SECURITY ENSURING PROBLEMS ON ELECTRONIC TRADE

GULIYEV Rafael - doctoral student of "Civil Law" department of Baku State University

DOI 10.32782/EP.2022.4.22

It is impossible to form a single model of legal regulation of e-commerce without taking into account privacy issues. It should be noted that one of the principles for the development of the information society at the World Summit on the Information Society was the principle of confidentiality and security in the use of information and computer technologies. It can be concluded that a person doing business on the Internet or processing (outsourcing: (external source use)) business elements related to personal data (IT infrastructure, accounting, etc.) faces a potential cross-border transfer of personal data. In this regard, in addition to fulfilling the requirements for localization, it is advisable to include in privacy policies and agreements with individual data subjects the conditions for their consent to such transfers.

Key words: Electronic trade, security, confidentiality, electronic document, electronic information exchange, electronic signature, information technology.

In connection with the development of electronic commerce in Azerbaijan in modern times, there is a need to formulate adequate legal provisions for electronic commerce as a special type of entrepreneurial activity. At the same time, the analysis of the legislation proved that the legal norms currently regulating electronic commerce in our Republic are not combined with the general strategy for legislative protection of this special business area.

As a whole, the difficulties in legal regulation are related to the expansion of the use of information and telecommunication networks in trade, the globalization of trade relations, and the development of legal norms regulating trade activities without taking into account the possibilities of modern information and communication technologies [5, p.112].

The features of this area of legislative regulation are manifested in the participation of parties in the exchange of electronic documents, telecommunication operators, providers, self-regulatory organizations in the process of electronic commerce. In addition, new concepts such as, information, public information systems and corporate information systems, information and telecommunication networks, electronic transaction, electronic document, electronic document exchange, electronic signature, electronic payments and settlements, electronic means of payment that are new to traditional jurisprudence in the field of legal regulation of electronic commerce are introduced. Provisions of international documents related to electronic commerce have not yet been adequately reflected in the current legislation of the Republic of Azerbaijan.

At the same time, the expediency of state regulation of relations in the field of legal regulation of electronic commerce in modern conditions and the possibilities of self-regulation, definition of basic terms and concepts, issues of determination of legal status of regulation of the participants and their responsibility, the procedure for exchanging electronic documents in conducting civil-legal transactions and making electronic payments, as well as the issues of ensuring privacy and security in the field of electronic commerce remain not fully

resolved. All this requires more multifaceted legal scientific development from the point of view of civil-legal regulation, including the formation of a modern model of legal regulation.

As the analysis of foreign experience in the field of e-commerce regulation indicates, the main problems of privacy and security in e-commerce have been identified in international experience [7, p. 28-29]. It is especially emphasized that "ensuring security and protecting privacy is one of the main concerns of online shopping. It is estimated that more than 30% of internet users in the European Union do not shop online due to security concerns [13, p. 170-173]. In this article, we have tried to study the problems related to privacy and data protection, that is, security in cyberspace.

Privacy is divided into two categories: data (or information) privacy and personal privacy. Information privacy refers to the means (methods) of information collection, recording, reception and dissemination. Privacy refers to a person's private life, an individual's personal space. Privacy principles are defined by the Organization for Economic Cooperation and Development.

In connection with the use of information and telecommunications tools in the implementation of electronic commerce, there are general security and privacy threats in this area: computer fraud, computer viruses, computer hacking, computer attacks, inaccurate information about the product and the seller, the location of the seller and the buyer, failure to transmit or delay in transmission of a message, transmission of data to an incorrect address, disclosure of confidentiality of data, etc. For this reason, legal guarantee of privacy of personal data, completeness and reliability of information; protection of the organization's accounting information; protection of intellectual property rights is important for electronic commerce activity.

In international experience, there are certain legal approaches to the regulation of this aspect of electronic commerce. For example, the Organization for Economic Cooperation and Development has developed relevant regulatory principles based on practical privacy and security legal issues [6, p. 220-222].

The security of electronic commerce is the situation of protecting the interests of subjects in relation to each other who carry out commercial transactions (deals) with the help of electronic commerce technologies [1, p. 172].

The emergence of personal data as a separate category in the information law and the legal world as a whole is closely related to the idea of protecting personal life, which is increasingly exposed to various threats in the context of the development of the information society. It was the desire to ensure proper protection of individuals from information threats that led to the idea of controlling the circulation of information about individuals - personal data, distinguishing them as a special type of information that requires protection.

Doctrinal definitions of personal data in jurisprudence are not so numerous and similar in many respects. According to the doctrinal approach to personal data presented in the European Union, information that cannot be attributed to the subject of the personal data cannot be the subject matter of the personal data [8]. However, it is noted that the identification of the individual should be evaluated objectively. This means that not only the legal and actual capabilities of the individual data operator, but also the capabilities of third parties should be taken into account [9].

Jayna Genti notes that "personal data" is any information relating to an identifiable living individual. This definition includes any piece of information that may lead to the identification of an individual, even if the personal data is identified, encrypted or pseudonymized. The only exception is personal data, which is provided anonymously without reversion to non-identification [10, p. 1].

Post-Soviet scientists, especially Russian experts (A.G.Areshev, I.L.Bachilo, L.A.Serjienko), clarify the content and importance of this category as follows: "personal data is a data created at the individual's personal request and on the basis of law, are used for its own interests and the interests of the state in the public environment based on international standards and national legislation, during contact

with the individual's state authorities, public and private institutions, other individuals" [4, p. 23].

The main purpose of personal data pro-

tection is the protection of human and citizen rights and freedoms, including personal life, family and personal privacy. Therefore, it seems logical to conclude that there is a direct connection between the protection of personal data and the right to private life, as well as the issues included in this right (the right of privacy, personal, family, name, surname and voting secrecy, etc.).

Personal data is collected in specific information resources in the manner and volume determined by law. If personal information is added to one or another information resource, that information is known as an information resource of personal data. Information resources can be created within a specific information system or separately. Information systems ensure the circulation of personal data, in other words, its life cycle, in accordance with the law.

The processes of collecting, processing, providing, distributing, transferring, freezing, anonymizing, and destroying personal data are common functional components of the life cycle of personal data [2, p. 69].

Currently, the legal basis of the personal data protection mechanism has been formed in two directions and has acquired a more precise system: specialized (or special) legislation and other (general) laws. Other laws include legal norms that guarantee the protection of personal data only in certain cases and regulate the protection of certain types of personal data.

Specific legislation primarily includes the Law of the Republic of Azerbaijan "On Personal Data". General laws include: Law of the Republic of Azerbaijan "On Information, Informatization and Information Protection, Law of the Republic of Azerbaijan "On Access to Information, Law of the Republic of Azerbaijan "On Biometric Information", Law of the Republic of Azerbaijan "On Telecommuni-cations", Law of the Republic of Azerbaijan "On Mass Media" and others.

As a whole, one of the first normative legal acts in the field of legal regulation of information processes in our country is the Law of the Republic of Azerbaijan "On Information, Informatization and Information Protection" dated April 3, 1998. This Law regulates the creation and use of information systems, technologies and means of their support on the basis of data collection, processing, storage, search, dissemination, the formation of information resources on the basis of data protection and determines the rights of persons participating in information processes [14].

Information processes on personal data are mainly applied by banks, insurance companies, government organizations, social organizations, large commercial enterprises, business and transport companies to obtain high income, to ensure information security and reduce risks [12, p. 552-565].

Although the mentioned Law does not define personal information, the concept of "confidential information" is used. From the analysis of the law, it can be concluded that confidential information is a different concept, personal information is confidential. According to the type of acquisition, personal information is divided into confidential and open categories.

As we mentioned, the specific normative legal document in the sphere of personal data protection in our Republic is the Law "On Personal Data" dated May 11, 2010. Before proceeding to the analysis of the law, let us note that this Law regulates the problems related to the collection, processing and protection of personal data, the formation of part of the personal data of the national data space, as well as the transfer of personal data abroad, determines the rights and duties of state bodies and local authorities, legal and natural persons [15].

Article 2.1.1 of the Law defines the term "personal data" as follows: personal data is any information that allows the identification of a person directly or indirectly. We believe that this concept is very broad and abstractive. The provisions of the law do not reveal the concept of personal data in detail. So the question arises: What information can be considered personal information that allows to identify this or that natural person? What is the scope of the definition of personal data? Another aspect of the issue is that the terms "direct" and "indirect" in this concept are not clarified, which leads to ambiguities in practice.

Our approach is that personal data is information related to that individual based on various criteria (physical, mental, physiological, economic, cultural, social characteristics, relationships and associations) in order to identify

the individual.

The following subjects are recognized as participants in public relations regulated by this Law: subject of personal data, owner, operator and user. Here, the subject is the physical person about whom personal data is collected, processed and protected, whose identity is determined or identified. The owner is the state body, legal entity or natural person that has the right of ownership over the information resources of the relevant personal data as determined by law. The operator is the owner with the right and responsibility for the collection and use of the relevant personal data, or the bodies, legal or natural persons to whom the rights and obligations are delegated. The term user of personal data means a state body or local self-government body, legal entity or individual who is given the right to use for himself and in the manner and scope determined by his authority, only for the purpose of obtaining the information he needs.

The authorized entity that creates the information resources and information system of personal data, while forming those information resources, shall observe the basic human and civil rights and freedoms, as well as legality, confidentiality, as well as the basic human and civil rights established in the Constitution of the Republic of Azerbaijan.

Modern technologies are also able to overcome a number of technical limitations associated with the collection of personal data. Thus, the significant cost reduction of the storage of huge information arrays stimulates the rejection of the principle of limiting the processing of personal data for predetermined purposes [11].

In any case, the process of collecting personal data should be legal and transparent so that people's trust and confidence in this system does not decrease. The data subject must know for what purpose, in what way the information about him will be collected and how it will be used. At the same time, the data subject must have access to that personal information.

After the adoption of the Law of the Republic of Azerbaijan "On Personal Data", a number of normative measures were implemented in the direction of the application of this Law, necessary additions and amendments were made to the law, and at the same time additions and changes were made to other legislative acts for the purpose of applying this Law.

It should be noted that, except for cases of mandatory collection and processing of personal data in accordance with the legislation of the Republic of Azerbaijan,collection and processing of personal data about any person is allowed only on the basis of written consent given by the subject, including an electronic document with a strengthened electronic signature, or on the basis of information provided in writing by the subject [15].

The absence of an objection from the subject of personal data to the processing of his personal data by the operator shall not be construed as his consent, as this is not of a specific nature. In general, silence, as you know, (contrary to the common saying) is not a sign of consent in law. The requirement that the consent is a specific nature implies the performance of any actions that indicate such consent. For example, the subject's provision of certain information about personal data may in some cases be considered as an expression of consent to their final processing.

The practice of consenting to the processing of personal data by ticking the appropriate box on the screen when placing an order in the field of e-commerce or registering on a website has become widespread. In principle, there is no reason to invalidate such consent provided it is informed and conscious. In practice, there are also cases where "registration of an Internet user on the site, confirmation with login and password means the consent of the subject to the processing of his personal data".

Another point is that the owner of the Internet resource must be ready to prove not only the fact that such consent was given, but also that a certain person consented to the processing of their personal data in the specified amount. As an option, you can reflect the fact of its existence in the e-mail sent to the user to confirm the registration or order, a copy of which remains with the operator. Although, if there is a dispute about whether such consent was given and the authenticity of the content of the e-mail provided by the operator is disputed, the will be little chance of successfully proving the fact of consent to processing. The

fact that a certain person gave consent without an electronic signature can be proven only by indirect evidence, for example, by using a bank card belonging to the subject of personal data as a means of payment.

We must not forget the possibility to object to the conditions included in the connection agreement, especially those concluded with the participation of the consumer. Thus, even if the relevant condition is included in such an agreement, there are cases where the court does not recognize the existence of consent to the processing of personal data. According to the court, in such cases, the subject of personal data does not have a choice, because the only possibility to not give such consent is expressed in the refusal to conclude a contract. In cases where prior consent to the processing of personal data in all possible ways is a necessary condition for the purchase of any service, it is debatable to speak of conscious consent. Such a requirement violates the principle of ensuring fair processing and is expressly prohibited in some jurisdictions.

In addition, it is risky to include the condition of consent to the processing of personal data not in the text of the document in which the user expressed his consent, but in the text of another document referred to by the first. Given that the user is unlikely to be familiar with its content, it is hardly possible to speak of informed and reasonable consent in such cases.

Finally, a few words should be said about publicly available personal data that can be processed by operators without the subject's consent. According to Article 5, Part 3 of the Law of the Republic of Azerbaijan "On Personal Data", the category of open personal data refers to the data entered with the consent of the subject into the information system that has been anonymized in the prescribed manner, announced publicly by the subject, or created for general use. The person's name, surname and patronymic are public personal information. Confidentiality of open categories of personal data is not required [3, p. 150-152].

Bibliography

1. Akbarov, M.G. Electronic commerce. - Baku: "University of Economics" Publishing House, – 2011, – 212 p. [in Azerbaijani].

2. Aliyev, E.A. Problems of regulating the life cycle of personal data in information systems / - Baku: Information society problems, – 2013.No.2 (8), –p. 67-76. [in Azerbaijani].

3. Askerov, F., Hasanova, R. Personal data security issues in electronic libraries / 5th Republican Conference on "Actual multidisciplinary scientific-practical problems of information security", November 29, 2019. Institute of Information Technologies of ANAS, Baku, p. 150-152. [in Azerbaijani].

4. Areshev, A.G. Personal data in the structure of information resources. Fundamentals of legal regulation / A.G. Areshev, I.L. Bachilo, L.A. Sergienko. – M., 2006. [in Russian].

5. Saliev, I.R. Problems of Ensuring Confidentiality in the Sphere of Electronic Commerce // Eurasian Law Journal. State and law. Legal Sciences. No. 7 (62). 2013, – p. 111-113. [in Russian].

6. Davidson, A. The Law of Electronic Commerce. – Cambridge: Cambridge University Press, – 2009, – p. 220-222.

7. Dickie, J. Producers And Consumers in EU E-commerce Law. – Portland, Oregon, 2005, – p. 28-29.

8. EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide. Second edition. IT Governance Privacy Team. – 2017. – 400 p.

9. Feiler, L. The EU General Data Protection Regulation (GDPR): A Commentary / L.Feiler, N.Forgo, M.Weig. – Surrey: Globe Law And Business, – 2018, – 333 p.

10. Genti, J. Do you need to worry about new eu prıvacy rules?// Virginia Employment Law Letter, – 2018, No. 5, –p. 1-4.

11. Lane, J. Privacy, Big Data and the Public Good: Frameworks for Engagement / J.Lane, V.Stodden, S.Bender, H.Nissenbaum, – Cambridge: Cambridge University Press, – 2014, – 344 p.

12. Parkinson, B. The digitally extended self: A lexicological analysis of personal data / B.Parkinson, D.Millard, K.O'Hara, R.Giordano // Information Science, – 2018, vol. 44, Issue 4, – p. 552-565.

13. Wang, F.F. Law of Electronic Commercial Transactions: Contemporary Issues in the EU, US and China. – London, New York, 2010. – p. 170-173.

14. Law of the Republic of Azerbaijan "On Information, Informatization and Information Protection" dated April 3, 1998. https://is.gd/mK2r8T [in Azerbaijani].

15. Law of the Republic of Azerbaijan "On Personal Data" dated May 11, 2010. https://e-qanun.az/framework/19675 [in Azerbaijani].

Рафаэль Гулиев - докторант кафедры Гражданского права Бакинского государственного университета

ВОПРОСЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В ЭЛЕКТРОННОЙ ТОРГОВЛЕ

Невозможно сформировать единую модель правового регулирования электронной коммерции без учета вопросов конфиденциальности. Следует отметить, что одним из принципов развития информационного общества на Всемирном саммите по информационному обществу был принцип конфиденциальности и безопасности при использовании информационных и компьютерных технологий. Можно сделать вывод, что лицо, ведущее бизнес в Интернете или обрабатывающее (аутсорсинг: (внешнее использование источника)) бизнес-элементы, связанные с персональными данными (ИТ-инфраструктура, бухгалтерский учет и т. д.), сталкивается с потенциальной трансграничной передачей персональных данных. . В связи с этим, помимо выполнения требований по локализации, целесообразно включать в политики конфиденциальности и договоры с отдельными субъектами данных условия их согласия на такие передачи.

Ключевые слова: электронная торговля, безопасность, конфиденциальность, электронный документ, электронный обмен информацией, электронная подпись, информационные технологии.