REPUBLIC OF AZERBAIJAN

On the rights of the manuscript

ABSTRACT

of the dissertation for the degree of Doctor of Philosophy

INFORMATION LAW VIOLATIONS AND INFORMATIONAL-LEGAL LIABILITY: THEORETICAL AND PRACTICAL ASPECTS

Specialty:	5614.01 – "Administrative law; financial law; information law "
Field of science:	Law
Applicant:	Huseyn Oktay Alizade

Baku - 2023

The dissertation was performed at the UNESCO Chair on Human Rights and Information Law of the Law Faculty of Baku State University.

Scientific supervisors: Doctor of laws, Professor
Ramil Mahir Aslanov

Philosophical doctor of laws
Gulnaz Aydin Rzayeva

Official opponents: Doctor of laws, Professor
Salmanova Olena Yurivna

Philosophical doctor of laws, Associate Professor
Nazanin Shahin Huseynova

Philosophical doctor of laws, Associate Professor
Asmar Alimusa Aliyeva

FD 2.44 Dissertation Council operating under the Baku State University

Chairman of the Dissertation Council: Doctor of laws, Associate Professor
Turgay Imamgulu Huseynov

Scientific secretary of the Dissertation Council: Philosophical doctor of laws, Associate Professor
Alizade Gurbanali Mammadov

Chairman of the Scientific seminar: Doctor of laws, Professor
Amir Ibrahim Aliyev

Azərbaycan Respublikasının Elm və Təhsil Nazirliyi
BAKI DÖVLƏT UNİVERSİTETİ p.h.ş.
Ministry of Science and Education of the Republic of Azerbaijan
Baku State University l.e.p.l.
ELMİ KATİB
SCIENTIFIC SECRETARY
İmzanı təsdiq edirəm:

GENERAL CHARACTERIZATION OF THE DISSERTATION

Relevance of the topic and degree of research. The study of informational-legal violations as an actual problem began after the formation of the information society. It was inevitable that there would be various negative situations in this society, which was expected to achieve successful results in the early days of its creation. As early as the 50s of the XX century, Norbert Wiener, the founder of the information theory, who defined information as the information obtained in the process of adaptation of us and our senses to the environment[1], raised problems related to the existence of threats in the application of automation and ICT. Over time, those dangers mentioned by N. Wiener began to spread widely as information law violations.

The aforementioned research is closely related to information security and human rights. Thus, it is noted in the legal literature that threats to information security in the conditions of modern globalization and the development of information technologies are directed against the national security of states, the general interests of society, including human rights and freedoms[2]. Threats occur in different directions and forms in a global and transnational nature[3].

Today, the Internet has penetrated all areas according to the needs of daily life and connected people from all over the world. In this

---

[1] Viner N. Cybernetics and society. Moscow: Publishing House of Foreign Literature, 1958, p.31 (in Russian).

[2] Akrivopoulou C.M., Garipidis N. Human Rights and Risks in the Digital Era: Globalization and the Effects of Information Technologies. Hershey: IGI Global, 2012, p.19.

[3] Aslanov R.M. Theoretical and constitutional foundations of legal guarantee of information security in the construction of information society in the Republic of Azerbaijan and the Russian Federation. Abstract of the dissertation submitted for the Doctor of Law degree. Baku: 2015, p.10 (in Azerbaijani); Aliyev A.I. Human rights. Baku: Nurlar, 2019, p. 128-129 (in Azerbaijani); Aslanov R.M. The right to information in the legislation of the Azerbaijan Republic // Computer Law & Security Review, 2016, Volume 32, Issue 6, December, p. 889-891.

direction, extensive historical, theoretical, and comparative analyzes in the legal literature[4] should be considered important, and they once again determine the wide scope of the issues we put forward in the research. The connection established with the help of the Internet allows people to communicate by shopping, transfer various information and even globalize in a free environment. Today, even states have to use information technologies for the implementation of their activities. With the Internet connection, the activities of the legislative, executive, or judicial bodies of the state are structured in such a way that, unlike the classical management system, the given instructions are carried out faster by being transferred between the state bodies in electronic form. The use of information systems in important infrastructure sectors such as energy, communication, agriculture, health, transportation, education, and finance has created the importance of the concept of cyber security, which is considered equal to national security. In the modern world connected by a single global network, the existence of cyberspace has become a controversial fact, along with the risk of losing the sovereignty of states, as well as the presence of specific borders. Because there is no central administration, it is very difficult to prevent or fight abuses in this area, and the regulation of one state is not enough.

According to Amnesty International's report, companies like Google and Facebook are turning the spaces we spend time in our homes into a private space through smart home appliances with the Internet of Things technology and smart urban design infrastructure, and in this way, people's personal data is being collected[5]. Therefore, the prevention of violations of the information law is not only important from one direction, it is also essential for the provision of

[4] Azizov R.F. Comparative legal analysis of regulation in the "Internet" network. Baku: Elm, 2017, 216 p (in Azerbaijani); Azizov R.F. Legal regulation in the Internet-space: history, theory, comparativism. Baku: Qanun, 2021, 352 p (in Azerbaijani).

[5] Surveillance giants: How the business model of google and facebook threatens human rights.https://www.amnesty.org/en/documents/pol30/1404/2019/en/

other human rights. In this regard, comments have been given in many literatures[6].

Reasons such as the inability to detect the damage caused by cyber-violations caused by the development of ICT, and the amount of information that is not calculated in terms of quality and quantity, lead to the increase of information law violations. However, it is very difficult to see it in statistical figures. The reason is that many violations remain latent due to the fact that they are not yet criminalized or detected and are not reflected in official statistics. For these reasons, there are many problems in terms of the effectiveness of legal regulations in the context of information law violations. The fact is that there is no statistical information about any investigative material or judicial experience of acts committed in cyberspace resulting in human death. No state has given a legal definition to information warfare, officially declared information warfare, or announced its support for such warfare. But despite this, calculating the damage caused by information violations in cyberspace, which is increasing day by day, creates enormous difficulties. Because such violations, especially cybercrimes, in most cases are not directed against one person, but against thousands and millions of people. Here, first of all, it should be noted the economic damage caused by acts that lead to the failure and destruction of various computers and networks, which changes with increasing dynamics every year. According to Cybersecurity Ventures, global cybercrime spending is expected to reach $10.5 trillion annually by 2025, from $3 trillion in 2015, growing by 15% per year over the next five years[7]. These figures confirm the extent of the economic damage caused and to be caused. As a result, acts such as illegal access to information systems constituting a state secret, etc. also cause political damage to various states. The human factor related to such violations should be brought

[6] Susi M. Human Rights, Digital Society and the Law: A Research Companion. New York: Routledge, 2020, 3412 p.

[7] Cybercrime To Cost The World $10.5 Trillion Annually By 2025. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

to the fore, as various information law violations aimed at obtaining income illegally by stealing personal data directly violate human rights and freedoms. For the mentioned reasons, their prevention and solving the issue of liability is considered an urgent problem.

Even the recent start of the construction of the Digital Silk Road necessitates the legal regulation of cyberspace in our republic, especially the legal solution of liability issues for information violations. The project, which envisages meeting the internet connection needs of states in the region through the Republic of Azerbaijan, will create conditions for our republic to become a transit country in cyberspace.

Fighting cybercrime has always been a complex issue due to the number of ICT network users, the cross-border nature of the Internet, and its decentralized architecture. Organized crime groups, both traditional and online-only, are and will likely continue to be several steps ahead of lawmakers and law enforcement. Because technological innovations in cyberspace are not always used for legal purposes. In fact, according to the calculations made in 2019, 69% of the experts who participated in the survey firmly confirmed that the cases of abuse on the Internet, or more precisely, violations of information law, have increased[8].

The fact that cybercriminals use the latest innovations in technology to commit crimes makes it even more difficult for law enforcement agencies to fight crimes. In this regard, it is important for the units that fight these crimes to know the technology used by the criminals and the characteristics of the criminals and develop strategies accordingly.

The current legislation is characterized by the lack of a unified approach to the evaluation of violations in the field of information technologies, the unity of the used conceptual apparatus, and the

[8] Dan Jerker B. Svantesson. Internet & Jurisdiction Global Status Report 2019. https://digital-strategy.ec.europa.eu/en/library/internet-and-jurisdiction-global-status-report-2019

application of inconsistent and unsystematic changes that do not give the expected result. In addition, the imperfection of legislation regulating the application and use of the achievements of scientific and technological progress, and the division of the regulatory base in approaches to the legal regulation of various aspects of technological progress continue to remain a common legal problem.

In foreign sources, Turkish authors have mostly explored directions related to cybercrimes, and there are enough studies in this field. For example, Murat Volkan Dulger ("Information Crimes" book), Ismail Ergun ("Cyber Crimes Penalty and Situation in Turkey" book), Dr. Muammer Ketizmen ("Information Crimes in Turkish Criminal Law" book), Ali Karagulmez ("Information Crimes and Investigation - Prosecution Phases" book), Levent Kurt ("Information Crimes" book) and others presented different approaches to crimes committed through ICT.

Scientists such as I.L.Bachilo, P.U.Kuznetsov, V.A. Kopilev, O.A. Gorodov, M.M. Rassolov, who study the information law as a new field, have commented in general on the issues related to information law violations and informational legal liability. Among the foreign authors, the scientific approaches of N. Winner, M. Castells, M. McLuhan, E. Tofler, and others were reviewed.

Some common points in this field have only been clarified in the "Information law" textbook published in our republic under the scientific editorship of A.I. Aliyev and G.A. Rzayeva. In addition, the works of R.M. Aslanov and R.F. Azizov also analyzed some close legal issues related to information law violations and information-legal liability. Later, despite the fact that extensive analyzes (R.M. Aliguliyev, R.Sh. Mahmudov, etc.) have been conducted in the fields such as information environment, security, etc. in various aspects and scientific directions, they almost do not cover the legal fields.

The object and subject of the research. The object of the research is the main problems of international and national legal regulation related to information law violations and informational-

legal liability, as well as existing contradictions in the field of legal solution of technical and organizational aspects. The subject of the research is legal norms and practical gaps from the international and national-legal aspects related to information law violations and information-legal liability.

Research goals and objectives. The purpose of the research is by determining the main distinguishing features of information law violations, to classify them, to analyze the forms of information-legal liability based on this classification, to reveal conflicts in the international-legal regulation related to the mentioned issues, as well as by analyzing the ambiguities in national-legal norms, to put forward legal proposals and recommendations for the improvement of the preparation.

The following tasks are defined in the research work:

- the determination of the concept and characteristic features of information law violations, differentiation of traditional and non-traditional elements in its content;
- the analysis of problems in legal regulation related to non-traditional elements of information law violations and presentation of optimal proposals;
- carrying out the legal classification of information law violations and determining the practical significance of such classification;
- the analysis of international legal regulations on information law violations, identification of "outdated" and conflicting norms in this area, presentation of new amendments;
- the analysis of the legislative experience of foreign countries related to information law violations and informational-legal liability;
- a detailed review of the legislation of the Republic of Azerbaijan regarding information law violations and informational-legal liability;

- the differentiation of information law violations from similar and related violations, including analysis of the problem from the context of human rights;

- the analysis of international-legal and national-legal problems in the legal regulation of forms of informational-legal liability;

- the analysis of information security from the aspect of informational-legal liability;

- the interpretation of the specific aspects of the informational-legal liability of legal entities;

- the analysis of the specific characteristics of the informational-legal liability of natural persons, investigation of the liability problems of humanoid robots;

- the disclosure of the content of cybercrimes and presentation of proposals for combating them;

- the establishment of visual comparative research in this field by preparing sufficient schemes and tables in information law violations, informational-legal liability, and other related fields;

- providing some proposals in the direction of improving the legislation of the Republic of Azerbaijan in information law violations, informational-legal liability, and other related areas.

Research methods. General and special methods were used comprehensively during the research. In determining the compatibility of the experience of foreign countries and international norms with domestic norms, comparative-legal analysis has been given a wider place. The results of the conducted analysis were summarized using the synthesis, and certain suggestions and recommendations were put forward.

The elements of information law violations were studied separately based on the analysis. At this time, the proposal of a single model was made possible by the construction of various imaginary (intangible) models. Interpretation of various legal norms and detection of contradictions was carried out on the basis of formal logic methods.

Scientific novelty of the research. In the national legal science, no comprehensive research has yet been conducted on the problem of

information law violations and informational-legal liability. As a result, this has led to an excessive expansion of the boundaries of information law violations. In the dissertation, the elements in the content of information law violations were classified into two groups for the first time, and the scope of information law violations was determined based on this classification criterion.

For the first time in the legal literature, an approach different from the technical approach of information law violation was presented in the dissertation work. Another scientific innovation, arising from the influence of ICT, consists in revealing existing gaps in the international legal regulations themselves.

The main new scientific propositions defended are the following:

1. There is a contradiction between the traditional interpretation of these violations and the modern explanation regarding information law violations. Traditionally, since information is mainly associated with media and news, information law violations were also interpreted from this context. The formation of cyberspace in modern society has formed the position that information violations are committed only in this space and are related to ICT. By not accepting such a narrow approach with the conducted analyses, it is emphasized that the information space is a broader concept, and it is accepted that the mentioned violations are committed in the information space. Because in the information society, information has become an integral part of our life. In this case, the interpretation of cybercrimes itself in a narrow sense is not considered correct from a legal point of view. Differentiation of violations related to cyberspace and ICT should be determined directly depending on the object, which consists of information recorded in different systems, i.e. data. Therefore, the name of the chapter in the criminal legislation of our republic, which provides for sanctions related to cybercrimes, can be considered somewhat unfortunate. This also creates confusion at the level of the Budapest Convention. The Convention considers cybercrimes, albeit flawed, as acts committed in cyberspace, taking it in a broad sense. Such a position of the Convention stems from the need

for a unified international legal framework for the trans-border nature of acts committed in cyberspace and the regulation of their jurisdictional issues in general. However, the mentioned chapter directly envisages actions that violate the given. Therefore, it is more appropriate to name the chapter as "Crimes against Data (or Computer data)". It would not be appropriate to lump all ICT-related crimes under cybercrime, as this would require the same sanction for crimes with very different statuses. Furthermore, if this distinction is not made, the scope of cybercrime will expand to such an extent that there will be enormous challenges for practice in the future.

2. In most cases, international norms are accepted as "benchmarks" and implemented in national law. However, the necessity of the modern era confirms the aging and modification of many international norms. In the study, it was proposed to carry out various revisions on such international documents related to information law violations. It can be considered that since national law is based on international law in most cases, such editing, and changes can contribute to domestic law as well. In addition, problems in legal translation have led to the misinterpretation of many globally accepted terms in national legislation. For example, the elements of completeness, availability, and confidentiality, which are called the "triad" of information security, are generally accepted. However, according to the translation of the Budapest Convention, availability is defined as "usability", and "confidentiality" as "privacy". Equating confidentiality with privacy, as well as the lack of availability, can create confusion in defining the general content of cybercrimes. This once again confirms the need to use a single terminology.

3. Information security, which is of special importance for the prevention of information law violations, should not be one of the main directions of the information policy of states. Also, information security should be ensured within individual organizations, and an internal policy plan should be developed in this regard. So, in most cases, criminals use the information systems of various organizations to commit cyber violations. Therefore, information security should

not be considered only as information protection. In our republic, with the amendments dated May 27, 2022, the legal definition of information security in the legislation can be considered a commendable case. However, it is appropriate to eliminate some shortcomings in the legal concept. Thus, it is not acceptable to include the element of credibility together with the completeness, availability, and confidentiality of information. Because the guarantee of the three elements we have listed is aimed at making the information reliable in each case.

4. The introduction of a legal approach to critical information infrastructure with the recent amendments to the national legislation and the addition of a chapter called "Security of critical information infrastructure" to the Law "On Information, Informatization and Information Protection" necessitated the revision of regulations related to violations committed in this area. Thus, according to the relevant amendment, the violation of the requirements for the security of critical information infrastructure causes administrative-legal liability (Article 20-4.6 of the Law and Article 371-1 of the Code). However, no amendments were made in the criminal legislation. Taking into account the state and public importance of the objects covered by critical information security, we consider it appropriate to provide regulation on the criminal-legal level as well.

5. Information technologies are rapidly changing, and at the same time, the methods and general nature of violations in the field of information are also changing. However, the legislation cannot fully adapt to these changes. Therefore, concreteness should not be allowed in the norms in the field of information, so that it can respond to future changes. Concepts such as "cyber-attack", "cyber-war", "cyber-espionage", "cyber-crime" do not have internationally accepted uniform definitions. At the same time, jus cogens rules adopted by states were not created in the field of cyber law. In fact, as a result of the increasing dependence of developed countries on the Internet, the shortcomings of the Internet have created a suitable environment for attacks by hostile states. Thus, due to the security

gaps created by the Internet, developed states are committing various cyber violations against less developed states. This is one of the consequences of the lack of definition in the field of international law. The fact that cyber-attacks that could lead to inter-state conflicts have no equivalent in international law is a significant shortcoming. Although recent changes in the national legislation include concepts such as cyberattack, cyberincident, cyberthreat, this is not enough for the legal regulation of violations committed in cyberspace.

6. Another important problem is that violations committed in cyberspace transcend jurisdictional issues due to the cross-border nature of the Internet. Therefore, in order to prevent such violations, in addition to strengthening the existing legal framework, updating and harmonizing old international and national norms, intersectoral cooperation at the national level, as well as the development of international cooperation in the field of detection, investigation, and prevention of crimes committed in the electronic environment are required. The organization of acts committed in the cyber environment should also be taken into account here. Many states lack adequate regulation to respond to the activities of organized cybercriminals. Therefore, solving the problem can be possible at the global level, because the Internet is a global network. In the absence of a global strategy, the problem is likely to worsen in the near future. In this regard, the way to solve the problem may be to develop a long-term action plan that includes coordination and harmonization of efforts at both national and international levels.

7. One of the main problems in our national legislation is the repetition of many terms. Thus, many norms related to the legal regime and types of information, which is the main object of information law violations, are repeated in various legislative acts. For example:

- The concept of documented information is provided both in the Law "On Information, Informatization and Information Protection" (Article 1) and the Law "On Obtaining Information" (Article 7). In terms of content, both mentioned articles overlap;

- Most of the principles related to obtaining information are repeated both in the Law “On Obtaining Information” and the Law “On Freedom of Information”;

- Concept norms related to information systems and services are provided in each of the mentioned legislative acts, etc.

Prevention of the mentioned repetitions is possible in two ways: first, supporting the position of the authors regarding the adoption of the "Information Code" and adopting such a Code; and the second is to make appropriate amendments to the existing legislative acts and issue repeated norms.

8. In general, the concept of cybercrime has led to various interpretations in the legal literature due to the fact that it is not given in either international or national regulation. Most researchers understand cybercrimes as acts that attack ICT and are committed through ICT. However, considering acts committed through ICT as cybercrime can lead to serious problems for the traditional views of legal science. It is logically and practically incorrect to combine the illegal seizure of data from the information system and the insulting of any person in cyberspace under the same name - cybercrime. This case can be applied to many crimes. Therefore, the most important element for cybercrime should be the target. For example, stealing bank information illegally should be considered theft, not cybercrime. However, if the use of ICT is identified as a constituent element in the disposition providing for the relevant act, then it will be necessary to describe the act as a set of crimes. Because the illegal seizure of information using ICT is itself criminalized as a separate criminal act (Article 272 of the Criminal Code).

We believe that the XIII UN Congress on Crime Prevention and Criminal Justice has made an interesting and compelling argument about this issue. The existence of problems in defining new forms of crime, especially the problem of terminology, is noted and the expression "newly emerging forms of crime" is addressed. [42, 4] Cybercrimes are also included in these new forms of crime. It should be noted that such new forms of crime not only include new causes

and methods of perpetration, but may also target new types of victims that may be more difficult to detect. The number of victims is also high in these types of acts. Thus, the distribution of one malicious program can harm multiple users at the same time.

9. It would be more correct if the legal concept of internet and host providers reflected in the Law "On Information, Informatization, and Information Protection" is provided in the Law "On Telecommunications", which provides for the liability of providers. In addition, the legislator needs to express his attitude to the transit provider because this service is used in practice.

10. In many cases, violations in the field of information did not create either an error or a criminal offense, but consisted only of temporary "user concerns". However, the practical examples we have presented once again confirm that a simple crack can eventually lead to loss of life. Therefore, law enforcement agencies should not be indifferent to complaints arising from this type of computer and Internet use, and should take preventive measures to prevent them.

The theoretical and practical significance of the research. The theoretical importance of the study is that information violations were classified here and their differences from other violations were determined. The new terminological explanations put forward for the complex approach to the problems and the elimination of the deficiencies in the existing sectoral legislative acts can be theoretically important.

The practical importance of the research should be noted in relation to the proposed forms of cooperation in the fight against information law violations, and the types and forms of information-legal liability.

At the same time, the research can be widely used in the teaching of subjects such as information law, the legal basis of information security, legal liability in the field of information, electronic state, cyber security law, etc.

Validation and application of research results. The results and innovations obtained in the research work are reflected in the

scientific works published by the author in various languages on the subject of the dissertation in the prestigious scientific journals of our republic and foreign countries, including in the materials of international scientific conferences.

The structure of the research. The research consists of Introduction, three chapters, conclusion, and a bibliography.

MAIN CONTENT OF THE RESEARCH

In the **Introduction** of the dissertation the relevance of the topic, the degree of its development is substantiated, goals and objectives, research methods, defense provisions are defined, novelty, theoretical and practical significance of the research, approbation and application of the research work, name of the dissertation organization, separate structure of the dissertation is provided.

The **first chapter** is **"The nature and legal determination of informational-legal violations"** and consists of three paragraphs.

In the **first paragraph**, the traditional and non-traditional elements in the content of information law violation are analyzed.

Informational-legal violations have many specific features that distinguish them from traditional violations: taking into account the dynamic and rapid development of ICT, it is very difficult to detect these violations and fight against them; the target of such violations can sometimes be an individual, sometimes an organization or thousands of people; depending on the global nature of cyberspace, it will not be possible to achieve successful results if the fight against information law violations is not carried out at the international level.

In the era of the formation of the information society and the rapid development of digitalization processes, ICT is used as the main factor or method in the commission of almost all legal violations. However, this should not mean that all those violations

are not related to information law violations. It is not correct to agree with positions in the legal literature that favor such an expansive approach. Of course, for any violation to be considered as an information law violation, it is committed using ICT. However, other elements should also be taken into account here. Basically, one of the important points is the cycle of public relations, which the violation intends. For example, insulting a person on a social network or disclosing information about his personal life, despite the fact that it is committed through ICT, is, of course, an act that violates the right to privacy. Therefore, the information, which is the main element of the content of the information law violation, consists of the information recorded on these violations, or more precisely, placed on various networks. Such information constitutes data. Therefore, it is better to use the concept of data rather than computer information in relation to information violations (whether administrative, civil, or criminal).

In the **second paragraph**, theoretical and legal approaches to the classification of information law violations are studied.

Accepting only the criminal-legal aspect of informational-legal violations is not enough to reveal their nature. Therefore, it is more correct to consider these violations as administrative errors, civil delicts, and crimes. In the digital society, there are numerous information violations that threaten civil law relations. So, in social media, which has billions of users, such violations have become very widespread. Even in cyberspace, organizations created against information spread from a negative aspect operate and promote the activities of states from a positive direction. For example, the WikiLeaks network exposes numerous high-profile cases of corporate and government corruption, and "Troll factories" creates fake social media profiles and websites to support troll operations. Employees of the Troll Factory not only write messages, but also respond to comments and participate in online discussions. They can simulate arguments to increase the impression of authenticity of the fake profiles through which they distribute the content they create.

Informational-legal violations should not be strictly limited to cybercrimes. Of course, cybercrimes are the main acts that violate the completeness, confidentiality, and availability of information. However, since information relations have a broader character, information law violations should also have a broader content.

The **third paragraph** analyzes the problems of formal and informal classification of cybercrimes.

At a practical level, the lack of a concrete definition raises particular concerns regarding cybercrimes, which are cross-border and transjurisdictional in nature, unlike traditional crimes. For a long time, the lack of a specific legal approach resulted in the separation of Internet-related crimes into two groups: cybercrimes in the narrow sense – includes acts that aim to attack computers and software; cybercrimes in a broad sense – includes all acts related to ICT or committed through it.

The main official classification was developed in 1991 by the INTERPOL working group. All codes in this classification have an identifier starting with the letter "Q". They themselves are divided into 6 groups depending on the type of intention, where the letters "A", "F", "D", "R", "S", "Z" are used. For example, the code consisting of the letter combination "QA" represents Unauthorized (unsanctioned) access and seizure, the code consisting of the combination "QF" represents computer fraud, the code "QR" represents illegal copying (piracy), etc. Each of these codes has its own classification depending on the way the crime was committed.

The **second chapter** is **"The prevention of information law violations and information security"** and consists of three paragraphs.

In the **first paragraph**, international cooperation on the prevention of information law violations is studied, universal and regional norms are analyzed.

Investigating a crime committed in cyberspace often involves the legal systems of many different countries and requires close international cooperation to bring the perpetrators to justice. The

Republic of Azerbaijan is a member of a number of official and unofficial mechanisms that demonstrate this cooperation. This includes the ratification of various Conventions, especially the Budapest Convention, as well as membership of key networks and multilateral forums.

In general, international cooperation can be formal or informal. Formal cooperation includes universal and regional conventions and agreements. Crimes committed over the Internet often exceed the jurisdiction of a single state, which is a threat to the entire international community. Since this global problem cannot be solved by the norms governing regional or limited relations, only an international solution and a multilateral approach, which is provided by the Budapest Convention, is currently required. It is important that Internet conduct that is criminalized in one jurisdiction is also criminalized in other jurisdictions. However, we should also note that the Budapest Convention itself has not yet been ratified by many countries. This reduces the effectiveness of the Convention, because the 66 countries that have ratified the Convention account for less than half of the world's Internet users.

In the **second paragraph**, the characteristic features of the experience of foreign countries on the legal determination of information law violations and their fight against them are studied.

Regarding information law violations, more attention is paid to criminal acts in foreign countries. Civil delicts and administrative offenses are somewhat neglected. The main reason for this is the numerous attacks on human rights in cyberspace. All foreign countries have criminalized illegal entry. However, there are already differences in the regulation of the use of computer data for the purpose of generating income. In some states, this is included in the list of information crimes, while in other states, it is defined as an independent component (for example, computer fraud).

In order to conduct comparative analysis, the dissertation referred to the legislative sources of several states and it was concluded that the German legislation defined the violations of

information law more fluently and concretely. An interesting feature is that cybercrimes in Germany are not considered in a separate chapter. Penalties for ICT-related acts are defined in specific articles depending on various criminal objects. Thus, the German Criminal Code provides for the following crimes related to ICT under "Breach of confidentiality of personal and private sphere": information espionage; phishing; preparedness for data espionage and phishing; processing (processing) of stolen data. "Computer fraud" (Article 263a) is included as a separate type of "Fraud and embezzlement". In addition, "Data manipulation" (Article 303a) and "Computer sabotage" (Article 303b) are defined as separate crimes.

The **third paragraph** examines the technical, organizational, and legal problems of preventing information violations and ensuring information security.

Information security consists of a set of measures aimed at ensuring the completeness, availability, and confidentiality of information. In many cases, this term is equated with "cyber security". But they belong to different types of security. Simply put, cyber security is about attacks from inside or outside an organization. It is a framework to protect all aspects of computers, devices, networks, servers, and applications that are vulnerable to attacks or unauthorized access. Cyber security is only about protecting data in digital form. In contrast, information security aims to protect data from all types of threats, whether analog or digital. Therefore, information security has a broader context and includes cyber security.

As cyber security has a wide range of applications, covering industries and various fields, each country's level of development or engagement is assessed on five criteria: legal measures, technical measures, organizational measures, human resource development, and cooperation.

The **third chapter** is **"The institution of informational-legal liability: international and national-legal regulation"** and consists of two paragraphs.

In the **first paragraph**, issues related to the informational-legal liability of legal entities, the formation of electronic management in the Republic of Azerbaijan, and a new approach to the institution of informational-legal liability are examined.

The division of informational-legal liability between individuals and legal entities is of particular practical importance. This plays an important role in determining the appropriate administrative or criminal sanction to be imposed, as well as in resolving a civil dispute. If in the early days of the information society, more individuals were prone to information violations, gradually criminal organizations began to use the "convenient and suitable" opportunities provided by ICT. As a result, cybercrime began to develop as a type of organized crime, which affects the determination of liability.

The Budapest Convention provides a specific regulation in this regard as well. First, the Convention requires states to determine the liability of both the individual himself and the corresponding legal entity for the violations committed by the person who has the authority to make decisions on behalf of any legal entity, exercise control functions, represent the legal entity, for the benefit of the legal entity. Secondly, we are talking about not only criminal-legal, but also other types of liability. Thirdly, the Convention does not consider the determination of the liability of legal entities as a mitigating circumstance, and emphasizes that it does not exclude the liability of a person as a natural person.

In general, the liability of legal entities for information law violations should be analyzed in the following directions: informational-legal liability of legal entities engaged in organized crime; informational-legal liability of internet providers; informational-legal liability of information owners.

In the **second paragraph**, the forms of informational-legal liability of natural persons are studied.

The main problem in determining the liability of natural persons for information law violations is the rapid emergence of new types of them. In many cases, it even creates a problem as to what type

of infringement is to be attributed. In this regard, theft of identity should be specially mentioned. Dishonest misuse of a person's registered digital identity by another person is called "theft of identity" in the literature. Unlike common fraud crimes, theft identifies that person as the victim of the crime.

The informational-legal liability of natural persons is also regulated by field norms, like legal persons. Unlike legal entities, natural persons are liable as users. The problem is that the criminal equivalent of violating the rules of using information resources (Article 371 of the Code of Administrative Offenses) is not provided. Violation of the rules of use of the information by the person who obtained the information cannot be attributed to any of the crimes against the data. So, depending on the content of the obtained information, the legislator defined public danger and provided criminal liability for spreading various secrets. For example, a person engaged in the legal profession has applied to the relevant body with a request about the property of the other party in the divorce case of his client. Since property information is considered personal information, the lawyer should not allow this information to be distributed or disclosed arbitrarily. In addition, it is also determined by law that a lawyer must protect the confidentiality of information known during his professional activity, and this information constitutes the lawyer's secret. Therefore, in this case, the lawyer's disclosure of personal information creates liability for the distribution of the lawyer's secret. Since there is no corresponding criminalized act, it is necessary to refer to the disposition on personal data (clause 2.1 of Article 156). This is where the legal conflicts come from. The legislator, classifying various confidential information, does not differentiate liability for the persons liable for the dissemination of such information.

The **Conclusion** of the dissertation notes the important proposals and results obtained in connection with the research. In general, they can be expressed as follows:

1. In order to reveal the essence of informational-legal violations, the elements included in the content of these violations

should be interpreted by us as traditional and non-traditional. In the content of informational-legal violations, the main traditional three elements have been mentioned. Because the characteristic features of these elements distinguish those violations from other legal violations: conditions for committing the violation; the object of the violation; the subject of the violation and its purpose.

2. Unfortunately, information systems are given a very confused and vague definition in the articles of the information legislation of the Republic of Azerbaijan, which provide for general concepts. In our opinion, it is more appropriate to make the following edit: "Information system is a device or a group of devices that performs data processing automatically and on the basis of appropriate programs and performs interconnected activities."

3. There are uncertainties in the legal interpretation of the terms "information" and "data" in national legislation. Summarizing both the theoretical and legal aspects, the legislator does not definitively determine that information appears in the form of information after being recorded. However, from the interpretation of many norms (for example, to obtain recorded information, a person must submit an information request, not a request for data), it is clear that in the legal regulation, recorded information, whether in electronic or paper carriers, is considered as information. But this itself is contradictory. Because the mentioned laws use the phrase "personal and family life information" (personal information). In this case, there is confusion in the terminological apparatus. Therefore, we believe that it would be more correct if the term "data" is used in the norms regarding the removal of any information from the information system in the Laws of the Republic of Azerbaijan "On obtaining information" and "On information, informatization and information protection". Besides, we propose to edit the definition of data as follows: "Data is any form of presentation of facts, information or concepts suitable for processing through information communication technologies, which ensures the implementation of any function."

4. Due to the fact that the global network covers all states, the states fighting against information law violations should develop a common legal language among themselves in order to carry out effective cooperation. Standardization of international norms on the basis of that legal language is an important condition that states of the world should implement their legal regulations in accordance with those international rules. An interesting point is that many international norms are already out of date, and taking into account the development of ICT, it would be better to make changes in the terminological apparatus.

5. Only one of the expressions of completeness, availability, and confidentiality, known as the "triad" of information security all over the world - "completeness" - has been correctly translated. "Confidentiality" is expressed by the word "privacy", which is completely contrary to the information law. "Availability" is translated with the equivalent of "usability". Furthermore, the term "isolation" referred to in the Convention means "blocking". The second concept is also used in national criminal legislation. In order to eliminate such problems, the legal translation of international legal documents should be revised.

6. With the changes made to the national information legislation dated May 27, 2022, information security was defined. The reliability element implied here will actually exist if the first three elements (completeness, availability, and confidentiality) are satisfied. Therefore, we consider it acceptable to include only three elements in the legal definition.

7. Information law violations are illegal, intentional actions committed in the field of information and that violate information law relations. ICT is mainly used here. However, every act committed using ICT cannot be regarded as an information violation. As mentioned, digitalization has led to the use of cyberspace to commit various crimes. In this space, only the actions against the information law relations in the field of information will be considered an information law violation. Therefore, there may be

informational violations committed without the use of ICT. It should be noted that such an approach has not been presented in the studies carried out so far. In all comments, information law violations are analyzed only from a technical aspect, connecting them with ICT. However, as we mentioned, the main condition for information law violation is violation of information law relations. In this case, it is impossible to interpret violations related to the restriction and violation of information law in the context of information law violations.

8. Information law violations should not be limited to cybercrimes. Yet, in most literature, "information crime" refers only to cybercrimes. The problem is that when violations are committed in the field of information, in most cases there is a need to apply criminal legislation. Because the lighter form of cyber crimes criminalized in the Criminal Code is not provided for in the Code of Administrative Offenses. So, while there are situations where ordinary theft is described as a crime and an offense, depending on the value of the object of the conspiracy, the legislator has not provided any alternative for the circumstances in which acts committed in cyberspace and directed against information systems and data lead to light consequences. There will be difficulties in the application of the Code of Administrative Offenses, which establishes a general offense such as "violation of the rules of use of information resources" (Article 371 of the Code of Administrative Offenses of the Republic of Azerbaijan). At the same time, another problem is related to the fact that a special subject is considered as an element for almost all cybercrimes. In our digital world, cases of data capture by ordinary people using ICT are not uncommon. We believe that the formal components provided for in the Criminal Code should be included in the Code of Administrative Offenses as an administrative offense. Also, the performance of those actions by all persons, not a specific subject, should lead to liability.

9. Although illegal actions related to data using ICT do not cause serious consequences in many cases, they cause certain concerns for

various people. For example, we can register emails with viral content. If the user does not open that slant, there are no negative consequences. But with this comes concerns. For example, temporary blocking of a website (chat, discussion forum, etc.) that a person frequently uses by administrators. Although legally there is no question of a crime, it is possible to solve the problem by applying liability as an administrative offense. Even foreign countries have experience in complaints related to damage caused in virtual space. Concerns that do not lead to serious consequences can lead to administrative liability.

10. The term "cybercrime" is not clarified in international norms. As a result, in the national laws of different states, such acts are called various types (electronic crimes, computer crimes, crimes in the field of computer information, crimes related to high technologies, etc.). Also, cybercrimes are interpreted in a broad sense in most sources, that is, all violations committed in cyberspace are considered cybercrimes. This is the approach of the Budapest Convention. However, in our opinion, such an approach may eventually result in all criminal acts being considered cybercrime. Because digitization creates wide opportunities for the criminal world. For example, insult or slander in its traditional form is almost non-existent. It would not be right to consider these acts as cybercrime. Because crimes must be classified depending on the object of intent. Therefore, the broad interpretation of cybercrimes cannot be considered acceptable. In this regard, it is more appropriate to amend the Budapest Convention itself. Because, although the Convention adopts a broad analysis approach, many acts committed using ICT (for example, making an open call to terrorism) are left out of the regulation. We would like to express our position based on the narrow interpretation of cybercrimes: "Cybercrimes are crimes committed by using ICT and computer information in cyberspace."

11. The legal classification of information law violations in the legislation of the Republic of Azerbaijan on criminal and administrative offenses is not conducted successfully. First, the

actions provided for in the chapter "Cybercrimes" of the Criminal Code are actions against registered information, more precisely, data. In the Convention itself, the acts that the Criminal Code defines as "cybercrimes" are titled as "crimes against the confidentiality, completeness, and availability of computer data and systems", and the latter is more correct.

12. Legal measures play a key role in preventing and combating cybercrime, including the criminalization of cyber violations and the determination of administrative liability as well as the liability of Internet service providers, regulation of procedural powers and jurisdiction, and international cooperation. If in the early days, both existing and new (or planned) legislative acts at the national level were only related to criminalization, now the world community prefers the re-editing of specific field norms. Information law violations are not an isolated issue, they can only be tackled with a comprehensive, collaborative, global approach that requires global cyber security awareness and global capacity building.

13. Prevention of informational-legal violations requires universal and regional cooperation on both organizational and material grounds. The importance of interstate cooperation is related to maintaining centralization and independence. As for the material basis, it has already been mentioned that violations committed in cyberspace are not only a matter of one state. In this regard, the organization of cooperation should be at a perfect level.

14. The notion "Transfering to cyberspace" of social life has led to an increase in legal uncertainty. The activities of both natural and legal persons (companies and other organizations) are regulated by relevant laws. It is very easy to determine the applicable law in an offline environment. But in the online environment, this issue is quite difficult and complicated. Currently, the lack of a single normative source that regulates jurisdictional issues in the Internet or cyberspace creates great difficulties during proceedings on information law violations. It is true that the Budapest Convention regulates matters of jurisdiction. But as we mentioned within the

study, 66 countries that ratified the Convention do not mean all the countries of the world. Therefore, there is a need to adopt a unified international legal document.

15. The most problematic point regarding informational-legal liability is that the use of ICT is considered an aggravating circumstance in most of the legislation. Considering the dynamics of digitalization, it is not logical to consider the application of ICT as an aggravating circumstance. Such application should be considered as one of the other methods.

16. The fight against informational-legal violations can also be successful if the reasons for their increase are minimized. These reasons, on the one hand, are related to problems in the legal and technical regulation of cyberspace, and on the other hand, they depend on the low level of awareness of individuals.

The main content of the research work is reflected in the theses and articles published below:

1. Information offense or cybercrime: an international and national-legal approach // - Baku: International law and integration problems, - 2020. № 1(59), - pp. 52-56.

2. Information law violations and cyber security: problems in international legal regulation // Materials of the international scientific-practical conference on "Interconnection and application of legal fields in the modern era: theory and practice", 2020, Baku: - pp. 366-370 (in Azerbaijani).

3. Theoretical and legal approaches to the classification of information-legal violations // - Kyiv: Law of Ukraine, - 2021. № 9, pp. 144–154.

4. Analysis of universal and regional norms on the prevention of information law violations // - Baku: Azerbaijan Law Journal, - 2021. No. 1, - pp. 98-108 (in Azerbaijani).

5. Informational-legal liability of legal entities: formation of e-governance in the Republic of Azerbaijan and analysis of a new approach to the institution of information-legal liability // - Baku:

Scientific News of the Police Academy, - 2021. No. 4 (32), - pp. 103-112 (in Azerbaijani).

6. Informational-legal liability of natural persons // - Baku: Transport law, - 2021. No. 1, pp. 207–216 (in Azerbaijani).

7. Traditional and non-traditional elements in the content of information offenses: act as a major factor changing the nature of information offenses // - İnternational Halich Congress On Multidisciplinary Scientific Research, - August 15-16, 2021, Turkey İstanbul: - p. 271-275.

8. Cybercrimes: official and unofficial classification // Materials of the international scientific-practical conference on "XXI century, new challenges and modern development trends of law", - December 21-22, 2021, Baku: - pp. 217-218 (in Azerbaijani).

9. Prevention of information law violations and ensuring information security: ways to solve technical, organizational and legal problems // Materials of the XXIV Republican scientific conference of doctoral students and young researchers, 2021, Baku: - pp. 150-153 (in Azerbaijani).

10. Information law violations and informational-legal liability: theoretical and practical aspects// - Baku: Azerbaijan Law Journal, - 2022. No. 3, - pp. 98-108 (in Azerbaijani).

The defense of the dissertation will be held at the meeting of the FD 2.44 Dissertation Council operating under the Baku State University on "29" "september" "2023" at "10:00".

Address: AZ 1148, Baku, Z. Khalilov Street 33, I Building, Auditorium 002.

The dissertation is accessible at the Baku State University Library.

Electronic versions of the dissertation and its abstract are available on the official website of Baku State University.

The abstract was sent to the required addresses on "18" "july" "2023"

Signed for print: 13.07.2023
Paper format: 60x84 1/16.
Volume: 2
Number of hard copies: 100.

Published by "Adiloglu" LTD.

Address: Baku city, Tbilisi avenue, 3007th block, 44 C
Tel.: (050) 593 27 77, (055) 339 75 77
E-mail: adiloglu2000@gmail.com