

ISSN 1563-0366
Индекс 75882; 25882

ӘЛ-ФАРАБИ атындағы ҚАЗАҚ ҰЛТТЫҚ УНИВЕРСИТЕТІ

ҚазҰУ ХАБАРШЫСЫ

Заң сериясы

КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ имени АЛЬ-ФАРАБИ

ВЕСТНИК КазНУ

Серия юридическая

AL-FARABI KAZAKH NATIONAL UNIVERSITY

KazNU BULLETIN

Law series

№3 (75)

Алматы
«Қазақ университеті»
2015



ХАБАРШЫ

ЗАҢ СЕРИЯСЫ № 3 (75)



ХАБАРШЫ
ВЕСТНИК
BULLETIN

3(75) 2015

25.11.1999 ж. Қазақстан Республикасының Мәдениет, ақпарат және қоғамдық келісім министрлігінде тіркелген

Күәлік №956-Ж.

Журнал жылына 4 рет жарыққа шығады

ЖАУАПТЫ ХАТШЫ

Ережепқызы Р., жауапты хатшы

(Қазақстан)

Телефон: +7727-377-33-36;

8-727-377-33-37 (ішкі н. 12-57)

E-mail: rose@mail.ru

РЕДАКЦИЯ АЛҚАСЫ:

Байдельдинов Д.Л., з.ғ.д., профессор

(бас редактор) (Қазақстан)

Кенжалиев З.Ж., з.ғ.д., профессор

(бас ред. орынбасары) (Қазақстан)

Сартаев С.С., з.ғ.д., академик (Қазақстан)

Тыныбеков С.Т., з.ғ.д., профессор (Қазақстан)

Ибраева А.С., з.ғ.д., профессор (Қазақстан)

Джансараева Р.Р., з.ғ.д., профессор (Қазақстан)

Усенинова Г.Р., з.ғ.д., профессор (Қазақстан)

Еркинбаева Л.К., з.ғ.д., профессор (Қазақстан)

Жатқанбаева А.Е., з.ғ.д. (Қазақстан)

Трунк А., профессор (Германия)

Монтекило С., профессор (БАӘ)

Бурхард Б., профессор (Германия)

Лисица В., профессор (Ресей)



ҚАЗАҚ
УНИВЕРСИТЕТІ
Б А С П А У Й І

Ғылыми басылымдар бөлімінің басшысы

Гүлмира Шаққозова

Телефон: +77017242911

E-mail: Gulmira.Shakkozova@kaznu.kz

Редакторлары:

Гүлмира Бекбердиева, Еркін Жайнақов

Компьютерде беттеген:

Айгүл Алдашева

Жазылу мен таратуды үйлестіруші

Мөлдір Өміртайқызы

Телефон: +7(727)377-34-11

E-mail: Moldir.Omirtaikyzy@kaznu.kz

ИБ №8886

Басуға 15.08.2015 жылы қол қойылды.

Пішімі 60x84 1/8. Көлемі 35 б.т. Офсетті қағаз. Сандық басылыс.

Тапсырыс №3514. Таралымы 500 дана. Бағасы келісімді.

Әл-Фараби атындағы Қазақ ұлттық университетінің

«Қазақ университеті» баспа үйі.

050040, Алматы қаласы, әл-Фараби даңғылы, 71.

«Қазақ университеті» баспа үйінің баспаханасында басылды.

© Әл-Фараби атындағы ҚазҰУ, 2015

Zhatkanbayeva A.Ye.

On the problem of protection of personal information

The article analyzes the concepts and different regulatory approaches to the concept and content of personal information. It accentuates the deficiencies of modern legislation on the status of personal information and their constituents. The article provides examples from practice confirming the existence of serious problems in the field of security of personal information. It also suggests actions on how to improve the domestic legislation.

Key words: personal information, personally identifiable information, information rights, privacy, confidential information, the constituencies of personal information.

Жатқанбаева А.Е.

Жеке мәліметтерді қорғау мәселесі

Мақалада жеке азаматтардың құрамы мен түсініктемелерінің түрлі нормативтік талаптары мен түсініктеріне талдау жасалынады. Жеке мәліметтер мен олардың субъектілерінің заманауи заңнамасының мәселелері назарға алынады. Жеке мәліметтерді қорғау саласындағы маңызды мәселелердің болуын нақтылаушы тәжірибеден мысал келтіріледі. Отандық заңнаманы дамыту бойынша ұсыныстар енгізіледі.

Түйін сөздер: жеке мәліметтер, жеке өмір, ақпараттық құқық, құпия ақпарат, жеке мәліметтер субъектісі.

Жатқанбаева А.Е.

К вопросу о защите персональных данных

В статье проводится анализ понятия и различных нормативных подходов к понятию и содержанию персональных граждан. Акцентируется внимание на проблемах современного законодательства о статусе персональных данных и их субъектов. Приводятся примеры из практики, подтверждающие наличие серьезных проблем в сфере охраны персональных данных. Вносятся предложения по совершенствованию отечественного законодательства.

Ключевые слова: персональные данные, частная жизнь, информационные права, конфиденциальная информация, субъекты персональных данных.

ON THE PROBLEM OF PROTECTION OF PERSONAL INFORMATION

Personally information is the information, the misuse of which may harm the dignity, honor, good name and reputation, as well as person's material and non-material wellbeing.

The Law «On personal information and its protection» from May 21, 2013 defines personal information as «information, relating to the specific subject or a subject that can be identified through this information, which was recorded in electronic, paper and (or) other tangible medium.» It is evident that the subject of the personal information is an individual to whom the personal information pertains. It should be noted that the Law does not differentiate between the types of subjects, including absolutely everyone independent of citizenship, gender, age and other characteristics.

According to the law, it takes the responsibility to «... regulate social relations in the field of personal information, and defines the purpose, principles and legal bases of activity relating to the collection, processing and protection of personal information» [1]. Consequently, this law must strictly regulate the fundamental ways in which the establishment, processing, and protection of personal information are regulated. Although, the law was adopted in 2013, there are many issues with its legal implementation. The majority of the major personal information database holders have already adopted internal regulations, rules and instructions regarding the establishment and storage of such databases.

It is worth noting that there are many such personal information database holders, which include governmental organizations, banks, various financial institutions, service providers and others.

The adoption of the law has not brought serious changes in the way the personal information is collected and preserved. However, the law has mandated the holders and operators of personal information to get subject's or their legal guardian's consent for the collection and processing of such information. The consent of the subject or the legal guardian must be authorized in writing, electronically or in any other way in which the privacy protection actions are used.

However, the domestic legislation happens to be very loyal to the owners of information systems and their operators. It can be concluded from the fact that the personal information is not part of the confidential information. Therefore, the Kazakhstani legislation has divided the personal information into the information for open

access and for restricted access; however, has not defined the boundaries of what is included in the restricted access.

If we refer to the foreign experience, we can note that in many European states for more than 25 years there has been a special institute of jurisprudence – institute of the protection of personal information. The purpose of this institute is to protect the personal life of an individual in the environment of automatization of personal information processing. More recent Constitutions, such as the ones of South African Republic and Hungary, have an addition to their Constitutions that addresses the rights to the security of personal information. In Article 11 of the legislation of the Russian Federation on «Information, informatization, and the protection of information» the personal information (personally identifiable information) is categorized as confidential information. Its collection, storage, use and distribution are allowed only with the consent of the individual to whom the information pertains based upon the judge's decision. Moreover, the Russian Federation has a law on «Personal information» from July 28, 2006 which regulates the restrictions on the circulation of such information.

Personal information is the primary component of an individual's confidential information, the scope of which is expanding though time. Nowadays, not only does it include the birth date, addresses, telephone number, but rather different identification codes and cyphers that must be protected by the government.

In the purpose of governmental regulation (social security, financial control, public and national security etc.), the unified informational systems are being adopted which in one or another way include personal information of the citizens. This is the particular intersection of the interests of the government and the personal privacy. Since the entry of the information on individuals in the information databases, resources and electronic documents, there is a need to discuss the personal information, and personally identifiable information.

Recently the problem of the personal information protection has exacerbated due to the changes in the economic mechanisms, as well as extensive automation of the data collection and processing of socio-economic information. The former has resulted in a number of new entities, such as legal entities independent of the government, which collect and process data. The latter has substantially simplified the process of copying, distributing and use of information of any nature, including the personal information. All of this contributed to

the emergence of a new kind of criminal activity – the theft and an illegal circulation of personal information. Since the inception of the worldwide web Internet, where the problem of identification of users still has been resolved, the cybercrimes have become widespread.

The objects of attacks are Internet resources, local computer networks of banks, large commercial companies, governmental and public organizations, but first and foremost, their databases.

Different kinds of confidential information in regards to citizens, including information on financial transactions, the identifiable settlement and payment data of electronic payment systems, the SIM card codes of radiotelephone public networks and others have turned out to be under the threat. Usually actions taken to obtain personal information are conduits to the future criminal activities.

The global community along with different governments clearly feels the negative impact of these incidents, which include direct financial losses, the breach of reputation and consequently, the loss of public's trust. The loss from the criminal turnover of personal information accounts for 20-25% of the total annual criminal activity.

During the III International Conference on «the Development of Information Security in Kazakhstan» in Astana experts highlighted that «Nowadays, the most desirable asset in the eyes of competitors, dishonest employees, and criminals is client's personal information. And what are the clients? It is us. Our mobile phone numbers, our WhatsApp, Skype are the tools used by criminals to earn money, by planning and conducting fraud, and fraudulent transactions. This information must be protected by any organization» [2].

In world practice, the scandals involving the leak of personal information are very common. For instance, one of the most recent scandals occurred in Denmark, where «Social Security numbers of approximately 900 Danish citizens became public on the Internet. ComputerCompany CSC, which is responsible for the preservation and protection of the data of government agencies, erroneously included the personally identifiable information into the 'Robinsonlisten' – the list of citizens who are protected from the email advertising and telephone marketing. During 51 minutes, when the database was in open access, the information was downloaded 18 times» [3].

In Germany, personal information security scandals are more often, and according to Special Forces «The personal information of 21 million individuals is sold in the black market. Deutsche Well

reports that initial investigations are held in the call-centers. The business magazine *WirtschaftsWoche* was offered to buy the bank account information of Germans for 12 million euros. As a sample, the editor received ‘demo-version,’ a CD with the information of 1.2 million people. Along with personal information, such as date of birth, the database included bank account information and their identification numbers, and some of them even have detailed transaction amounts in the accounts»[4].

At the end of 2014, the United States experienced a major leak of personal information. The major retail store TJX Cos reported that hackers for more than one and a half years had access to the payment information of clients who paid with debit and credit cards. Consequently, the hackers acquired 45.7 million card numbers. The experts from Gartner Company state that this leak has become the largest identity theft in the history of using plastic cards. Notably, the company’s executives found out about the theft two months ago, however decided to not publicize this information that is why it only became public today. According to the police, the initial suspicion occurred yearly in January of 2007, when the administration of the stores TJ Max, Marshall, and several other brands operating under the direction of TJX Cos reported that about 455,000 buyers in North America and the UK have complained that their personal data was stolen» [5].

Although Kazakhstan does not occupy the leading position, but it has also been involved in various scandals. For instance, the «a group of Russian hackers have broken into the database of the Special Forces of Kazakhstan, which contained the personal and work-related information of more than 130 million residents of Kazakhstan and other CIS states. In this database, along with the information from the Ministry of Internal Affairs and the Federal Special Forces there were confidential information and conversations from social networks such as V Kontakte, Odnoklassniki.RU, and other confidential information which has been collected for the past ten years. And to highlight the Special Forces’ failure, they posted all the secret information from the database for open access in the popular ‘National Data Search’ portal» [6]. Here it is already interesting that the federal forces of the Russian Federation have access to our personally identifiable information.

Personal information is regularly used by fraudsters. For example, the law enforcement services of the Republic of Kazakhstan repeatedly recorded cases of the use of personal information

(copies of identity cards and PIN) by bank employees to obtain mortgages in the names of certain citizens without their awareness. The same scheme is used for the sale of real estate, purchase of expensive goods and so on. Often the participants or direct executors of these schemes are people who have direct access to such data, information, and materials. Today, the telephone numbers are used to extort money in different ways, and so forth. Experts say that in 80% of cases, the prosecutors of such crimes are internal employees who have direct access to personal information.

In fact, the legislation of Kazakhstan has created all the conditions for the implementation of single database which would contain the personal information of all the citizens. In particular, the legislation has allowed the electronic information sources containing the personal data about the individuals to be legally regulated. The Law of the Republic of Kazakhstan «On Information» defines personal data as «information about facts, events, and life circumstances of an individual or information that allows identification of the individual» [7]. Article 13 of this Law identifies the legal regime of electronic information sources, containing personal information about individuals such as:

1. Electronic information resources, containing personal information about individuals, belong to the category of sensitive electronic information resources, obtaining, processing and use of which is limited to the purpose for which they were collected.

2. No person has a right to demand from individuals against their will the details of their lives, personal and family secrets, secrecy of correspondence, telephone conversations, telegraph and other communications with other individuals, including information relating to their origin, health, views, political and religious beliefs for the purpose of forming electronic information database or for any other purpose.

3. For electronic information resources containing personal data, keeping the confidentiality is required from the moment the data is presented by an individual to whom the data relates.

4. It is prohibited to use the electronic information resources, containing personal data of certain individuals for the purpose of harming their material and/or moral well-being, limiting their freedom and rights, which are guaranteed by the Republic of Kazakhstan [7].

However, these legal norms are not adequate to guarantee compliance with the law by all government agencies, individuals and organizations. In its most general form, the personal data, information may include:

1. Biographical facts;
2. The information about the marital status;
3. The information about the state of health;
4. The information on the financial status and on the estates owned.

Government Resolution from June 5, 2007 № 460 approved the list of individuals' personal data included in the state electronic information resources, which include:

1. Full name;
2. Transcription of name and surname;
3. Birth information: date of birth, place of birth;
4. Nationality;
5. Gender;
6. Marital status;
7. Data on citizenship: citizenship (previous citizenship), the date of acquisition of citizenship of the Republic of Kazakhstan, the date of loss of citizenship of the Republic of Kazakhstan;
8. Personal Identification Number (PIN);
9. Portrait image (digitized photograph);
10. Signature;
11. Legal address, date of registration (deregistration) of legal address;
12. The information from the identity document: document title, document number, date of issuance of the document; validity of the document, the authority that issued the document [8].

Meanwhile, different regulations define personal data differently. Thus, the Law of the Republic of Kazakhstan «On State Registration of Rights to Real Estate and Transactions therewith» from 26 July, 2007 include surname, first name and date of birth of an individual, the name and registration number of the legal entity as components of personal data. Concurrently, Code of the Republic of Kazakhstan «On Taxes and Other Obligatory Payments to the Budget» from 10 December, 2008 include the following in the personal data: 1) surname, first name and patronymic; 2) date and place of birth; 3) gender; 4) residential address; 5) the number of identity card or other document proving the identity of the taxpayer [9].

The list of personal data must comply with Clause 1, Article 19 of the Constitution of the Republic of Kazakhstan, which establishes the right of each individual to decide to indicate or not to indicate his/her national, party and religious affiliation. This right was intended to protect the citizens of Kazakhstan from the possibility of discrimination. So, Clause 2, Article 14 of the Constitution of Kazakhstan states: «No one shall be subjected to any discrimination for reasons of origin, social, official status, estate

ownership, sex, race, nationality, language, attitude to religion, personal beliefs, place of residence or for any other circumstances.» In this regard, we consider it necessary to legally prohibit the use of personal data revealing racial, national, ethnic, linguistic, religious or party affiliation, except for circumstance expressly provided by law.

Security of confidentiality of personal data requires a clear legal regulation, namely the establishment of a legal working regime. Given the importance and meaning of the institute of personal data and its role in a person's life at the moment, as well as the fact that its use is likely to cause substantial harm to the person, his authority, financial well-being, professional image, and so forth, the legal regulation of the circulation of such data should be done at the legislative level. In this regard, we consider it necessary to adopt the Law «On the personal data.» The same position is shared by many countries who have adopted special legislations.

When dealing with personal information, holders of personal data must ensure its safety and confidentiality. Circulation of data that constitutes personal information, as well as circulation of any other information, includes the collection, storage, processing, transmission, blocking, depersonalization and destruction. In addition, it is necessary to establish on the legislative level the list of reasons for the collection of personal data, in order to avoid its abuse. In our opinion, when dealing with personal following requirements and conditions data must be taken into account:

1. Personal data and information can be collected by specially authorized state bodies, as well as legal and physical persons on the basis of the current legislation of the Republic of Kazakhstan;
2. Personal data must be collected precisely for the purposes defined by the law and any other use must be prohibited;
3. The personal data should be stored for a fixed period of time, which should be determined based on the purpose and use of personal data;
4. The integration of personal data databases must be prohibited;
5. Use of personal data should be carried out in secrecy, keeping information from unauthorized access, destruction, leakage, disclosure, uncontrolled use, and its modification;
6. It should be prohibited to collect personal data of individuals or legal entities for the purpose of causing material and moral damage;
7. The individual must consent to share personal information willfully in his/her interest, and must be able to withdraw from the agreement.

8. Public databases created to provide information to citizens should collect the data only with the written consent of the holders. This data should be removed at any time at the request of the individual. Public personal information is the personal data to which access is granted with the consent of an individual to the public or to the member countries that are not subject to the confidentiality requirements in accordance with the national legislation.

9. Persons who have direct access to such confidential information may be subject to criminal, administrative and civil liability;

10. For analytical, statistical or other similar work all personal data must undergo the process of depersonalization, which are actions taken to

eliminate the possibility of identification of an individual.

11. In case personal original data on individuals converges, it is necessary to give them distinctive characteristics.

These requirements should form the basis for the confidentiality of personal data.

As guarantor of citizens' rights to privacy and confidentiality of personal data state must regulate and have control over compliance with the following requirements for the holders of personal data:

- Licensing of actions on personal data;
- Registration of personal data;
- Registration of personal data holders;
- Certification of information systems used for the processing of personal data.

References

- 1 Law of the Republic of Kazakhstan from May 21, 2013 № 94-V «On personal data and its protection»
- 2 If Kazakhstan does not protect personal data, its manipulation will become the norm // <http://kapital.kz/gosudarstvo/34888/kak-zacshhitit-personalnye-dannye-kazahstancv.html>
- 3 In Denmark – the scandal with the leakage of personal data of nearly a million citizens // <http://www.svoboda.org/archive/radio-svoboda-news/latest/16564/16564.html?id=25445415>
- 4 In Germany, the scandal erupted again with the theft of personal data of millions of citizens // <https://xakepy.cc/showthread.php?t=45392>
- 5 The largest personal data theft occurred in the United States <https://xakepy.cc/showthread.php?t=25472&s=2d611667cd2dc5f6d826dd8bc577129f>
- 6 Personal data of all citizens of Kazakhstan and the CIS were in the public domain on the Internet // <http://www.news-kz.com/>
- 7 Law of the Republic of Kazakhstan «On informatization» from January 11, 2007 №217-III LRK// Information system «Paragraph»
- 8 The list of individuals' personal data included in the state electronic information resources. Approved by the Government Resolution from June 5, 2007 № 460 // Information system «Paragraph»
- 9 Law of the Republic of Kazakhstan «On taxes and other obligatory payments to the budget (the tax code)» from December 10, 2008 // Information system «Paragraph»