as a result to contain COVID-19 has arisen not only in each country but also in the whole world as a whole. Governments and other organizations today are taking unprecedented (and sometimes fundamentally new and cutting-edge) measures to contain COVID-19, which, according to current legislation, may include, among other things, the collection and private information processing. The result of such manipulations with personal data can be unpredictable. Since the mechanism of collecting and processing personal data is far from all countries have received proper and decent legal regulation.

The right to private information inviolability, as an integral part of the complex structure of human rights, is a socio-historical phenomenon. Analyzing the progressive experience of European legislation and law enforcement, it can be noted that European normative acts have become a global standard implemented by non-European countries. This is explained not only by the universality of their norms but also by the fact that the ideas contained in them are the result of an analysis of the accumulated practical experience of European countries regarding the application of the principles established by previously signed international documents.

The right to privacy in today's digital world faces many threats and dangers: illegal distribution and extraction of personal data, cross-border movement, insufficient regulation of mechanisms to protect against violations, and the search for a balance between state interference in private information and public interests. It is currently difficult to ensure full protection of an individual from violation of his right to privacy on the Internet due to gaps in regulation and monitoring of possible violations of these "privacy" boundaries by other entities. That is why the European community faces the need to improve the legal regulation of this sphere of legal relations.

In general, the spread of the use of information and communication technologies in the conditions of a global pandemic leads to significant changes in all spheres of society. This requires a radical revision of the foundations of the legal regulation of novellas by the needs of the time and the creation of an effective human rights protection mechanism. The Republic of Kazakhstan, participating in the global information space, regularly faces the problems of legal regulation and protection of the sphere of private life from the negative impact of new information and communication technologies, as well as the pandemic. Due to the lack of domestic experience in solving similar problems, it will be advisable to turn to foreign practice. One of the most important conditions for the development of an open information society should be an effective legislative framework that takes into account the interests of all subjects of informational legal relations and creates a balance for their satisfaction. And the main thing in this process is to ensure the confidentiality of the individual since a person's lack of confidence in the effective protection of personal information will inhibit scientific and technological progress.

We believe that European standards serve as a guide for legal reform in the Republic of Kazakhstan, taking into account differences in legal traditions, systems, and structures while reflecting a collective understanding of the relevant structures of the law enforcement system. International standards can be used at the national level to facilitate in-depth evaluation leading to needed reforms. They can be used in the development of subregional and regional strategies. Globally and internationally, standards and norms are "best practices" that states can adapt to their national needs. EU legislation in the field of personal data is recognized throughout the world and is a kind of model that serves as a reference for other countries. Today, the modernized legislation reflects a high level of control and protection of personal data, and contains measures to counter threats associated with the ever-expanding possibilities of processing a huge array of personal data in the conditions of COVID-19. Therefore, the role of international, particularly European, standards in the field of privacy protection is significant. Thanks to

them, states orient their domestic legislation to the implementation of internationally recognized principles and rules.

References

Ablameyko M.S. (2018). Legal regulation of personal data taking into account the introduction of ID cards and biometric passports. *Journal of the Belarusian State University. Law*, 1: 14-20.

Chernyshev I.A. (2010). *Legal positions of the Constitutional Court of Russia and the European Court of Human Rights: genesis and mutual influence*. Tomsk: Tomsk State University.

Council of Europe Committee of Ministers (2016). Recommendation CM/Rec (2016) 5 (1). -- Retrieved from: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415fa.

Council of Europe (1950). Convention for the Protection of Human Rights and Fundamental Freedoms. -- Retrieved from 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 on the Protection of Individuals with regard to Automated Processing of Personal Data (Convention 108). -- Retrieved from: https://zakon.rada.gov.ua/laws/show/994_326#Text.

Council of Europe (2018a). About the roles and responsibilities of Internet intermediaries. -- Retrieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016808c6193.

Council of Europe (2018b). Modernized Convention 108+. Retrieved from: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf.

Dechesne F., Sears A. M., Tani T. and Hof S. (2018). A comparison of data protection legislation and policies across the EU Bart Custers. *Computer Law & Security Review*, 34(2): 234-243.

ECtHR, 'K.U. v. Finland. Application no. 2872/02' (HUDOC – European Court of Human Rights, 2 December 2008) -- https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-89964%22]} accessed 2 December 2008.

ECtHR, 'Uzun v Germany. Application no. 35623/05' (HUDOC – European Court of Human Rights, 2 September 2010) -- https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=003-3241790-3612154&filename=003-3241790-3612154.pdf} accessed 2 September 2010.

European Parliament (1995). Directive 95/46/EC. -- Retrieved from: https://zakon.rada.gov.ua/laws/show/994_242#Text.

European Parliament (2016). Regulation 2016/679. General Data Protection Regulation. -- Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj.

European Parliament (2016). Regulation of the European Parliament and the Council (EU) 2016/679. -- Retrieved from: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

General Assembly (1966). International Covenant on Civil and Political Rights. -- Retrieved from: https://zakon.rada.gov.ua/laws/show/995_043#Text.
Goddard M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, 59(6): 703-705.
Gracheva M.A. (2017). Features of the interpretation of the right to inviolability of private and family life, home and correspondence in European legal systems. *Modern Science*, 8(1-3): 8-15.
Ilyubaev A.S., Pleskachev D.V. and Kusainova U.B. (2021). Recommendations for ensuring confidentiality on the Internet. *NIR/S&R*, 1(5): 41-44.
Kashkin S. Yu. (2018). *European Union Law: Textbook for Academic Bachelor's Degree*. Moscow: Yurayt Publishing House.
Kazakh truth (2017). Internet and privacy of private life. -- Retrieved from: https://kazpravda.kz/n/internet-i-neprikosnovennost-chastnoy-zhizni/.
Komarov S.A. and Mytskaya E.V. (2018). Legal responsibility for violation of the legislation on personal data in the Russian Federation and the Republic of Kazakhstan. *Legal thought*, 1: 52-61.
Lozovaya O.V. (2015). Legislation of the Republic of Kazakhstan in the sphere of personal data protection: a comparative analysis with the law of the European Union. *Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan*, 1(37)*:* 128-133.
Macenaite M. (2017). From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation. *New Media & Society*, 19(5): 765-779.
Malgieri G. (2019). Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations. *Computer Law & Security Review*, 35(5): 127-135.
Mondschein C.F., & Monda C. (2019). The EU's General Data Protection Regulation (GDPR) in a research context. *Fundamentals of Clinical Data Science*, 1: 55-71.
Pankevich O.Z. (2018). The right to privacy: some current trends in the practice of the Strasbourg court. *Socio-Legal Studies*, 1: 23-30.
Parliament of the Republic of Kazakhstan (1995). Constitution of the Republic of Kazakhstan. -- Retrieved from https://online.zakon.kz/document/?doc_id=1005029.
Parliament of the Republic of Kazakhstan (2013). Law of the Republic of Kazakhstan "On personal data and their protection" -- Retrieved from: https://online.zakon.kz/Document/?doc_id=31396226.
Parliament of the Republic of Kazakhstan (2015a). Law of the Republic of Kazakhstan "On Access to Information" -- Retrieved from: https://online.zakon.kz/document/?doc_id=39415981.
Rustad M.L. and Koenig T.H. (2019). Towards a global data privacy standard. *Florida Law Review*, 71, 365.
Schwartz P.M. (2019). Global data privacy: The EU way. *New York University Law Review*, 94, 771.

Shadrin S.A. (2019). *Legal regulation of personal data protection in the European Union: genesis and development prospects.* Kazan: Kazan Federal University.
UN General Assembly (1948). Universal Declaration of Human Rights. -- Retrieved from https://www.un.org/sites/un2.un.org/files/udhr.pdf.
UN General Assembly (1966). International Covenant on Civil and Political Rights. -- Retrieved from https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.
UN Security Council (2011). Resolution 1973. -- Retrieved from: https://zakon.rada.gov.ua/laws/show/995_j33#Text.
Vabyshevich V.V. (2020). Experience of criminal law protection of personal data of Kazakhstan and Germany. *Fighting crime: theory and practice*, 1: 22-25.
Vedaschi A., & Lubello V. (2015). Data retention and its implications for the fundamental right to privacy: A European perspective. *Tilburg Law Review*, 20(1): 14-34.
Volchinskaya E.K. (2014). Place of personal data in the system of information of limited access. *Journal of the Higher School of Economics*, 4: 199-211.