ELECTRONIC PROVES AS ONE OF THE MODERN INDEPENDENT MEANS OF EVIDENCE

a Beibit Birzhanov, b Assemgul Sakenova, c Erkin Abeuov, d Kairat Birzhanov, e Assel Sopyhanova, f Gulmira Talapova

ABSTRACT

Objective: the purpose of this study is a determination of the procedural status of electronic documents as electronic evidence and identification of gaps in legislation regarding their legal regulation.

Theoretical framework: theoretical materials were based on international scientific publications, reports, and scientific papers. And also for a more complete and objective presentation of the problem being studied, also practical materials from criminal cases were used.

Method: is a dialectical method of understanding general patterns and particular manifestations of the essence of phenomena of objective reality. The comparative legal method made it possible to qualitatively study foreign legislation from the point of view of the legal regulation of electronic evidence and their application in practice. The method of mathematical analysis and logic made it possible to analyze everything that could relate to electronic evidence, identifying their characteristics.

Results and conclusion: electronic evidence is information in electronic digital form, suitable for communication, interpretation or processing. In the electronic digital environment, the main interacting objects are various kinds of information objects (data sets, files, programs, etc.) with a complex hierarchical structure. Data in electronic digital form are intended to transmit information through media, information systems and telecommunication networks, and in the event of a crime being committed against them, their protection is of primary interest, and the nature and content of this data fades into the background.

Originality/value: the value of the study lies in the fact that, based on a comprehensive analysis, electronic evidence has a unique structure and ensuring their safety is one of the

a PhD Student, Head, Center for Research of Problems of Forensic Support of the Activities of the Department of Internal Affairs Research Institute Karaganda academy of the Ministry of internal affairs of the Republic of Kazakhstan named B. Beisenov, Kazakhstan, E-mail: b_b_k@mail.ru, Orcid: https://orcid.org/0000-0002-7470-0996
b PhD in Law, Professor, Department of Criminalities Karaganda academy of the Ministry of internal affairs of the Republic of Kazakhstan named B. Beisenov, Kazakhstan, E-mail: assemgul_s@mail.ru, Orcid: https://orcid.org/0009-0007-5596-6055
c PhD in Law, Associate Professor, Head, Center of the Interdepartmental Research Institute of the Academy of Law Enforcement Agencies under the General Prosecutor's Office of the Republic of Kazakhstan, Kazakhstan, E-mail: abeuov_74@mail.ru, Orcid: https://orcid.org/0009-0002-4122-0002
d PhD in Law, Maslikhat of Karaganda Region, Kazakhstan, E-mail: b_k_k_61@mail.ru, Orcid: https://orcid.org/0009-0008-7997-7266
e PhD in Law, Faculty of Law, Karaganda Buketov University, Kazakhstan, E-mail: sopyhanova09@mail.ru, Orcid: https://orcid.org/0000-0001-7272-7653
f PhD in Law, Assistant Professor, Faculty of Law, Almaty Management University, Kazakhstan, E-mail: talapova74@mail.ru, Orcid: https://orcid.org/0000-0001-9783-8245
criteria for their use, as well as the possibility of introducing a copying function will expand the process of processing evidence. The concept of “computer information” is the author’s definition, which will allow us to consolidate electronic evidence as an independent type.

Keywords: evidence, electronic evidence, computer information, information technology.

PROVA ELETRÔNICA COMO UM DOS MEIOS DE EVIDÊNCIA INDEPENDENTES MODERNOS

RESUMO

Objetivo: o objetivo deste estudo é a determinação da situação processual dos documentos eletrônicos como prova eletrônica e a identificação de lacunas na legislação quanto à sua regulamentação legal.

Referencial teórico: os materiais teóricos foram baseados em publicações científicas internacionais, relatórios e artigos científicos. E também para uma apresentação mais completa e objetiva do problema em estudo, também foram utilizados materiais práticos de processos criminais.

Método: é um método dialético de compreensão de padrões gerais e manifestações particulares da essência dos fenômenos da realidade objetiva. O método jurídico comparado permitiu estudar qualitativamente a legislação estrangeira do ponto de vista da regulamentação jurídica das provas eletrônicas e da sua aplicação na prática. O método de análise matemática e lógica permitiu analisar tudo o que se pudesse relacionar com as evidências eletrônicas, identificando as suas características.

Resultados e conclusão: evidência eletrônica é informação em formato digital eletrônico, adequada para comunicação, interpretação ou processamento. No ambiente digital eletrônico, os principais objetos que interagem são diversos tipos de objetos de informação (conjuntos de dados, arquivos, programas, etc.) com uma estrutura hierárquica complexa. Os dados em formato digital eletrônico destinam-se à transmissão de informação através de meios de comunicação, sistemas de informação e redes de telecomunicações e, em caso de crime contra eles cometido, a sua proteção é de interesse primordial, ficando a natureza e o conteúdo destes dados em segundo plano.

Originalidade/valor: o valor do estudo reside no facto de, com base numa análise abrangente, a prova eletrônica ter uma estrutura única e a garantia da sua segurança ser um dos critérios para a sua utilização, bem como a possibilidade de introdução de uma função de cópia expandirá o processo de processamento de evidências. O conceito de “informação informática” é a definição do autor, o que nos permitirá consolidar a evidência eletrônica como um tipo independente.

Palavras-chave: evidência, evidência eletrônica, informação computacional, tecnologia da informação.
1 INTRODUCTION

Currently, information technology influences almost every area of life. Electronic evidence is a binary computer code that is created using computer means and exists on technical media. The specified code cannot be felt, it has no material expression, but exists in an intangible form on technical means. The essence of this feature distinguishes electronic evidence from written and physical evidence, which exists only in material form and is inextricably linked. But the legislation still does not have a clear definition of computer information and its characteristics; therefore, the task of our research is to analyze the concept of “computer information” and its constants in the legislation.

Electronic evidence is characterized by the impossibility of its direct perception, because electronic evidence is actually a recording of information using machine code. A review and study of the physical state of the electronic evidence carrier (disk, flash drive, etc.) is not a study of electronic evidence, because judges participating in the process cannot examine the actual data that is recorded on it. Moreover, the main problem with the use of electronic evidence is not to view a specific electronic storage medium, but to carry out the authentication process, that is, to establish certain rules and methods, with the help of which judges participants in the process can determine the reliability of evidentiary information. Therefore, one of the tasks is to consider the safety of computer data and their legal status, as well as the process and mechanism for their seizure.

Otherwise, such a means of proof cannot be used for evidentiary activities. The presence of a technical information carrier. A specific process for creating and storing information that allows you to easily change the medium without losing content. In fact, the technical information carrier has similarities with material evidence, because they contain evidentiary information in their physical properties. Meanwhile, unlike material evidence, electronic evidence carriers make it easy to create, change and delete factual data. Evidentiary information on electronic media is quite vulnerable compared to traditional means of evidence. Lack of electronic copies of this type of evidence. In addition, some legal scholars also highlight such features of electronic evidence as the possibility of its transmission using communication channels, the possibility of using electronic evidence simultaneously to several persons.
2 LITERATURE REVIEW

With the rapid development of science and technology, especially the popularization of the Internet and social media, electronic evidence such as emails, blog posters, instant messages, electronic trading records, correspondence records and login logs have become new additions to the family of evidence in all over the world. China officially recognized electronic data as a category of legal evidence in 2012 when the Criminal Procedure Law and Civil Procedure Law were revised. It is generally accepted that the use of this new evidence must be subject to different rules of evidence because electronic data have some features that differ from other traditional evidence. To regulate the use of electronic evidence in criminal cases, the Supreme People's Court of China (SPC), the Supreme People's Procuratorate (SPP) and the Ministry of Public Security (MPS) jointly issued Regulations on several issues related to the collection, seizure, examination and adjudication of electronic evidence in criminal cases. Criminal cases in 2016. Then in 2019, the Department of Public Security published more detailed rules for obtaining electronic data as evidence in an attempt to address the practical problems encountered in the collection, seizure and inspection of electronic data. The SPC included some new provisions on the use of electronic evidence in civil cases when it revised the Rules of Evidence in Civil Cases in 2019. These legal documents not only provide a general legal framework for the use of electronic evidence in both civil and criminal proceedings, but also provide useful technical guidance and procedural rules for the collection and examination of digital evidence. However, very few legal researchers in China have conducted in-depth research on this topic due to its interdisciplinary nature between law and technology, let alone English literature. This paper attempts to review key issues regarding the collection, seizure, examination and adjudication of electronic evidence in criminal and civil cases, identify weaknesses in current legislation, and put forward some legislative proposals for future reforms (Zhiyuan Guo, 2022).

Mason, Stephen and Seng, Daniel (2021) have assembled a team of experts in the field to provide a comprehensive approach to electronic evidence.

Several initiatives are currently underway to address jurisdictional and conflict of law issues caused by the ubiquity of cloud storage. By introducing a new approach to international cooperation through the clarification of the Lawful Overseas Use of Data Act (CLOUD Act), the United States of America (US) is leading the charge to reform
cross-border data access. The US approach deserves closer examination, given its impact on shaping international standards governing law enforcement access to cloud data, as well as its impact on other upcoming reform initiatives. Although many blogs and reports have been written about the Cloud Computing Act, a comprehensive academic analysis appears to be lacking (Halefom, 2019). However, Stephen Mason is exploring whether it is possible to move towards a global or regional electronic evidence law. The aim is to start a debate, especially as the advent of instant communication has arguably led to the ability of the world's judicial systems to communicate globally and across jurisdictions in the interests of justice as a whole.

Crime and cybercrime have a huge impact on our modern economy, with annual losses estimated at hundreds of billions of dollars. Effectively combating cybercrime in an interconnected society faces a number of obstacles due to conflicting understandings of cross-border electronic evidence retrieval, the legality of the data requested, and the rules of cooperation with communications service providers. The document provides an assessment of the current legal situation and existing regulations that allow the collection of cross-border electronic evidence (Borka and Klobučar, 2019).

But effective criminal investigations still depend on reliable access to evidence. Thanks to the widespread use of cloud computing in various forms, electronic evidence of criminal activity can no longer be found on the criminals themselves or their associates. Most likely, evidence is stored with cloud providers, often on servers outside the premises of the law enforcement agency conducting the investigation (LEAS). Thus, even in completely domestic criminal investigations into crimes committed within a country against a local victim, the relevant electronic evidence may be stored in a cloud storage facility in another country. Obtaining evidence in such situations can be difficult (Svantesson et al., 2015).

In this regard, it can be noted that digital evidence and digital forensics have a significant impact on criminal investigation. This requires an examination of whether the fair trial principle remains valid in the new area (Stoykova, 2022).

3 MATERIALS AND METHODS

Modern computers and digital devices process information only in digital form, not only in two-, but also in multi-level sampling systems for storing and transmitting information. In accordance with the operating principle of digital devices, information
(text, image, video, etc.) is pre-encoded and converted into digital form. When entering information, each character is encoded with its inherent combination of numbers, and when outputting, it is converted into a readable (text) or understandable (video, sound, etc.) format for the user.

As we consider it, a form of information is processed, stored on digital devices and transmitted through communication channels in two levels of discrete signals, designated as “0” and “1”. In this connection, information processed, stored and transmitted by technical means has acquired the name “digital”. Today, digital information has become generally accepted and no one by this term means recording in the Arabic or Roman number system.

The argumentation of our position is based on its technological nature, since information stored in digital devices is presented in the form of a binary number system, a system of numbers, symbols, signals that transmit information, and are of a discrete nature. “Information encoded and recorded by signals of two levels has received the conventional name “digital information” or “information in digital form”

Using the analytical method, we analyzed concepts, compared them and analyzed definitions. As a result, digital information is understood as any information presented in the form of a sequence of numbers, available for input, processing, storage, transmission using technical devices, indicating that the importance lies not in the external form and method of perceiving information, but in the way of its existence, expressed in its consolidation through digital technologies.

This definition requires some clarification, namely in terms of the absence in the definition of technical means intended for entering, processing, storing, and transmitting information. These include mechanical, electrical and other devices. At the same time, the phrase “available for input, processing, storage, transmission...” seems to us inaccurate and limited, since it limits the process of circulation of information; we believe it is appropriate to use the term “intended” in this definition.

Analyzing the above definitions of information in electronic digital form, it is necessary to highlight its distinctive features, such as ease of processing, storing and transmitting information, regardless of its medium.

A. E. Sharkov (2004) identified the following characteristics inherent in computer information:

- voluminous and quickly processed;
very easily and, as a rule, destroyed without a trace;

- impersonal;

- can only be located on machine media;

- can be created, modified, copied, applied, used only with the help of a computer;

- easily transmitted via telecommunication channels of computer networks, and almost any amount of information can be transmitted to any distance;

- relatively simple to forward, transform, reproduce; when it is seized, unlike a seized item, it is easily stored in the original source; several users can simultaneously have access to the same file containing information.

The highlighted characteristics, such as volume, ease of destruction and preservation in the original source, parallel access and impersonality, although to a lesser extent, are also inherent in other types of information. The remaining characteristic features of computer information are related to its form and features of the electronic digital environment. Based on this, we believe that the feature that determines the specificity of computer information is that it is in electronic digital form.

Being located only on computer media as a sign of computer information is now outdated, since, as we said above, the list of media has expanded. This circumstance once again emphasizes the need to use the form in relation to computer information, and not its medium. Thus, when highlighting the features of computer information, instead of indicating its carrier, we consider it appropriate to indicate its form.

Based on the method of mathematical logic, the understanding of computer information available in legislation, such factual data should be defined as information that does not have physical characteristics, stored on a medium in electronic digital form. Based on this, computer information is a form of information determined by the characteristics of the environment of its existence.

In accordance with the international standard in the field of system and software engineering, as well as modern concepts, information is considered intangible, and what is contained in the structure of objects is usually called data. In computer science, the term data is more often used, which comes from the word data - fact, and information (informatio), which means explanation, presentation, i.e. information or message. Data is a collection of information recorded on a specific medium in a form suitable for permanent storage, transmission and processing. Transformation and processing of data
allows you to obtain information. Information is the result of data transformation and analysis. The difference between information and data is that data is fixed information about events and phenomena that is stored on certain media, and information appears as a result of data processing when solving specific problems. For example, various data are stored in databases, and for a specific request the database management system provides the required information.

The concept of “data” is a relatively new term, generally characterizing a certain set of symbols that can be stored, transmitted, and transformed. Typically, data is the input or output information of any information process or system.

For example, for a computer program or algorithm, the input may be a character or a word. For a person, a telephone number is data that needs to be transmitted to the telephone exchange in order to connect with the desired subscriber. There is no need to look for deep meaning in a phone number.

In the State Standard of the Republic of Kazakhstan in the field of information technology, which we discussed above, regulating the electronic exchange of information, there is a definition of the term “data”, which is understood as “a representation of information interpreted in a formalized way, suitable for communication, interpretation or processing”

In accordance with the State Standard of the Republic of Kazakhstan regulating the technical protection of information, the term data is understood as “information presented in a formalized form suitable for transmission, interpretation or processing with human participation or by automatic means.” The same GOST provides a definition of protected information, which is understood as “information that is the subject of property and is subject to protection in accordance with the requirements of legal documents or the requirements established by the owner of the information”

Data refers to the method of representation, storage and elementary processing operations of information. First of all, data is the basis of information. Thus, data are letters, and information is a message, information that has a certain meaning.

It should also be noted that in the legislation of foreign countries the term “data” is used in relation to information on electronic (machine) storage media.

Thus, in accordance with the report “Computer and other crimes against information technology in Canada,” which is followed in the United States and the Netherlands, the differences between the concepts of “information” and “data” are
important not only for technological, but also for legal reasons. The main premise of the position under consideration is that information is not a thing, but a process or relationship that occurs between consciousness and a certain stimulus. Data is a simple representation of information. Information is the result of interpretation of observed data. Depending on the interpretation, different information can be obtained from the same data, for example, the set of numbers "01010110" has no meaning until they are interpreted or assigned a meaning.

If data is lost or stolen, only the representation is lost or stolen, not the information. To obtain information, it must first be interpreted and deciphered. According to D. K. Piragoff (1992), awareness of the difference between “information” and “data” is a mandatory and important component for the development of legislation in the field of computer offenses and misappropriation of information.

Taken as a basis by the legislation of most European states, this definition is used in the formulation of definitions in national legislation. For example, Article 80 of the Dutch Criminal Code states that the term “data” “may be used to designate any representation of facts, concepts or instructions, whether agreed upon or not, capable of being communicated, interpreted or processed by human beings or computer devices and systems”.

4 RESULTS AND DISCUSSION

The issue of the relevance of the fight against cybercrime at the international level arose a long time ago, so in 2001 the European Convention on Computer Crime was prepared. Currently, most European countries, having brought their national legislation into conformity with the Convention, have ratified it. Noting the high level of theoretical preparation of the Convention, we consider it appropriate and necessary to be guided by its provisions when developing national legal acts in the field of combating cybercrime, as well as analyzing current problems. We would like to note that the Convention was adopted in 2001, later its name was changed as the “Convention against Cybercrime”.

According to Article 1 of the Computer Crime Convention, “computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system, including programs capable of causing a computer system to perform a particular function. When assessing computer data, European legislators are based on the form of their presentation, and not on their location.
Based on this, it follows that information entered into a computer (information system, telecommunications network, etc.) and translated into “computer language” will be data. The considered opinion also corresponds to the understanding of information proposed in this work, i.e., information transmitted between subjects through formalized language. Programming and data processing languages, along with the languages of the world, can be translated and comprehended.

The relevance of the issue of ratification of this Convention is beyond doubt; the conclusions we propose will only simplify its understanding and will contribute to its ratification.

The operation of modern digital devices is based on millions and billions of transistors that exchange electromagnetic signals. The human brain is unable to predict the behavior of such systems by constructing equations that describe the movement of each electron in each transistor of the system, and then solving this system of equations.

For convenience and simplicity of the concept of the operating principle of modern digital devices, some abstraction is required in representing the process of operation of a complex system of digital devices. Abstraction allows you to manage a complex system and implies the exclusion from consideration of those elements that are unimportant in a particular case. Abstraction from unimportant details allows the user, i.e., us, not to think about the quantum oscillations of electrons or the organization of computer memory as a result of its operation.

It should also be noted that managing a complex system has three fundamental principles, such as:

- the principle of hierarchy, which involves dividing the system into separate modules, as well as into fragments to a level that makes it easy to understand the behavior of each specific fragment;
- the principle of modularity, which requires each module in the system to have clearly defined functionality and a set of interfaces, as well as the ability to connect with other modules;
- the principle of regularity, which requires compliance with uniformity when designing individual modules of the system.

It should be understood that computer data is not a special or separate type of information; it acts as a source of information, a source of evidentiary information. And
in order for computer data to acquire evidentiary value, it must first be converted into a human-perceivable form.

Information is not just the result of reflection, not just knowledge. It is precisely messages, information, that is, knowledge that is needed and has a consumer. Only by interacting with the consumer does knowledge acquire the character of a message, information, i.e., it becomes information.

It should also be taken into account that numbers and symbols of natural language or their encoded representation in the form of a string of binary bits are components of data; based on this, we consider it appropriate and appropriate to use the term “data” in relation to information in electronic digital form.

Thus, the domestic legislator defines computer information based on its medium (electronic media), while European legislators understand computer data as any representation of information in a form suitable for processing by computers.

Another important conclusion from the differences in the understanding of information is that, in accordance with the domestic understanding of information, it can be a type of information, and in the foreign understanding, computer data is a form of presenting information.

Form (Latin forma, Greek μορφή) is a concept of philosophy, defined in relation to the concepts of content and matter. In relation to content, form is understood as the orderliness of content - its internal connection and order. In relation to matter, form is understood as the essence, the content of knowledge about existence, which is the unity of form and matter. At the same time, the spatial form of a thing is a special case of form as the essence of a thing.

So, if computer information is a certain code, it would be correct to talk about it as a certain form of representation, rather than about its type. Electronic digital data acts as a shell for the content of information.

We believe that when considering data in electronic digital form, the form of its existence is of primary importance, and the location and content of the information fade into the background. For example, in transport crimes, the purpose of vehicles is to transport people and goods, in the event of a traffic accident, the transported people or goods suffer (Nurkhan, 2018). However, these circumstances do not give us grounds to classify this incident as a crime against person or property. Accordingly, data in electronic digital form is intended to transmit information through media, information systems and
telecommunication networks, and in the event of a crime being committed against them, their protection is of primary interest, and the nature and content of this data fades into the background.

So, in our opinion, electronic digital data is information in electronic digital form, suitable for communication, interpretation or processing.

In the electronic digital environment, the main interacting objects are various kinds of information objects (data sets, files, programs, etc.), which have a complex hierarchical structure, when analyzing which it is impossible to talk about any of its external structure.

V. A. Meshcheryakov (2004) proposes replacing the term “computer information” with “electronic digital object”, by which he means “a labeled system of discrete electronic signals intended to designate (according to an established coding system) any information and presented in a form suitable for its automated processing, storage and transmission using computer technology.”

In accordance with the Handbook for law enforcement, special agencies and courts on the appointment of forensic examinations to the Forensic Examination Center of the Ministry of Justice of the Republic of Kazakhstan, the objects of forensic examination of computer technology are:

1) hardware objects;
2) software objects;
3) information objects;
4) objects containing information necessary for conducting expert research.

Under software objects of forensic examination, system software is indicated (various operating systems for personal computers and local networks MS-DOS, UNIX, Windows of various versions, etc., auxiliary programs - utilities, tools for developing and debugging programs, service system information, etc. Under the information objects are files prepared using the above and other software tools (with extensions of text formats .txt, .doc, graphic formats .bmp, .jpg, .cdr, database formats .dbf, .mdb, spreadsheets .xls, .cal, etc.); data in multimedia formats.

The legislation provides various complementary definitions of each other. To summarize, we come to the conclusion that the sources of information in electronic digital form (environment), reflecting changes under the influence of criminal actions and containing potential information about the circumstances of the event under investigation,
are units of named data (such as a file, a program intended for exchange or performing various functions with data).

Thus, by sources of information in the electronic digital environment we understand data in electronic digital form that reflect changes due to the impact of a crime event and contain potential information about the circumstances of the event under investigation.

But if we approach the issue of electronic evidence from the other side. Of particular interest are screenshots of correspondence in instant messengers (WhatsApp, Telegram, Viber, etc.), since they can be easily changed and corrected. In the conditions of the modern world and digital capabilities, it is quite easy to falsify information located, for example, on a screenshot. In addition, new variations of digital evidence are emerging, but the legislator still does not regulate their concept, types, and evaluation criteria have not been developed. Moreover, a screenshot is sometimes equated with a photograph; this approach is fundamentally incorrect, since there are differences in the mechanism for creating photos and screenshots. In addition, the issue of the relevance of a “screenshot” to a specific type of evidence has not yet been resolved. There is also no consensus in the legal literature. As a rule, a screenshot is classified as written or physical evidence. There is no clear distinction in the legislation.

One of the problems of cognition of electronic evidence lies in its wide variety, which is determined by the level of scientific and technological development and the degree of use of various technological means in the everyday life of people. This, in turn, determines the widespread dissemination of digital information that can be used in evidentiary activities, in many cases becoming no alternative means of proving the circumstances of the case, on which the results of its consideration by the court depend.

We would also like to consider the criteria for dividing electronic evidence into groups. Depending on who records the electronic information, electronic evidence is divided into the following groups:

Electronic evidence, the content of which is recorded by the court. The possibility of recording electronic evidence directly in court is a novelty in procedural legislation. Its existence is due to the need to simplify for participants the procedural possibility of using electronic evidence obtained from the Internet.

Electronic evidence, the recording of which is carried out by the parties to the case. In general, the existence of such a group is clear. Proof of the circumstances to
which the participant in the proceedings refers as the basis for his claims and objections must be carried out using means of evidence, which may also be electronic. At the same time, the problem of recording electronic evidence by the participants in the proceedings lies in the absence of the procedure prescribed by law recording electronic evidence. For example, an electronic document can be printed and provided to the court in written form, which will be considered a paper copy of the electronic evidence. At the same time, such types of electronic evidence as audio or video recordings cannot be printed, but presentation in court is carried out either in the original or in a copy reproduced using technical means. Electronic evidence, the content of which is recorded by special entities. The use of electronic evidence, in addition to the court and the parties to the case, can be assisted by other special entities. For example, in some cases, the correct handling of electronic evidence requires the use of special knowledge (carrying out forensic computer-technical examination). It can also be noted that the current legislation is possible to engage a notary to record electronic information.

Based on global judicial and law enforcement practice, blockchain technology, as well as metadata analysis, can be used for these purposes, along with the electronic signature, which is not used in all electronic documents.

It is a relatively new technology that can increase the degree of trust in electronic evidence and its security. It can be defined as a distributed ledger that refers to a list of records (blocks) that are linked and protected by cryptography and recorded on a decentralized peer-to-peer network. By its structure, blockchain is resistant to data changes.

For example, in Chinese law, changes were made to the civil procedural code regarding electronic evidence quite a long time ago. The legislator determined in 2012 that evidence in a case can be presented in the form of electronic documents, messages and emails exchanged through digital devices. It can also be information that is published through online platforms, blogs, web pages and much more.

5 CONCLUSION

In conclusion, it should be noted that the improvement of science and technology leads to the fact that the progressive type of evidence will be electronic evidence, therefore they need to be separated into a separate category means of proof:
1. It is necessary to make appropriate changes and additions to the Code of Criminal Procedure, namely the inclusion of “computer information” in Article 118 of the Code of Criminal Procedure as an independent means of proof.

2. To make changes and additions to Article 15 of the Law of the Republic of Kazakhstan “On Communications”, to Article 254 of the Code of Criminal Procedure of the Republic of Kazakhstan on ensuring the operational safety of computer data for use as evidence. (поменяла местами, так как во введении обозначила задачи и вот их выводы согласно тому порядку что во введении)

3. Introduce an addition to Article 254 of the Code of Criminal Procedure of the Republic of Kazakhstan on the possibility of copying computer data documents without seizure and providing them as electronic evidence.
REFERENCES


