SOCIAL SCIENCE AND HUMANITIES

Manuscript info:
Received June 24, 2019., Accepted June 19, 2019., Published July 26, 2019.

PERSONAL DATA AS THE OBJECT OF INVASION OF PRIVACY

Kubenov, Gizat Manapovich
Doctoral student
Varna Free University "Chernorizets Hrabar"
gizat_1985@mail.ru

http://dx.doi.org/10.37057/2521-3253-2019-7-2

Abstract. The article considers the genesis of the personal data institute in the law of foreign countries. Special attention is attached to the problems of protecting personal information in the context of information environment and globalization. It is substantiated that personal information and data compose the significant element of the right to inviolability of private life. It is recommended to examine the best foreign practices in the field of the personal data protection and integrate them into the national human rights machinery.

Key words: personal data, right to private life, personal data protection, transborder transfer of data, information, information society.

Recommended citation: Kubenov, Gizat Manapovich. PERSONAL DATA AS THE OBJECT OF INVASION OF PRIVACY. 7 European Journal of Research P. 28-36 (2019).

Introduction:

The Republic of Kazakhstan, in the course of its development in line with the globalization and informatization processes, has faced new challenges of securing the inviolability of private life. But the study of these issues has not been adequately reflected by Kazakh legal science and practice, despite of their today's urgency. This is conditioned by the fact of Kazakhstan having no legal traditions of securing the inviolability of private life, which is calling for addressing the foreign countries' best practices on such right protection that may be helpful to the national legislation and law enforcers.

The intensive scientific and technical progress in the environment of the information space expansion and introduction of the information technologies into our day-to-day life, have resulted in new challenges and threats to the modern society and government.

First, the risk of the non-sanctioned collection, procession and dissemination of personal information provokes the gradual loss of the autonomy of the individual's life. Denying the absolute nature of the individual's autonomy from the society and state, we nevertheless believe that it should rely on just and optimal balance of public and private interests.

Second, the states' concerns on the increased terrorism and violate extremism threats, as well as increased efforts and development of new methods for combating them, resulted in legalization of the state's interference in the citizens' private life. Some restrictions on the telephone tapping, surveillance of mails, tracking of bank transactions have been already lifted; unique personal identifiers and biometrical data are introduced. At the world trends background we think that the counter-terrorist policy and toughing the anti-terrorism legislation must not become an excuse for constraint of the civil freedoms, whereas the respect of the human rights standards should become the priority number one.

Third, the continuing emergence of the new information and communication technologies, along with the more sophisticated methods of violating privacy, results in the imbalance between the interests of an individual, society and state, since the modernization of legal nature and content of such powers is needed, with the inclusion of new elements serving for the effective mechanism for the human personal life inviolability.

The main object of the issues raised by the article is the comparative law study of protecting the personal data institute in the context of the human right to violability of private life.

Research methods

The study is based on the materialistic dialectic approach to the research subject as the universal method for understanding reality in its natural historical development. The problem study was also based on the set of epistemological methods and techniques, including the complex analysis and set of common and special scientific methods of inquiry. The comparative study is one of the main methods used for this article purposes.

Results and discussion

The use of the 'personal data' category in the legal science and legislation is conditioned by the idea of securing private life in new information society, where the technologies threaten privacy. Such threats encroach on the information free circulation and are reflected in its illegal collection, storage and use. Due to the information space globalization, such threats go far beyond the national security sector. Thus, the mechanism for preventing the illegal use of information plays significant role in the international information policy.

Following M.V. Bundin, it is the desire to ensure the adequate protection of an individual from the information threats that resulted in the idea for controlling the traffic of the individuals' information, i.e.

personal data, by positioning them as a particular type of information to be protected [1, p. 14].

The study of such aspect of the private life inviolability as the personal data protection requires us to pay attention to the process of this institute emergence and performance in foreign legislation, which was the first to regulate it and now is providing guidance to the Republic of Kazakhstan due to the great digital gap between the developed and developing nations.

Emergence and development of the studies, focused on the personal data protection, are conditioned by the dynamics of the information and telecommunication technologies and, therefore, entering the information era and forming the information society by the leading countries.

Legitimization of personal data served for the study of this legal phenomenon by different judicial sciences, i.e. general theoretical, special judicial, applied, sectoral ones etc. At that, all of the sciences, despite of their personal specifics, address different aspects. That is why the "personal data" term is used in a different meaning by different scientific communities.

However, we are concerned on the legal implementation in order to be able to investigate the judicial nature of this phenomenon with respect to the private life inviolability. That is why the "personal data" term will be defined through the analysis of the international and foreign legal acts addressing this definition.

Europe and the USA can be fairly regarded the founders of the relevant regulations. It is there that in the 60's of the last century were adopted the first legal acts regulating the personal data protection.

The researchers are unanimous in the law "On the personal data protection" of the Hessen Land in FRG of 1970, being the first legal source for the personal data regulations [2, p. 625-627].

Sweden and Austria are also regarded as the pioneers in the personal data protection, provoked by the country's computerization. Denmark, France, Great Britain and the others took the same road.

In 90's the Eastern Europe countries joined the process. The adoption of legal acts in this sector was accompanied by the development of the law on protecting the inviolability of private life.

Hungary adopted the law "On protecting the personal information and access to the information of public importance" on November 10, 1992.

The Republic of Bulgaria has a significant set of legal acts in the sector of information relationships in general and personal data protection in particular. In 2000 the law "On access to the personal data" [3] was adopted; in 2002 - the law "On protecting personal data" [4]; in 2018 - the law "On cyber security" [5].

In general, measures taken by the European governments with respect to the personal data protection can be regarded as quite progressive, timely and humane. However, it should be presumed that the progress of their

implementation in the European Union remains uneven, as well as accumulation of the best relevant practices and policies.

Considerable experience in regulating relationships in the personal data protection sector has been accumulated by the USA. Despite of the USA having no any act ensuring the full protection of private life, the set of its legal documents serves for the high level of its protection in different spheres. However, the USA's practice on the personal data protection has some disadvantages, which resulted in the USA remaining in the list of the countries failing to ensure adequate personal data protection.

The Canada's law "On the personal data protection" is quite interesting, too. It really works due to the effective mechanism for the personal data protection. What is important is that the Canadians themselves pay proper attention to the issues of collecting, storing and processing personal data. Sociological surveys illustrate the high level of the Canadians' literacy in respect of both their rights in this sector and mechanisms for protecting them. The law also imposes on the government the liability for the legality of collecting and storing data and control over the purposes on those [6, p. 53].

It is worth remembering that we are examining the foreign countries' legislation on the personal data protection in the context of its conformity to the European security standards. It is not random, since it is the European Union who is the holder of the best legal mechanism in the personal data sector.

Starting from 1998, the European Union countries set a course for creation of the unified personal data system. The European best practices on the personal data protection formed the basis of the Convention on the protection of natural persons in the automated processing of personal data ETS #108 of 1980 [7].

Being binding to the EU countries, the Convention #108 is applied to the data procession, run by both private and public entities, including courts and law enforcement institutions. It insures natural persons from any abuse, related to their personal data procession, at the same time trying to regulate the transborder personal data flows. As far as the data procession is concerned, the principles, declared by the Convention, address just and legal collecting and automatic processing of data for the purposes defined by the law. It means, the data must be not used for the purposes, incompatible with the initial ones, nor stored longer than needed. These principles must be also applied to the quality of data, i.e. their adequacy, relevance, non-excessiveness and certainty.

One more act, defining the personal data term, that should be mentioned, is the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data of 1995 [8]. Following article 2 of the Directive, "personal data" is any information about a natural person, whether identified or identifiable.

On 15 December 1997 the Directive 97/66/EC of the European Parliament and the Council concerning the processing of personal data and the protection of privacy in the telecommunications sector was adopted [9], offering the personal data definition and insisting on the regulations of the member countries' to be harmonized in order to ensure equal rights and freedoms protection level, in particular with respect to the private life inviolability at the procession of personal data in telecommunication sector, as well as free movement of such data, telecommunication equipment and services inside the Community.

Growing complexity of the relationships in the information technologies sector, law enforcement practice of the EU countries not meeting modern needs, regular law changes conditioned the modernization of the EU law on data protection. Many years of hard work on the improvement of the regulation of the personal data circulation and protection resulted in the Regulation 2016/679 of the European Parliament and the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General data protection regulation). GDPR (Brussel, 27 April 2016) [10].

The Regulation requires the EU countries to make relevant amendments to their laws on the personal data protection in order to synchronize them with it. It means European countries must bring their own laws in line with the Regulation #2016/679, which came into force on 25 May 2018, so that the common understanding would be reached and employed. Thus, the personal data definitions, as well as the entire conceptual framework, should be unified. For example, the Austrian law "On data protection" sets the "personal data" definition similar to that of the Regulation. The Bulgarian law "On the personal data protection" has been already brought in line with the Regulation.

The Regulation #2016/679 illustrates the common features of the EU countries' laws on data protection, and makes it applicable to the main rights protection in the context of economic and social problems of the digital era.

The EU countries' option for the tough regulation of dealing with personal data, is calling for the states to review their approaches for the purpose of compromise. However, such dialogue lays the foundations for further collaboration between states and organizations of all continents, aimed on establishing universal and generally accepted international standards.

Having acknowledged the unique and progressive nature of the European regulations on the personal data protection, we find it reasonable to implement them into the legislation of the Commonwealth of Independent States as an integrating organization, having adopted the Model law "On personal data" of 29 November 2018 [11].

When analyzing the foreign legislation and returning to the task of defining the "personal data" category we set above, we should note they are defined through the "information" category, as similar definitions are offered by the international legal acts. In particular the OECD Council recommendations for the Guidelines for protecting the inviolability of private life and transborder transfer of personal data (2013) define the "personal data" as any information attributed to a natural person ("data subject"), whether identified or identifiable [12]; the Convention on the protection of natural persons in the automated processing of personal data (1981) states the "personal data" is information with respect to a certain or identifiable person ("data subject") [7]; the Regulation 2016/679 of the European Parliament and the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data interpret the personal data as information related to whether identified or identifiable natural person [10]; the CIS model law of 29 November 2018 refers personal data to the information about a personality, i.e. the one that allows whether directly or indirectly identify a natural person (the personal data subject) or can be equated to him/her [12].

Therefore, the international and foreign legal acts apply the "personal data" definition to the information enabling us to clearly identify a person. It is the ability to identify a person that closely connects personal data with private life. That is why, the right to private life (privacy) as a theory of control over the information first of all means we call private the information, over which its owners would like to keep their control.

In other words, information about the person's private life, including personal data, is deemed confidential. Confidentially means its disclosure and leak must be prevented. Confidential information means the "not subjected to any publicity, discreet information" [13, p. 559].

The regime of the "information confidentiality" is a logical consequence of limiting the access to the information, conditioned by the need for a balance between the interests of a person, society and state.

Nowadays any society faces the need for the personal data confidentiality. Both theoretical and practical aspects of this problem need to be settled in the nearest future, as the threats to the personal data become bigger and more aggressive. This is illustrated by the analytical report of the "InfoWatch" Center: "In the 3d quarter of 2019, 648 cases of leak of the confidential information from the private and public sector all over the world were registered. 1.58 billion of personal data records were compromised in July-September of 2019. The high compromising volume in the 3d quarter of 2018 was delivered by the mega-leak in China: the contractor of the local communication companies stole up to 3 billion records. The biggest for the 3d quarter of 2019 leak of the users' data started at the beginning of September, when the security researcher had found on the Internet

unprotected data base of 419 million Facebook users' contacts. Probably, the compromised data warehouse belong to one of the companies specializing in data analysis [14].

The above mentioned statistics prove the extreme importance of and need for the personal data confidentiality. On the efficiency of the personal data protection in the course of collecting, storing and processing them very much depends the level of a person's trust to the information resources and the degree of his/her involvement in the informatization process.

The global Internet can be considered the most dangerous and commonly encountered source of the threat to the personal information. It is conditioned by the fact that exactly through this net a person enters into different social intercommunications, makes online shopping through various profiles (pages) and email (electronic mail box), which contain the person's personal data. Such accounts hacking may result in the loss of the person's data. We presume this aspect of the problem in question is extremely important. In most cases, the mass personal data leak to the open space or sale of data, or even sale of the company's client base, is provoked or executed by dishonest and irresponsible disadvantaged workers. Along with the listed causes, the risk growth is conditioned by the level of the employees' social and economic vulnerability, as well as the absence of the tough response to such abuses.

Special attention should be paid to the issue of the people's judicial ignorance in the field of information technologies. Following the experts, the citizens without questioning the possible consequences voluntarily disclose their personal data and give consent for their procession to the third persons [15, p. 38]. We think, this matter could be settled through the increase of the level of legal literacy in the field of personal information security, so that social networks users themselves could maintain the balance between confidentially and openness.

Having analyzed the European law making and enforcing practice, the scientists note that the European legal acts have become the world standard followed by the other countries. It is conditioned not only by their universal nature, but the fact the ideas declared by them base on the results of the analysis of the European countries' expertise on implementing the principles, stated earlier in the international documents [16, p.15].

Today, the national law is not the only regulator for the institute of the private life inviolability. The modern problems in this sector are characterized by their "supranationality" and transborder nature, conditioned by the development of transportation and means of communication, as well as emergence of the publicly available world information networks etc. Therefore, these problems settlement is not only the internal matter of individual countries, but should conform with the relevant international and regional legal standards. Such standards should define the content and scope of the right to the private life inviolability and its guarantee, as well

as the states' liabilities and forms of collaboration between the countries on this right execution in the framework both of the national law and international relationships. That is why the special accent is made by all countries, including the EU states, on the personal data protection.

In the environment of the development of the global information society, the information exchange all over the world has become more prompt, extensive and accessible, which is conditioned by the wide spread of the information and communication technologies. At that, on different electronic resources the huge information file, including that of a personal nature and sometimes containing private data, have been accumulated.

The dynamics of the collection and exchange of the big information flows entails the risk of violating the people's fundamental right to the personal data inviolability, in particular at their transborder transmission. Therefore, the role of the human rights machinery, serving for the balance between the privacy and free information exchange, is increasing.

The experts note that not all countries nowadays pay proper attention to the issues of securing personal data on relevant territories, which fact, undoubtedly, results in the emergence of additional barriers at the transborder personal data transfer [17, p. 114].

This gives rise to concerns on the fundamental human rights and private life inviolability, as the individual's right to his/her personal data protection is the key one in the open information society, where transborder data transmission is unavoidable. The continuous transborder relationships in the field of the personal data circulation moves their protection mechanism from the national level to the international one. That is why the need for relevant international legislation is increasing with each new spiral of the development of information technologies, globalizing the information processes. Such legislation unifies regulations and standards in the field of the personal data protection.

Conclusions

It can be resumed that in the modern world of open information the state is responsible for securing the private life inviolability. First, the state must own the relevant legislation, and take adequate measures for its real efficiency instead of remaining on paper. Second, the reliable mechanism for control over such right execution should be established, focused on the human person, its dignified and free of control existence as supreme values.

References

1. Bundin M.V. Personalnyye dannyye v sisteme informatsii ogranichennogo dostupa: Diss. ... Candidate of Legal Sciences: 12.00.13. - M., 2017. - 218 p.

2. Gesetz und Verordnungsblatt fur das Land Hessen. - 1970. - #1. - P. 760.

3. Закон за достъп до обществена информация of 22 June 2000 // https://www.lex.bg/bg/laws/ldoc/2134929408

4. Закон на Република България за защита на личните данни // https://www.lex.bg/bg/laws/ldoc/2135426048

5. Закон за киберсигурност of 31 October 2018 // https://www.lex.bg/bg/laws/ldoc/2137188253

6. Korovyakovsky D.G. Rossiysky i zarubezhny opyt v oblasti zaschity personalnykh dannykh // Ugrozy i bezopasnost. - 2009. - #3 (38). - P. 48-54.

7. Convention on the protection of natural persons in the automated processing of personal data (Strasbourg, 28 January 1981) (with amendments of 15 June 1999). https://online.zakon.kz/document/?doc_id=1034061#pos=0;0

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

9. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector. https://www.tgl.net.ru/files/infosafety/%D0%B4%D0%BA%D-66.pdf

10. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). GDPR (27 April 2016). https://online.zakon.kz/document/?doc_id=39559334#pos=1;-119

11. The CIS model law of 29 November 2018 "On personal data". https://iacis.ru/upload/iblock/f43/prilozhenie-k-postanovleniyu-48_9.pdf

12. The OECD Council recommendations for the Guidelines for protecting the inviolability of private life and transborder transfer of personal data (of 2013). // digital.report/rekomendatsii-soveta-kasayushhiesya-rukovodstva-po-zashhite-neprikosnovennosti-chastnoy-zhizni-i-transgranichnoy-peredache-personalnyih-dannyih/

13. Big legal dictionary. ed. 3, reviewed and amended. / Under the edit. of the prof. A.Ya. Sukhareva. - M.: INFRA-M, 2007. VI. - 858 p.

14. Tretiy kvartal: chislo utechek sokratilos, no oni stali opasneye. https://www.infowatch.ru/resources/analytics/digest/16916

15. Kryukova D.Yu., Mokretsov Yu.V. Aktualnyye problemy pravovogo regulirovaniya oborota i zaschity personalnykh dannykh v Rossii // Vestnik instituta: prestupleniye, nakazaniye, ispravleniye. - 2017. - #2 (38). - P. 34-38.

16. Kucherenko A.V. O garantiyakh prav sub'yektov pri osushestvlenii transgranichnoy peredachi personalnykh dannykh // Information law. 2009. #3(18). P. 14-17

17. Polyakova T.A., Khimchenko A.I. Aktualnyye organizatsionno-pravovyye voprosy transgranichnoy peredachi personalnykh dannykh // Pravo. Zhurnal of HSE. - 2013. - #1. - P. 113-122.