Protection of personal data: balancing the interests of an individual and the state

Gulnar Aytzhanovna, Alibayeva[1], Serik Kozhanovich, Zhetpisov[2],
Alexey Vladimirovich, Boretsky[3]
[1]*D.A. Kunaev University of Transport and Law, Almaty, Kazakhstan, Doctor of Law, professor.*
[2]*Innovative University of Eurasia, Pavlodar, Kazakhstan, Candidate of legal sciences, assistant professor.*
[3] *Innovative University of Eurasia, Pavlodar, Kazakhstan, Senior lecturer*

ABSTRACT
Today, the right of privacy undergoes global rethinking not only in developing countries but also in developed countries with a stable democracy. Absence of a qualitative legal framework in existing and emerging technologies both at the international and national levels leads to multiple violations of the right of privacy.
Relations associated with the transfer of personal data and privacy protection, are subject to legal regulation by national and international standards. However, despite the apparent simplicity of the question, there is the problem of fragmentation of legal regulation of different states at the national level and the lack of specialized universal documents at the international level;
In the scientific article the legal regulation of personal data protection in international legal acts and national legislations of states are examined, as well as adoption of positive international experience to improve the legislation of the Republic of Kazakhstan.
KEYWORDS*:* personal data, the right of privacy, protection of personal data, the national system of human rights protection, international legal standards of personal rights and freedoms.

INTRODUCTION

International law has not yet taken a single universal agreement which would comprehensively regulate all aspects of the right to privacy, the content of which is constantly expanded and refined. Regulation of this law, both at domestic and international levels is directly related to technology development, first in picture and sound, and then in the computer processing and transfer of personal data.
The right to privacy acts as cornerstone of modern democracy, it is one of the most fundamental and complex problems which faces the international community. In addition, its urgency is determined by reevaluation of the right to privacy itself, its "politicization", i.e. recognition of its connection with the category of political freedom, its acknowledgement as law in force in respect of the citizen and the state. For many Western countries the concern with protection of privacy is stronger than the fear of terrorist attacks. However, recent events have forced most countries in Europe and the United States to resort to harsh methods of combating terrorism, even the legalization of state intervention in the private lives of citizens. Some restrictions on wiretapping, censorship of e-mail and tracking of banking operations.
On the background of the world events, we believe that tightening of the anti-terrorism legislation should not become an excuse for restricting civil liberties and departing from the values lying at the basis of international law.
This will be indicated in the UN General Assembly resolution on the right of privacy, which is being accepted these days. This is the only document of international scale in the field of privacy over the last 25 years, and it is expected to mark a "breakthrough" in the field of personal data protection in the global community.
Focus on human rights issues in general and the right to privacy specifically is characteristic for both domestic and foreign authors. Therefore, when writing the article the common works of scholars were analyzed such as: Jean C. O'Connor [1], Scot Cunningham [2], Kiran Mehta [3], Timothy J. Brueggemann [4], I.L. Petruhin [5], L.O. Krasavchikova [6], G.B. Romanovsky [7], O.E. Kutafin [8], M. Wugmeister [9], W. Steinmuller [10] A.V. Boretskii and S.K. Zhetpisov [11], A. Westin [12], Louis D. Brandeis, S. Warren [13], etc. The purpose of this study is a systematic and comprehensive study of the international legal problems of legal registration, implementation and enforcement of the law on human rights to privacy.

RESEARCH METHODS

Methodological framework of this research is composed from common scientific methods of knowledge (dialectical, formal-logical, and structural-functional) and special (historical-legal, comparative legal) methods.

RESULTS AND DISCUSSION

The urgency of protecting the right to privacy is increasing every year. But the events of recent decades, associated with the most massive terrorist attacks, technological progress, the desire to ensure national security, have led to serious limitations in the area of privacy.
Governments of many countries launched hundreds of key policy initiatives that threaten the basic elements of citizens' private lives. Among them are proposals for establishment of archives and data

banks, which include:

- Biometric data (e.g. national databases of DNA or fingerprints of citizens);
- Data of migration;
- Financial data of all citizens and residents (this tendency leads to the conclusion that all citizens, regardless of their legal status, are under suspicion);
- Scans of the irises through the public sector;
- Various systems of real time monitoring.

In addition, serious work of creating a global information exchange in the framework of international agreements and elimination of anonymity in the cyberspace is conducted.

Due to the increased terrorism threat the growing number of countries introduces the practice of collecting fingerprints. Initially, this procedure had become necessary for the entry into such countries as USA, UK and Japan. Now, from the November 14, 2013 biometric data (fingerprints and biometric photo) will be collected to apply for a Schengen visa, in all the Schengen countries representative offices in Kazakhstan. At the core of this innovation lies "joining the diplomatic missions in Central Asia to "Visa Information System" of the Schengen States (Visa-Informationssystem (VIS))" [14].

In addition, the personal data is collected, distribution of which due to technical malfunctions or other causes, can severely damage the private lives of many citizens. For example, the international human rights organization "Privacy International" has criticized Britain for the world's largest network of surveillance cameras (about 4 million). In addition, according to the head of "Privacy International" Simon Davies, a recent loss of the disk containing the personal data of 25 million people in the United Kingdom demonstrated how high is the risk of storing personal information in centralized national databases [15].

Programme of the U.S. intelligence electronic surveillance, reported by the ex-CIA officer Edward Snowden, also raise serious concerns about the protection of privacy in the United States and other developed countries.

This is confirmed by data published by the international human rights organization "Privacy International", which monitors compliance with the right to privacy in the different countries of the world. For the annual "International rankings of privacy" they attract more than 200 experts from around the world and evaluate about 100 countries.

The report's authors note the general deterioration of the right to privacy protection in the world. In most developed countries there is a tendency to scale back the rights to privacy and guarantees of confidentiality, and the degree of government control has reached unprecedented levels. At the same time, the laws that are supposed to protect the privacy and liberty have many reservations that allow authorities to invade privacy. Researchers believe that a number of states cannot take special legislation; however, they have taken steps aimed at establishing additional protection of privacy and personal data. [9]

The above, allows stating that the world today faces the global challenge – to ensure a balance between the interests of the people and the interests of the state and businesses that collect and use personal data of these people to maintain the security of the state and business. Scientists examining questions of necessity and urgency of further research in the field of personal data protection, state the appearance of a new branch of law: the right to electronic data processing - "close relative" of the right to freedom of the media - media rights [10].

Based on the analysis of regulations of foreign countries and international acts, it can be stated that the right to privacy is considered in conjunction with other related rights, and it is here that the privacy can be traced to the personal data. They can be viewed as both the single-order right and the elements of the right to privacy.

In favor of the versatile concept of "private life" indicate scientists' research. In particular, A. Westin talks about the four forms of privacy. The first - "privacy" that is a condition in which a person is relieved from observation by others. The second - "intimacy", closed communication, suggesting voluntary maintaining of a contact with a few individuals. Third - "restraint", i.e., the existence of a psychological barrier between the individual and the people around him. Fourth - "anonymity", the possibility of a separate existence in the social environment [12].

The most interesting is the constitutional practice of the United States, having a long and instructive experience in the field of human rights. American legal science highlights "privacy" - a basic human right that belongs to everyone. In the 90-ies of the XIX century, the future U.S. Supreme Court Justice Louis Brandeis formulated the concept of privacy, which meant that every person has the right to be left alone [13].

In other words, American lawyers define privacy as a human right to control and protect their "living space" and "their personality" from physical intervention or information publishing.

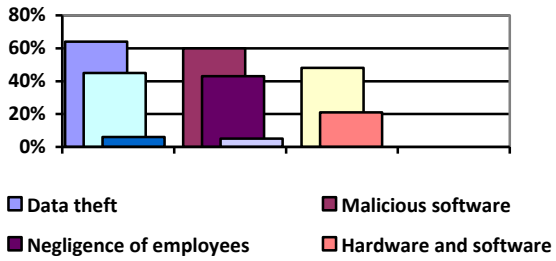
It is known that privacy – the most significant and fundamental human right, is enshrined in specialized agreements, governing this sphere of social relations in greater detail, in addition to the basic agreements that set out safeguards to protect personal data – Universal Declaration of Human Rights of 1948 (Art. 12) [16], the International Covenant on Civil and Political Rights of 1966 (Article 17) [17], the European Convention for the Protection of Human Rights and Fundamental Freedoms of 1950 (Article 8) [18], the CIS Convention on Human Rights and Fundamental

Freedoms [19]. Among those specialized agreements are the Directive of the European Parliament and the Council of Europe 95/46/EC "On the protection of individuals in regard to the processing of personal data and the free circulation of these data" [20] and the Directive of the European Parliament and of the Council of Europe 2002/58/EC of 12 July, 2002 [21]. Both Directives relate to the protection of personal data and the protection of personal data in the electronic communications sector, govern the use of personal data and provide guarantees of privacy in the telecommunications sector.

Despite this, there is a number of conditions and factors that create a potential or actual risk of a breach of confidentiality, availability, and (or) the integrity of the information.

According to statistics in relation to these threats, the following data can be included (according to the studies conducted in 15 countries by "InfoInter" company);

1) Data theft - 64%;
2) Malicious software - 60%;
3) Hacker attacks - 48%;
4) Spam - 45%;
5) Negligence of employees - 43%;
6) Hardware and software failures - 21%;
7) Theft of equipment - 6%;
8) Financial fraud - 5% (Figure 1).



Due to the fact that nowadays there are many ways and means to intervene in the private life of an individual, by wiretapping, setting hidden cameras, etc., owing to the excess interest of the media in public persons, the need for qualitatively new legal acts, based on the principles of legality, justice, equality before the law, humanism, taking into account the rapid development of technology became visible.

Protection of personal data - is one of the priority areas for improving the present international and national legislation. This is evidenced by many facts of judicial practice. Here are some of the most striking examples.

- The European Court of Human Rights (ECHR) has rejected the appeal of Austrian companies publishing newspapers Kronen Zeitung and Kurier, against the decision of the local courts for recovery of the non-pecuniary damage for publication of the name of the sexual violence victim. In the complaint, the applicants relied on Article 10 (freedom of expression) of the European Convention for the Protection of Human Rights and Fundamental Freedoms. However, the ECHR has confirmed the presence of violations of the victim's right to privacy in the journalists' actions, namely, the right to protection of personal data.
- In Canada, the Supreme Court upheld the requirement for judges to ban publishing information revealing the identity of victims of sexual violence. However, journalists are allowed to attend the court sessions and cover the course of the proceedings.
- A similar position is held by Britain. The National Code for Victims of Crime of 2006 stipulates that before publishing any details of a case in the media, the police, transmitting the case materials, and the media themselves, must obtain the consent of the victim, both during and after the process. The only thing that can be reported is the victim's age and gender, but the court may order the media not to divulge any personal information about the victim at all, including its address, school name, the names of friends and relatives.
- Press council in the Netherlands, examining the case against the newspaper "Eindhovens Dagblad", stressed that the decisive argument is the fact of causing undue additional harm and the ability to anticipate and avoid it. Council condemned the mention of the victim's name before establishing of her identity, which put her family in a difficult position, though it could have been foreseen and her name from the article could have been deleted. Thereafter, the Department of Justice has developed a series of acts for employees about precautions when transmitting information to the media. One of the instructions prohibits mentioning the names of crime victims, except when they have no objections.
- Ambiguously this issue is resolved in the United States. In two cases, to protect the privacy interests the court assumed that since the information was obtained by journalists from public sources, there is no reason to prosecute them. In case of "Cox Broadcasting" the name of the rape victim had been mentioned in the warrants for arrest of a suspect, which are public information. In the case of "Florida Star" - in the police report, that was located in the sheriff's Office of public relations and the media. Saving this information was the responsibility of the public authorities. The Court also took into consideration the traditional public interest in such cases. In addition, U.S. law specifically provides that the publication should not be humiliating for a person, while the fact of the publication is not an offense. At the same time, in some States, the court may order the non-disclosure of personal information about the victim, if the corresponding application was filed. The U.S. Supreme Court has ruled in 1979 that if the media "by lawful means extract truthful

information about matters of public importance, the authorities can not punish them for publishing this information if the need to protect the best interests of the state is not concerned" [22].

In many countries (Belarus, Spain, Sweden, Sri Lanka, and others), prohibitions for disclosure of the victim's personal data is not established in the law but in the Code of Professional Ethics for Journalists. Disclosure of names is allowed with the consent of the victims, if giving full and accurate information is necessary.

In the Republic of Kazakhstan the Law of the RK № 94-V "On personal data and protection of them" was adopted, on May 25, 2013 [23]. In accordance to the paragraph 1 of Article 31, the law comes into force six months after the first publication. Thus, the law was enacted on November 25, 2013. The law is based on one of the fundamental human rights: the protection from the privacy interference. According to the law the procedure for handling personal data is defined and fixed. The law provides a legal framework to protect the rights and freedoms of a human and citizen in the processing of their personal data, including the protection of the rights to privacy, to personal and family privacy. This, in particular, introduced the notions of personal data and determined the order of their treatment, basics of organizational and legal support of legal persons and public authorities' activities, organizing and carrying out the processing of personal data of individuals.

The analysis of the national legislation demonstrates the need to set a balance between privacy and freedom of expression. First and foremost, it must be done at the international level. The conflict between these two rights occurs when privacy is not interpreted as a basic human right (including the right to anonymity), but as a limitation to the freedom of expression. Participants in such disputes - individuals seeking compensation for damage caused to their interests by giving the facts of their privacy unwanted publicity. In the consideration process of such cases compliance of the publication to "public interests" is determined. That is, making the decision to impose such restrictions, the courts need to understand how it will affect the media's right to freedom of expression, to publication of information that meets the interests of society as a whole, to ensure the transparency of the justice.

For absolute and complete realization of the proclaimed principles of international law in the field of human rights and freedoms it is necessary to create effective legal mechanisms that would support human rights. Society should aim to ensure that laws guaranteeing human rights and freedoms operate automatically, regardless of one's will or arbitrary subjective understanding, without regard to the political forces in power and to the state system. In this connection, it is recommended to pay attention to the following problematic aspects:

- Analysis of the international legal instruments shows that the right to privacy is formulated in very general terms. At the same time, there is neither any universal, nor regional treaties clarifying the rule on the right to privacy. However, the need for specification of this right in international law is already overdue.
- An important problem in international law is the ratio of different human rights when the basis for the intervention of one person into the privacy of the other is a legitimate desire of the first to implement their own right. The most common example is the collision of the right to information and freedom of expression with the right to privacy.
- The right to privacy in the national legal systems, as well as other universally recognized human rights, can be properly interpreted and applied only when it is enshrined in the international instruments. Since the right to privacy is not an established concept, its interpretation, protection, restriction in different countries is very diverse.
- Analysis of the national legislation and practice, suggests that currently the vast majority of states are facing a serious dilemma: to ensure its own security and human rights on the basis of compliance with the UN Charter, or to deal effectively with terrorism and other violations of human rights by unilateral actionы with the use of armed force and further limitation of fundamental rights and freedoms of a human and citizen.
- Respect for the principle of proportionality between the limitations of rights and freedoms is an essential condition of reasonableness, adequacy and legality of measures taken by the government in the fight against terrorism, therefore it is necessary to develop common principles of conceptual approaches to formation of the theory of restrictions on human rights and freedoms, to be followed by the state during application of such response, compelled and exceptional in its content measure.

All the above questions suggest the direction of further improvement of the international standards intended to ensure the right to privacy. It should be remembered, however, that there is no international standard giving all the answers and can not be considered as recipes for all occasions. Article 17 of the Covenant, and article 8 of the Convention contains the idea that for implementation of these standards it is necessary to adopt domestic legal acts at the level of laws, revealing the general concepts used in these articles. For example, paragraph 2 of Art. 17 provides that everyone has the right to protection of the law from the corresponding attacks. But the interpretation of standards in national legislation also can not solve all problems. A more detailed interpretation is possible only at the level of practice. Decisions of the European Court of Human Rights, general

comment made by the Human Rights Committee, interpreting the provisions of the Covenant, promote the adjustment of national legislation and domestic jurisprudence. For example, in the decisions of the European Court of Human Rights there can be traced quite clear criteria for lawful wiretapping of telephone conversations [24]. However, the legislation, judicial and administrative practice of various countries in ensuring the right to privacy could be much closer to a common denominator, if universal standards in the area were specified.

CONCLUSIONS

We believe it is necessary to develop an internationally universal document of non-interference in privacy, which could serve as a starting point for improvement of the national legislation to protect the right to privacy.

REFERENCES

1. O'Connor Jean C. Informational privacy protections: Do state laws offer public health leaders the flexibility they need? Ph.D. The University of North Carolina at Chapel Hill 2007;pp:138.
2. Cunningham Scot. Protecting privacy in recorded conversations. M.S. Northern Kentucky University 2007;pp:101.
3. Mehta Kiran. Protecting location privacy in sensor networks against a global eavesdropper. M.S. The University of Texas at Arlington 2008;pp:70.
4. Brueggemann Timothy J. Is information technology reducing privacy: A study of protecting Personally Identifiable Information. Ph.D. Capella University 2009;pp:169.
5. Petruhin IL. Personal secrets (man and power). Moscow: Lawyer 1998;pp:212.
6. Krasavchikova LO. The privacy of citizens under the protection of the law. Moscow: Legal Literature 1983;pp:158.
7. Romanovsky GB. The right to privacy. Moscow: MZ-Press 2001;pp:312.
8. Kutafin OE. Inviolability of the constitutional law of the Russian Federation. Moscow: Lawyer 2004;pp:354.
9. Wugmeister M. Privacy law: International data protection developments. Twelfth Annual Institute on Privacy and Data Security Law. Practising Law Institute 2011;pp:559.
10. Steinmuller W. Law Political questions of law and administrative automation in Germany. Datenverarbeitung im Recht 1974;1-2:106-108.
11. Boretsky AV, Zhetpisov SK. Combating Human Trafficking: Cooperation of the Middle East Countries and the Republic of Kazakhstan. Middle-East Journal of Scientific Research 2013;14(11): 1422-1427.
12. Westin A. Privacy and Freedom. London: The Bodley Head 1970;pp:488.
13. Brandeis Louis D, Warren Samuel. Right of Privacy. Harvard Law Review 1890;pp:193.
14. The fingerprints of Kazakhs will be required for a Schengen visa. 2013. http://interfax.kz/?lang=rus&int_id=10&news_id=8825.
15. Privacy is under threat in most developed countries. 2008. Centre for Humanitarian Technologies. http://gtmarket.ru/news/state/2008/01/06/1562.
16. The Universal Declaration of Human Rights. Adopted in resolution 217 A (III) of the UN General Assembly on December 10, 1948. http://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml.
17. International Covenant on Civil and Political Rights. Adopted in resolution 2200 A (XXI) of the UN General Assembly on December 16, 1966. http://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml.
18. Convention on "Protection of human rights and fundamental freedoms." Concluded in Rome on November 4, 1950. http://echr.ru/documents/doc/2440800/2440800-001.htm.
19. Convention of the Commonwealth of Independent States "The Rights and Fundamental Freedoms." Enclosed in Minsk on May 26, 1995. http://www.zakonprost.ru/content/base/14221.
20. Directive 97/66/EC of the European Parliament and of the Council of the European Union concerning the use of personal data and the protection of privacy in the telecommunications sector. Adopted on December 15, 1997. http://www.eos.ru/eos_delopr/eos_law/detail.php?ID=59637&SECTION_ID=671.
21. Directive 2002/58/EC of the European Parliament and of the Council of the European Union in regard to the processing of personal data and the protection of privacy in the electronic communications sector. Adopted in Brussels on July 12, 2002. http://base.consultant.ru/cons/cgi/online.cgi?base=INT; n = 50258; req = doc.
22. Balance between the rights to privacy and freedom of expression. 2012. http://zakon.ru/Blogs/OneBlog/1906.
23. Law of the Republic of Kazakhstan "On personal data and protection of them" Adopted on May 21, 2013. http://online.zakon.kz/Document/?doc_id=31396226.
24. Entin ML. International human rights guarantees. Experience of the Council of Europe. Moscow: MNIMP 1997;pp:234-235.