LEGAL FRAMEWORK FOR THE PROTECTION OF PERSONAL DATA IN THE REPUBLIC OF AZERBAIJAN AND THE EUROPEAN UNION

AYSEL Hacıyeva - Baku State University, Law faculty, Doctoral student of Human rights and the right to information UNESCO department

UOT. 34.002
DOI: https://doi.org/10.71404/NP.2026.1.18

Personal information refers only to information about individuals. What is meant by personal information? Personal information means any information or set of information that identifies the person to whom the information belongs by various means. What information is specifically included in the scope of personal data? The article focuses on the explanation of these questions. Personal information is regulated by the Law of the Republic of Azerbaijan dated May 11, 2010 "On personal data". At the same time, there are other legislative acts that regulate in this area. The article examines the mutual analysis of the legislation of the Republic of Azerbaijan in this area with the legislation of the European Union in the first and second degree, the impact of EU legislation on the legislation of the Republic of Azerbaijan in this area, future prospects and relevant proposals. The purpose of the article is to study the regulatory trends in the field of personal data, international, regional, especially the European Union and the Republic of Azerbaijan, the legislative practice, to comment on existing gaps, to use EU legislation in a positive direction.

Key words: The right to privacy, personal information, biometric data, regulatory agencies, the right to privacy, the right to respect for private and family life.

Problem statement

The formation and rapid development of the information society, the electronicization of processes resulted in the 4th revolution. Such globalization necessitates the emergence of new legal relations, areas of law, the legal system to regulate these areas of information, information culture, information security, personal data market, privacy, Big data, etc., which have no full legal equivalent in our language. One of the new regulated areas is personal data and their protection. Samuel Warren and Louis Brandis, the first American scholars to lay the foundations for the right to privacy, the means of potential protection, and the importance of legal protection in general, argue that the right of every individual to respect his or her identity, religion, and should have the right, even the right to be alone. This area of law was reflected in international law before it was created and regulated by the domestic legislation of any state. They note that intrusion into privacy is possible with one of four means:

- interference with private life and work;
- disclosure of shameful private facts to the public;
- Undesirable advertising of individuals; and
- Assimilation of name or similarity for financial advantages [3, p. 54].

The article's objective is to identify what is privacy, what is scope of privacy. How the privacy law is regulated in Azerbaijan Republic and European Union and how international law reflects them? "The right to privacy" was recognized as an international human right before it was enshrined in the constitution of any state. In the years World War II, when the human rights system was established, state constitutions protected only certain aspects of

the inviolability of private life. Such guarantees included, for example, the inviolability of the home and correspondence, and the classic problem of unfounded searches of the body. However, no state constitution provided a general guarantee of the right to privacy. Prior to the adoption of the Universal Declaration of Human Rights in 1948, local legal systems protected only certain aspects of what we now consider to be the right to privacy. Article 12 of the Universal Declaration of Human Rights of 1948 [16] and Article 17 of the International Covenant on Civil and Political Rights [15] do not protect the individual as necessary or insufficient. Article 17 states that no one shall be subjected to arbitrary or unlawful interference with his privacy, family life, housing or correspondence, and that his honor and reputation shall not be compromised. In the event of such interference, everyone has the right to the protection of the law.

Basic content

Personal information is inviolable and an integral part of your personal life. Legislation, which includes the inviolability of privacy, directly reflects the activities aimed at the protection of personal data. Article 8 of the European Convention on Fundamental Human Rights [17] and Freedoms provides for direct respect for private and family life. Except as otherwise provided by law, interference with the exercise of this right is permitted. Due to the application of this article, the Court's interpretation of the concept of private life states that private life cannot be described in its entirety. This concept is completely free in relation to each individual, and each individual can expand the component of this concept himself. The scope of the concept can also vary from individual to individual. This term is expressed in English as "Privacy" and is considered in our language as the equivalent of the word personal life. However, this concept is not fully covered. Because there is no legal or scientific explanation of this term. Privacy is a legal category in Anglo-Saxon legal systems that encompasses the privacy, privacy, and inviolability of the individual, as well as other concepts that may fall within this framework.

At the same time, in the Referendum of March 30, 2009, Article 32 of the Constitution of the Republic of Azerbaijan added the right to collect, store, use and disseminate information about a person's private life without his permission, and everyone has the right to access information about him. In addition, everyone has the right to demand the correction or removal (cancellation) of information collected about him that is inaccurate, incomplete, as well as obtained in violation of the law [1].

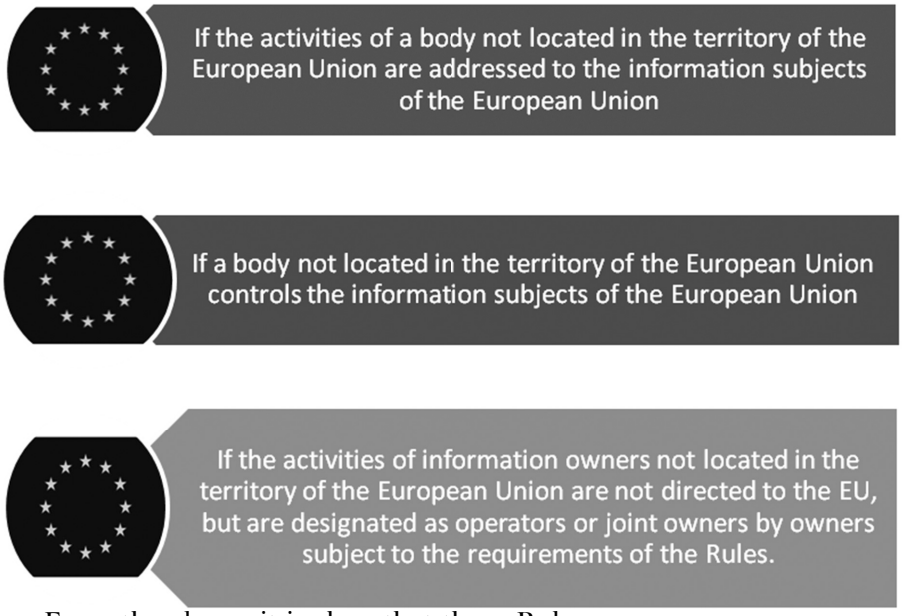
In 2016, the European Parliament and the Council adopted the European Union General Data Protection Regulations 2016/679, which came into force on 25 May 2018. The European Union's General Data Protection Regulation (GDPR) [12] is being adopted as a new global regulation. The Guidelines are based on and replaces the 1995 Directive on the Protection of Personal Data and the Free Flow of Such Data[10]. The rules aim to harmonize data privacy legislation in Europe to protect individuals involved in the processing of personal data and the free movement of such information. The Regulation apply to both EU citizens and non-EU individuals. In general, the Regulation promote many innovative innovations. According to the preamble of this directive, matters not regulated by this directive are governed by the following directives [12].

1.European Union on Privacy and Electronic Communications Directive (2002) [11].

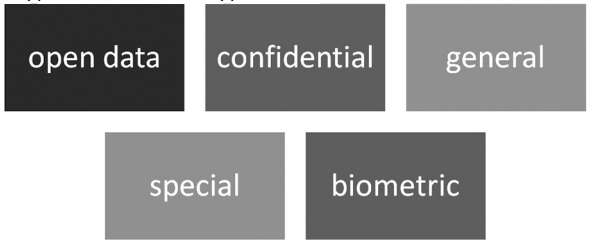
2.Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [13].

3.Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [14].

The Regulation may be applied by bodies not located in the territory of the European Union in the following 3 cases:



From the above, it is clear that these Rules have an extraterritorial (exterrorial principle). That is, there are no specific territorial restrictions. Personal information refers only to information about individuals. What is meant by personal information? Personal information means any information or set of information that identifies the individual to whom the information belongs by various means. What information is specifically included in the scope of personal data? A person's name, surname, address, contact number, information about his parents, family, marital status, bank accounts, e-mail address, mobile number, photo, voice recording, handprints, etc. are included in his personal information. However, not all such information is considered personal information. For example, in order for this information to be considered personal data, it must belong to a specific individual. An absurd e-mail, an unknown phone number cannot be considered personal information. Processing, storing, collecting, transmitting personal data, etc. operators and owners should know in advance about the resolution of other procedures. Personal data owners and operators must protect personal data. The protection of personal data includes their unauthorized and accidental destruction, unlawful interference, loss, alteration, or invalidation. Personal data owners and operators must organize an effective solution to the above issues and, in accordance with the legislation, register personal data information systems with the relevant executive authority, ie the Ministry of Digital Development and Transport. Relevant rules for registration are set by the Ministry of Digital Development and Transport. Personal information is regulated by the Law of the Republic of Azerbaijan dated May 11, 2010 "On personal data"[2]. At the same time, there are other legislative acts that regulate in this area. The article examines the mutual analysis of the legislation of the Republic of Azerbaijan in this area with the legislation of the European Union in the first and second degree, the impact of EU legislation on the legislation of the Republic of Azerbaijan in this area, future prospects and relevant proposals. The purpose of the article is to study the regulatory directions of international and regional, especially the European Union and the Republic of Azerbaijan in the field of personal data, legislative practice, to comment on existing gaps, to use EU legislation in a positive direction. According to the legislation of the Republic of Azerbaijan, information in the field of regulation consists of personal data, state secrets, taxes, banking secrets and trade secrets. According to the Law of the Republic of Azerbaijan "On personal data", personal information applies directly to individuals[2]. Personal information is any set of information and data that directly or indirectly identifies the individual to whom the information belongs.Personal data can be divided into several groups according to their arrangement.



General information is information that is partially and fully known by the society and the public, open to a certain category of the public, related to work activity, open to civil society and certain audiences due to the fact that the individual is a socially active person. Such information includes the individual's name, surname, e-mail address, place of work, mobile phone number, position, etc. Specific information includes the individual's religion, race, social affiliation, beliefs, health status, property status, movable and immovable property in his name, information on whether he has a criminal record, bank payments, bank history, telephone conversations, correspondence, etc. The specific feature of such information is that such information is not made public, i.e any third party does not have access to such information, except as provided by law.Biometric data are physiological and biological characteristics used to identify a person. Biometric data is regulated certain law of Azerbaijan Republic [5]. However, this information may not be considered biometric depending on its purpose. It directly depends on where the information is processed. For example, an individual's image can be related to general information, to specific information, or to biometric information. If a photo of a person is written on a book, it is already general information, because it is directly open to the public. If a photo of his face is taken for control and protection when entering an enterprise or office building, it is already biometric information, because in this case the photo directly identifies him. However, if the photo of the person is accompanied by information that is considered a personal matter in connection with his / her employment, then the photo is of special nature, because the photo is not directly accessible to third parties and is not open to the public. Thus, it can be concluded that what is important here is not the subject, but its purpose. The subject may be the same, but if its purpose serves different purposes, the legal category is already defined here. Who are the subjects and operators of personal data? First of all, it should be noted that the operator of personal data can be both an individual and a legal entity. The subject must be only an individual. Because we mentioned at the beginning of the article that personal data means only information about individuals. Here is a practical example: In order to get regular information from the bank, you fill out a questionnaire. Your personal information, both general and specific, may be included here. Here, the subject of the information providing the information, the bank receiving the information is the operator of the information, and the information specified in the form is the subject (object) of the information. According to the law on personal data, the subject of personal data is the person about whom the operator collects information. Such an issue arises here. The person about whom the information is collected is the person to whom the personal information belongs. For example, in the first case, the person who received the information from the Bank is A, and A himself provided this information. In the second case, the person who received the information from the Bank is A, and A himself provided B's information, for example, the person entered his parent's information, not his own, when filling out the request. The law distinguishes between these concepts. This begs the question: who should be the subject of the information? The person who provided it or the person to whom the information belongs? The information belongs to A, but is provided by B. A is the subject of information. Who is B? B is the user of the information. The user of the information can be a state or local self-government body, a legal entity or an individual. The user of the information must have the right to use personal data or this right must be given to them. A user of information means a state or local self-government body, legal entity or individual who has been granted the right to use personal data for the purpose of obtaining information for himself.

The Republic of Azerbaijan signed and ratified the 1981 Convention on the Ratification of the Convention for the Protection of Persons Related to the Automated Processing of Personal Data by the Law of the Republic of Azerbaijan of September 30, 2009 [4]. This Convention is contained in the Additional Protocol on Control Authorities and the Transboundary Data Flow [9]. However, the Republic of Azerbaijan has not signed this protocol. The Republic of Azerbaijan, Malta, San Marino and Slovenia have signed the Protocol in the member

states of the Council of Europe [18]. What does the signing of this Protocol promise to the Republic of Azerbaijan? By signing this Protocol, the Republic of Azerbaijan can deepen its integration into the European Union, organize its relations on a broader level, and at the same time make the process of harmonizing the legislation of the European Union with the legislation of other member states. The protocol was adopted in 2001. The purpose of the Protocol is to improve the provisions and principles of the Convention. Improvements are planned in two directions:

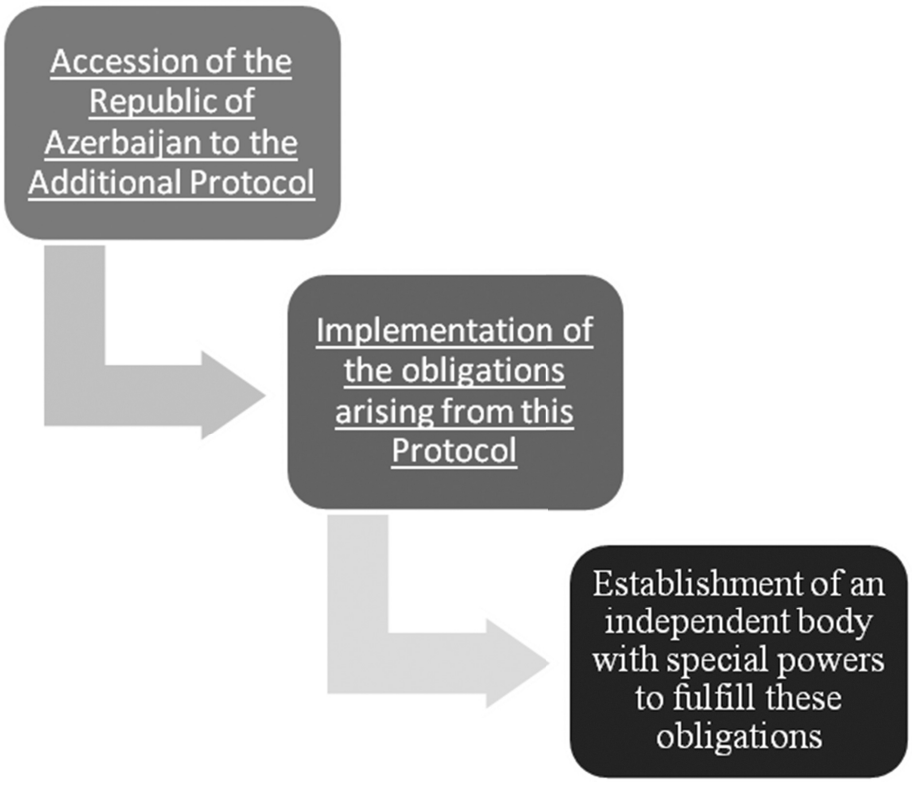
1) Establishment of a supervisory body to ensure the protection of personal data of the Parties to the Convention

2) Transboundary transmission of information to States not party to the Convention [18].

There is no single specialized body in the field of personal data protection in the Republic of Azerbaijan. Relevant activities in this area are carried out by various local executive authorities within their respective areas. However, such activities do not meet efficiency standards due to the lack of coordination, and the process of preventing violations of personal data protection legislation is difficult.

In today's world, where online processes are more prevalent than live or traditional processes, the protection of personal data is at stake, given the high level of information exchange, the importance of protecting fundamental human rights minorities, accountability measures and sanctions, and privacy and privacy. work to bring it to a higher level of necessity. At the same time, it is important to formulate and review sanctions in this area, to ensure that sanctions are adequate to protected legal relations and violated rights, and to comply with the principles of proportionality and necessity.

Additions and amendments to the legislation of the Republic of Azerbaijan in the relevant sphere will ensure its more effective regulation in this sphere in accordance with the requirements of the time. The main purpose of the article is to study the gaps in this area, to formulate relevant scientific provisions, and to put forward proposals. Accession of the Republic of Azerbaijan to the Additional Protocol and work on the implementation of the obligations arising from this Protocol, as well as the establishment of a body authorized to implement these obligations, will be an important step towards the development of legislation and institutional mechanisms in the field of personal data protection.

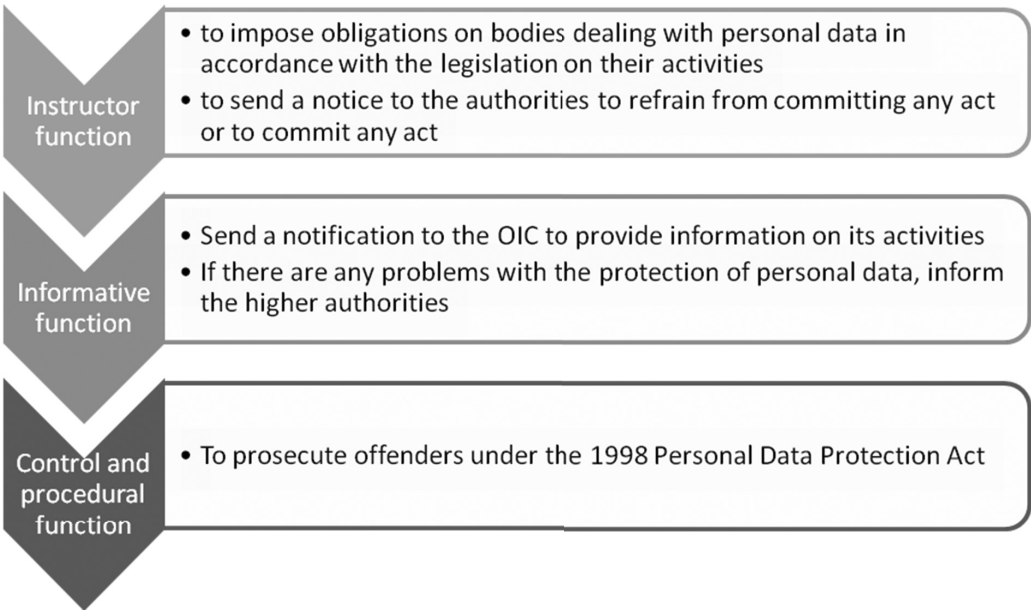


As mentioned above, there is no specific body in the field of personal data protection. Various government agencies do this within their jurisdictions. It is implemented within the Ministry of Digital Development and Transport, Ministry of Justice of the Republic of Azerbaijan, Ministry of Internal Affairs of the Republic of Azerbaijan, State Security

Service of the Republic of Azerbaijan, Ministry of Taxes, Security Service of the President of the Republic of Azerbaijan, State Service for Special Communications and Information Security. If we look at the practice of various states in implementing the obligations arising from the Additional Protocol, we can see that many member states have already formed such oversight bodies. As required by the 1995 Directive, member states must establish a single oversight body within their territory [10]. However, there are several institutions in Austria and the Netherlands. One of these bodies is a data protection body, and the other is a supervisory body within its competence. In contrast to the Directive, the Additional Protocol allows Member States to have more than one oversight body [9]. Prior to the establishment of such an institution in Romania, these powers were delegated to the Commissioner for Human Rights. In Finland, these functions are currently performed by the Commissioner for Human Rights. In a number of countries, for example, in Austria and Poland, these control bodies are not authorized to stop the actions of a person or body acting outside the law on personal data [6,p. 25]. Such an oversight body does not have the authority to prohibit the processing, deletion or destruction of personal information. In addition, in these countries, the opinion of such bodies is not taken into account when drafting legislation in this area. It seems that the powers of such bodies are extremely limited, they cannot act procedurally, they cannot give advice and opinions, they cannot conduct research and investigation. These bodies are fully consultative and do not have the force of law. The fact that these bodies operate with such incomplete powers is completely ineffective. Personal data control bodies should be the decisive body and report directly to the executive body in this area, and provide information on the status of activities. In general, these agencies should work together with agencies that work with personal data. In this case, the effectiveness can be restored.

The system of control over the protection of personal data of the Federal Republic of Germany also differs due to the special structure of the state itself. The FRG consists of 16 lands and the land has its own individual control body. The Federal Republic of Germany also oversees personal data legislation and data protection. The Federal Commissioner was established in 1978[20]. The main powers of this body were formed after 2006. In 2006, the German Freedom of Information Act was adopted in Germany.

In the UK, the OIC (Office of the Information Commissioner) [21] has relatively improved powers as a personal information oversight body. OIC has the function of monitoring individuals, legal entities, organizations, institutions working with personal information. It has the power to impose fines while controlling them. The IMO also has the authority to [21]:



In France, the Commission on Information Technology and Freedoms was established in 1978 as an independent oversight body that is not overseen or instructed by any body. The authority of the organization is wide [22]. It also has the authority to consent to the processing of sensitive data, including biometric data. It also analyzes the extent to which such activities affect individuals' privacy and inviolability. In accordance with the law, the Commission may impose a fine of three hundred thousand euros on legal entities that violate the law in this area. This authority has been given to him since 2004. He also has the authority to inform the public about the fine.Ukraine ratified the Additional Protocol in 2010. In 2011, the State Service for the Protection of Personal Data was established. The service is an executive body and reports to the Ministry of Justice. The Institute for the Protection of Personal Information has been established in Georgia [7, p. 3]. The Institute has been operating since 2013. It is independent and not subordinated to any organization. The agency reviews citizens' appeals, monitors the processing of information, investigates its legality, and provides advice, opinions and suggestions in this area. Makes an annual report. Russia has a rule that it does not send any information to a country that has not adopted such EU legislation without the consent of the individual. The Federal Service for Communications, Information Technology and Media Control operates here.

The Law of the Republic of Azerbaijan on Access to Information contains the issue of establishing an "Information Commissioner". However, since the law was amended in 2012, this position has been transferred to the Human Rights Ombudsman. However, despite the Ombudsman's annual general report, it does not report in this area alone. This has a direct impact on the effectiveness of the activity.

Conclusions

It is clear from the activities of the legislative and regulatory bodies of many of the above countries that most of these bodies are non-independent. An independent and incompletely competent body cannot defend any legal relationship. When establishing an organization, first of all, its functions, powers, responsibilities and duties, budget, sphere of activity and jurisdiction of the subject must be clearly defined. Otherwise, the activity of the institution is ineffective and is not taken seriously by the society, and there is no public trust in the institution. Taking into account the above, it is necessary to pay attention and take into account a number of issues when assuming the accession of the Republic of Azerbaijan to the Additional Protocol and the obligations arising from it. First of all, let's pay attention to the organizational form of the control body. We mentioned above that one or more institutions can be created. It would be more effective to create a single body and create information departments for different groups, or rather for the regulatory sphere. The institution should be subordinated to the Ministry of Digital Development and Communications. Powers, duration, budget, members, personnel and resources, activities shall be determined directly by the Ministry. In the field of information in some executive bodies, the powers delegated to various bodies should be transferred to this body.

According to the additional protocol, individuals can apply for the processing of their information. If it is possible to file such a petition in the Republic of Azerbaijan, it will have the right to make decisions in the purely information sphere and use these decisions as a precedent. The petition can be submitted to this oversight body, as well as an independent specialized court can be established in this area. The establishment of a specialized court may not be necessary at this time, as the burden of litigation in this area is currently small. At a time when developing, globalizing and electronic processes are at their peak, the implementation of general management, implementation, control, educational processes in electronic form in our society increases the need for regulation in this area, and violations of the law are inevitable. Given this, the establishment of a specialized court as a future perspective, the separation of such cases from general jurisdiction will reduce the burden on the general court and create conditions for more effective decision-making in this area. Of course, this can be considered as a future perspective.

Article 375 of the Code of Administrative Offenses of the Azerbaijan Republic provides

for an administrative fine for violation of the legislation on personal data. Violation of the requirements of this legislation is punishable by a fine of 300 to 500 manat [23]. Such a low level of administrative fines can lead to further violations of the requirements of the Personal Data Act.

For example, the maximum penalty for violating the GDPR rules, which came into force in May 2018, is up to twenty million dollars, or four percent of the violator's turnover (the largest amount is selected). Such penalties are imposed for serious violations, such as the processing of personal data without the consent of customers, and the discrediting of confidential information. Such a penalty mechanism is important for the protection of the rights of operators or other authorized persons to personal data subjects. We propose to amend the relevant legislation of the Republic of Azerbaijan to review the sanctions in this area and make the standards adequate to the public danger of an administrative offences or crimes.

In the international arena, there is a concept called the Personal Data Market. The personal data market is a database obtained by illegal means, methods and techniques that break the framework of legal protection. In modern times, such internet fraud (internet gambling), misappropriation of people's bank information, various illegal transactions on behalf of people, theft of people's personal information (through the acquisition of identity card information) stems from the formation of a personal data market. In short, the personal data market is made up of information stolen by illegal means.

References

1. Constitution of Azerbaijan Republic. / http://www.e-qanun.az/framework/897

2. The Law of the Republic of Azerbaijan "On Personal Data" of May 11, 2010.

3. "Requirements for protection of personal data" approved by the Decision of the Cabinet of Ministers of the Republic of Azerbaijan dated September 6, 2010.

4. The Law of the Republic of Azerbaijan of September 30, 2009 on the ratification of the Convention for the protection of individuals with regard to automatic processing of personal data

5. The Law of the Republic of Azerbaijan "On Biometric Information". June 13, 2008.

6. Irwin R. Kramer, The Birth of Privacy Law: A Century Since Warren and Brandeis, 39 CATH. U. L. REV. 703, 715–19 (1990).

7. Vivek Krishnamurthy.Symposium OnThe GDPR And International Law A Tale Of Two Privacy Laws: The GDPR And The International Right To Privacy 2020, 5 p.

8. Convention for the protection of individuals with regard to automatic processing of personal data, Strasbourg, 28.I.1981.

9. Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows)

10. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

11. European Union on Privacy and Electronic Communications Directive (2002)

12. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (European Union General Data Privacy Regulation- GDPR)

13. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data

14. Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repeal-

ing Council Framework Decision 2008/977/JHA

15. International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 UNTS 171

16. Universal Declaration of Human Rights, Dec. 10, 1948, GA Res. 217 A (III) (1948).

17. European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950.

18. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=181

19. https://www.cnil.fr/fr/cadre-europeen

20. https://core.ac.uk/download/pdf/80399406.pdf

21. https://ico.org.uk/

22. https://www.cnil.fr/en/home

23. https://www.legislationline.org/download/id/3439/file/Azerbaijan_Code%20on%20Administrative%20offences_2000_eng.pdf