Ivane Javakhishvili Tbilisi State University
Faculty of Law

Journal of Law

№1, 2021

უნივერსიტეტის გამომცემლობა

Tornike Khidesheli*

On the Issue of Computer Data Concept, Its Characteristics and Authenticity

This letter addresses a topical issue such as computer data and its use in criminal proceedings. Given, which is completely different from the traditional evidence and due to its specific and technical characteristics has become a significant challenge for the legal community. Comprehending its content, demonstrating the distinction between material and electronic documents, and determining the authenticity of electronic data turned out to be complicated. Accordingly, the paper aims to research the essence of computer data, identify its features and outline the prerequisites for authenticity.

Keywords: *Computer data, Computer system, Digital evidence, Electronic evidence, Authentication of computer data*.

1. Introduction

The rapid growth of technology and its establishment in society often outpaces their inclusion in legal frameworks. Computer data is a clear example.

Although computers have been around for a long time, just 20-30 years ago its use in the interests of the investigation was a notable event. Occasionally, its importance has increased and today it has become an integral part of the investigation.[1] As result words related to computers, such as computer data, electronic and digital evidence, etc. have emerged in different legislations. It is noteworthy that these words attracted the attention of many international organizations and it took quite a long time to determine their exact and comprehensive content. Compared to other countries, computer data and related investigative actions are novel for Georgian procedural legislation. It is currently on the path of development and thus there is a lack of information in the Georgian legal literature. [2] This deficiency creates some legal obstruction both in terms of investigation and case law.

Also, authentication of computer data became a point of contention. The legal basis for discussion was its characteristic features. Some scholars consider that new legislation is required for electronic data,[3] but others think that regardless of the nature of digital data it is possible to apply the rules which have been developed concerning the authentication of traditional evidence.[4] Worthy of

---

* Doctoral student, Visiting Lecturer at Ivane Javakhishvili Tbilisi State University, Faculty of Law.

1 *Kerr S. O.,* Searches and Seizures in a Digital World Harvard Law Review, Vol. 119, 2006, 1.

2 *Meurmishvili B*., Georgian Criminal Procedure Law, Special part, *Papiashvili L. (eds.),* Tbilisi 2017, 534-539. (in Georgian). *See: Toloraia L.,* Commentary on the Criminal Procedure Code of Georgia, *Giorgadze G. (eds.),* Tbilisi, 2015, 422-425 (in Georgian).

3 *Brenner W. S., Frederiksen A. B.,* Computer Searches and Seizures: Some Unresolved Issues, Michigan Telecommunications and Technology Law Review, Vol. 8, Issue 1, 2002, 60-63, 80-82.

4 *Clancy K. T.,* The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and A Primer, Mississippi Law Journal, Vol. 75, 2005, 193.

attention that the extraction of computer data is differently regulated by the Georgian Criminal Procedure law and establishes some procedural restrictions, which is partially caused by the international law and but a mostly superficial understanding of the essence and features of computer data.

According to the urgency of the issue, the purpose of the article is to fill information scarcity to some extent, examine computer data, identify hallmarks of electronic evidence, and given the legal literature and the experience of different countries outline challenging issues related to its authenticity.

2. The Essence of Computer Data

The intensive development of information and communication technologies has led to the introduction of investigative actions related to obtaining electronic evidence. Since without such a procedural tool it would have been virtually impossible to obtain relevant information of the case and its use in the evidentiary process, accordingly with foreseeing of the Convention on Cybercrime, the actions related to computer data had been depicted in XVI chapter of Criminal procedure code of Georgia.[5]

Consequently, new words appeared in criminal procedure law, such as computer system, computer data, service provider, internet traffic, etc. Due to their technical and specific features, an accurate and in-depth understanding of their content was difficult not only for the interested persons but also for the lawyers. Therefore, we will try to make the contents of the computer system and data more intelligible for them.

It is noteworthy that the definition of computer data is given both in the Convention on Cybercrime and in the Criminal Procedure Code of Georgia. The definitions given in both sources are identical and look like this: "Computer data – means the information displayed in any form convenient for processing in a computer system, including software that ensures the operation of the computer system" [6]

To understand the essence of computer data it would be better to discuss it in detail. Firstly, let's explain what the computer system means. The definition is identical in both of the above-mentioned documents and looks as follows: "A computer system is any mechanism or a group of interconnected mechanisms which through the software automatically process data". Like the definition in national legislation, the Convention on Cybercrime focuses on automatic data processing, which indicates that the process is managed through the program.[7] In turn, the definition of computer data contains the term "suitable for processing" which means that the data is put in such a form that it can be directly processed by the computer system. [8]

---

5 *Meurmishvili B*., Georgian Criminal Procedure Law, Special part, *Papiashvili L. (eds.),* Tbilisi 2017, 534 (in Georgian).

6 Criminal Procedure Code of Georgia, LHG, 03/11/2009. Convention on Cybercrime (Budapest Convention), 23/11/2001.

7 The Explanatory Report to the Convention on Cybercrime, European Treaty Series – № 185, Budapest, 23/11/2001, 5.

8 Ibid.

A computer system should be considered as a combination of two elements: hardware and software.[9] It consists of a variety of devices, but CPU, data storage, and software are the main components.[10]

CPU – is the functional core constituent of any electronic device, which receives the data, performs logical-arithmetic operations[11] and produces an output that may be displayed on the screen[12], passed to a local storage facility or uplinked via a network connection to another device.[13]

Software – consists of programs that give instructions to the digital device. There are two main categories of software: system software and application software. [14] As the name suggests, the system software is required for the basic operation of a device. It performs the basic function of connecting to devices, folders, and application software. [15] Application software – is "special purpose" software that enables the user to undertake specific kinds of tasks on the computer. These include web browsing, email, social networking, and so on.

Data storage devices – information storage media are mainly hard disk and RAM. Any program that ensures the functioning of the computer runs in RAM. RAM includes the information which is being processed and data will not be saved if the power is disconnected. That's why it is called volatile storage. Therefore, law enforcement attempts to capture data in RAM before disconnecting the power during computer searches. This is commonly known as "Live Data Forensics".[16]

Unlike RAM, a hard drive disk is a permanent memory and if the device is disconnected from the power supply, information on it is not lost. [17] Since it is non-volatile, it is a significant source of computer data (afterward electronic evidence).

Also, computer data may be stored in differpaent storage facilities. For example compact disk, memory sticks da, etc. Besides, data may be stored remotely on "cloud" facilities.[18]

By summarizing, we can conclude that a computer system is a device, which integrates one or several active parts and at least one of them automatically receives, processes, and transmits data through the software.

---

9 *Stanfield R. A.,* The Authentication of Electronic Evidence, Queensland University of Technology, Australia, 2016, 61.

10 *Mason S., Weir R. S. G.,* The Sources of Electronic Evidence, 4th ed., Institute of Advanced Legal Studies, *Mason S., Seng D. (eds.),* London, 2017, 1-5. *Otkhozoria V., Tsiramua Z., Svanishvili Sh*., Supporter Specialist of Information Technology*,* Tbilisi, 2015, 8 (in Georgian).

11 Input consists of words, numbers, images, sounds, or a combination of the above. Keyboard, compact disk, mouse, scanner, digital camera, internet, etc. are frequently used for storing data in computers.

12 A common device used to output information is a printer and a voice adapter. Also, floppy disk, storage media, etc. If the computer is connected to the network, it can be considered as an output device.

13 *Mason S., Weir R. S. G.,* The Sources of Electronic Evidence, 4th ed., Institute of Advanced Legal Studies, *Mason S., Seng D. (eds.),* London, 2017, 1.

14 Ibid, 2.

15 *Otkhozoria V., Tsiramua Z.,* Information Technology, Tbilisi, 2015, 226 (in Georgian).

16 *Council of Europe,* Cybercrime Training for Judges, 2010, 35, <https://rm.coe.int/16802fa028> [23.02.2021] (in Georgian).

17 *Mason S., Weir R. S. G.,* The Sources of Electronic Evidence, 4th ed., Institute of Advanced Legal Studies, *Mason S., Seng D. (eds.),* London, 2017, 4.

18 Ibid, 5.

To such an extent, we have talked about computer systems, but the content and essence of computer data are of interest. According to the definition of the Code of Criminal Procedure and the Convention on Cybercrime, computer data means any representation of information or facts in a form suitable for processing in a computer system, including a program to perform its function. [19]

It is important to determine whether computer data can be considered as a document. For criminal proceedings, a document is any source in which information is recorded in the form of words and signs and or photo-, film-, video-, sound or through other technical means. [20] To perceive the connection between these independent terms and to discuss the issue in-depth it would be better to look at the experience of other countries. In this regard, it is interesting how the document is interpreted in different jurisdictions. For example, according to Australian legislation, a document is any source of information where signs, figures, symbols, photos, and drawings are depicted.[21] Also, compact disk, audio files, and more.[22] And this definition of a document is broad enough to include computer data/electronic information.

As for the United States Criminal Procedure law, unlike Civil Procedure, it does not contain a definition of document.[23] However, Federal Rules of Criminal Procedure define the "Property" which includes material objects like documents and records as perceptual and comprehensible information.[24] And the Evidence Code of California considers any representation of information as a document, regardless of where and in what form is stored. For instance, manuscript, photo-audio, and more.[25]

In this regard, Canadian legislation has gone further and separately defines „electronic document". According to Canada Evidence Act, electronic documents are – data that is recorded or stored by the computer system or other similar device and that can be read or perceived by a person or any medium.[26]

In the legislation of England and Wales, 'Data' is defined as information stored in a computer system for further processing, that is processed automatically and that information is part of the system.[27]

An analysis of the legislation of different countries has shown us that the contents of computer/electronic data are resembling. Similar to the legislation of Georgia, in other jurisdictions, the document is widely explained and covers electronic information. However, in foreign legal literature instead of "Computer data or Electronic information," it is used "Digital or Electronic Evidence'. And its definition is offered by lots of international organizations. To cite an example, the definition proposed by the Scientific Working Group on Digital Evidence (SWGDE) defines 'Digital Evidence' as information of probative value that is either stored or transmitted in binary

---

19 Criminal Procedure Code of Georgia, LHG, 03/11/2009. Convention on Cybercrime (Budapest Convention), 23/11/2001.
20 Ibid, Article 3(23).
21 Evidence Act, 23/02/1995; Acts Interpretation Act 1901 (Amendment of 14/01/2019).
22 Evidence Act, 23/02 1995.
23 Federal Rules of Civil Procedure, 20/12/1937.
24 Federal Rules of Criminal Procedure, 26/12/44.
25 Evidence Code of California, 18/05/1965.
26 Canada Evidence Act, 1985.
27 Data Protection Act, 16/ 07/1998.

form.[28] Another definition proposed by the International Organization of Computer Evidence (IOCE) is – information stored on transmitted in binary form that may be relied upon in court.[29] When the above-mentioned organizations are interpreting the concept, they focus on the probative value of electronic data not its importance during an investigation.[30] But a broader definition is proposed by the Association of Chief Police Officers (ACPO) and 'Digital Evidence' is information and data of investigative value that are stored on or transmitted by a computer.[31] A similar notion has the National Institute of Justice (NIJ) that 'Digital Evidence' is information and data of value to an investigation that is stored on receive, or transmitted by an electronic device.[32]

Since our goal was to determine the essence of computer data, first of all, it was essential to understand the nature of computer systems in depth. While working on the issue, it was revealed that to consider a device like a computer system, it is mandatory to have it 1. CPU (Central Processing Unit) – an integral device that performs computational operations and processes information; 2. Software – which provides relevant instructions for the operation of an electronic device; 3. Data Storage Facilities – where processed information is stored.

These are the three core components of a computer system. For a computer to be able to create computer data, store, process, or transmit, human resources are required. Human, who is the creator and user of all above-mentioned property. Thus, we can conclude that computer data is any information entered by the user into the computer system, then automatically processed, stored, or transmitted by the electronic device. And electronic/digital evidence is – computer data available in computer systems that are valuable to the investigation or to a party to the proceedings to prove important circumstances in court.

3. Characteristics of Computer Data

It is noteworthy that electronic evidence and computer forensics are relatively recent additions to the means of proof in legal proceedings. Unlike other forensic disciplines, digital evidence has caused controversial discussions among legal professionals.[33] Besides, different legal systems approached in various ways to this new challenge. Some systems have introduced new legislation to specifically address electronic evidence. Others try to establish a 'closest match' to existing legislation and have applied wherever possible existing rules analogously.[34]

The adoption of the new legislation was due to the difference between electronic and traditional forms of evidence. And where analogous approaches are used, the emphasis is on the similarities

---

28 Scientific Working Group on Digital Evidence (SWDGE), SWGDE Digital and Multimedia Evidence Glossary, 2016, 7, <https://www.swgde.org/documents/published> [20.02.2021].

29 *Casey O.*, Digital Evidence and Computer Crime, 3rd ed., USA, 2011, 7.

30 Ibid.

31 Ibid.

32 *Goodison E. S., Davis C. R., Jackson A. B.*, Digital Evidence and U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence, NIJ, USA, 2015, 3.

33 *Schafer B., Mason S.*, The Characteristics of Electronic Evidence, Electronic Evidence, 4th ed., Institute of Advanced Legal Studies, *Mason S., Seng D. (eds.),* London, 2017, 18.

34 Ibid.

between traditional and digital evidence.[35] If we share this notion, separation of the chapter of computer data-related investigative actions in the Criminal Procedure Code of Georgia and applying provisions of secret investigative actions on them should be explained not only by the ratification of the Convention on Cybercrime but also by the fundamental differences between electronic and traditional evidence.

The legal literature focuses on lots of features of electronic evidence. According to scientists, electronic evidence is latent in the same sense as fingerprints or DNA evidence can transcend borders with ease and speed[36], can be easily altered.[37] Therefore, compared to material evidence it requires precautious treatment.[38]

A particularly important form of evidence in all developed legal systems is proof by the document. The same can be said for electronic ones. Herewith, comparing a written document to an electronic document is the best way to illustrate the characteristics of electronic evidence.[39] Especially when electronic documents have the same visual appearance as documents typed on paper. It is possible to turn their pages, put them in folders and discard them in baskets. And this inauthentic familiarity can create the misleading impression that the electronic document maintains its structural integrity even when the file is closed or the computer switched off, in the same way, a paper document continues to exist when we put it into a folder.[40] This does not necessarily mean that an electronic document is inevitably fake or unreliable. However, due to its characteristics confirmation of its authenticity requires accurate and consistent verification.[41]

When talking about the main features of electronic evidence, we should not forget the Sedona Conference Working Group[42], which has made great efforts to determine its characteristics. According to their notion, the fundamental distinction between electronic and written documents can be grouped into the following six categories: Metadata; Volume and duplicability; persistence; dynamic – changeable content; environment dependence and obsolescence; dispersion.[43]

---

35 Ibid.

36 *Mukasey B. M., Sedgwick L. J., Hagy W. D*., Electronic Crime Scene Investigation: A Guide for First Responders, National Institute of Justice, USA, 2008, 9.

37 *Gonzales R. A., Schofield B. R., Hagy W. D*., Investigations Involving the Internet and Computer Networks, National Institute of Justice, USA, 2007, 2. See*, Casey E*., Foundations of Digital Forensics, Digital Evidence, and Computer Crime, 3rd ed., USA, 2011, 26.

38 *Goodison E. S., Davis C. R., Jackson A. B*., Digital Evidence and U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence, NIJ, USA, 2015, 3.

39 *Schafer B., Mason S.*, The Characteristics of Electronic Evidence, Electronic Evidence, 4th ed., Institute of Advanced Legal Studies, *Mason S., Seng D. (eds.),* London, 2017, 20.

40 Ibid.

41 Ibid, 21.

42 The Sedona Conference – A non-profit, research, and educational institute that was founded in 1997 by *Richard G. Braman.* The Sedona Conference has several working groups, including "Electronic Document Retention and Production" Working group dedicated to the development of guidelines and standards about electronic information management, discovery, and disclosure, <https://thesedonaconference.org/> [20.02.2021]

43 *Diana J. A., Esteban A. A., Guglielmo P. J., Hiser S. T., Kuckelman D., Mandel P. E., Opstnick M. T., Ragan R. C., Sharp C. D., Tully T. M.,* The Sedona Principles, Best Practices, Recommendations &

3.1. Metadata

Metadata is data about data.[44] This is an additional source of information, which includes the content, category, ownership, format, creation, and methods, location, conditions for its use, etc. It should be noted that this list is not exhaustive, as metadata is generated both by the user of the device and automatically by the software and this kind of information can be diverse.[45] Metadata created automatically by the software is more difficult to alter, manipulate or delete. The reason is its invisible nature. Imagine a user creating an electronic document. The software will add metadata about the time when the document is created, who is the author, and where the document is stored. Since it is invisible to the user, he/she may not only know how to alter or delete it but also about its existence.[46]

The metadata may not be infallible.[47] Its authenticity depends on the proper functioning of the computer system as well as other external factors.[48] For more clarity, imagine a device, which time zone is not accurate. Consequently, the metadata about the time of creation will be false.[49] The same can be said about the author of the document. If the computer system is used by the third-party and the latter uses an account registered by the owner, any actions taken by him and related metadata belong not to the owner of the account, but to a third party who uses the device.

In summary, metadata is an integral part of any electronic document[50] and unlike a written document it only characterizes it. Because it is an automatic, software-generated artifact, the difficulty is both to delete it and to obtain it without damage. Besides, its authenticity significantly depends on the proper functioning of a computer system as on other circumstances.

3.2. Volume and Replication

Despite the existence of physical-geographical boundaries, the development of computer technology and telecommunications has led to the rapid exchange of information. Once computers are networked together, a greater volume of information can be rapidly distributed around the world. Internet communications, social networks, and email provide prominent examples. These not only

---

Principles for Addressing Electronic Document Production, 3rd ed., The Sedona Conference Journal, Vol. 19, № 1, 2018, 207.

44 *Riley J.,* Understanding Metadata, National Information Standards Organization, Baltimore, MD, 2017, 1.

45 *Schafer B., Mason S.*, The Characteristics of Electronic Evidence, Electronic Evidence, 4th ed., Institute of Advanced Legal Studies, *Mason S., Seng D. (eds.),* London, 2017, 27.

46 Ibid.

47 *Diana J. A., Esteban A. A., Guglielmo P. J., Hiser S. T., Kuckelman D., Mandel P. E., Opstnick M. T., Ragan R. C., Sharp C. D., Tully T. M.,* The Sedona Principles, Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 3rd ed., The Sedona Conference Journal, Vol. 19, № 1, 2018, 211.

48 *Schafer B., Mason S.*, The Characteristics of Electronic Evidence, Electronic Evidence, 4th ed., Institute of Advanced Legal Studies, *Mason S., Seng D. (eds.),* London, 2017, 28.

49 Ibid.

50 *Stanfield R. A.,* The Authentication of Electronic Evidence, Queensland University of Technology, Australia, 2016, 64.

allow data to be transmitted quickly but multiply it indefinitely. For more clarity, email users frequently send the same email to many recipients. These recipients, in turn often forward the message to others. At this time, numerous copies of the email are created.[51]

By way of example, in *AMP v Persons Unknown*[52], the claimant lost his/her phone, and the number of photographs stored in the phone was sexual in nature. Shortly after the telephone was stolen, images were uploaded on various social media websites and enabled others to download and share the images. As a result, the photographs covered the entire Swedish internet space. Another proof of easy duplication of electronic information is the creation of a data backup by the computer system. The purpose is to restore the original in case of data loss.[53]

Along with duplicating electronic documents the issue of its volume is noteworthy. If previously a certain amount of written material could occupy a large area, now the same or larger volume of stuff can be stored electronically on smaller devices. With the development of technology, storage media is becoming more easily accessible, which means customers are available to keep the desired amount of data for an indefinite time.

A common form of information storage is 'cloud computing' technology, which involves outsourcing electronic documents to third-party servers. Along with the benefits of decentralized storage of information, the cloud leads to legal issues such as jurisdictional and data ownership.[54] In this regard, the user faces the obstacle when deleting or destroying information, because erasing in the electronic environment does not mean expunged.[55] Consequently, the danger of infringement of the right to privacy by improper and illegal handling of digital documents by the service provider still exists.

Thus, we can convincingly say that the volume and replication indicate a significant difference between traditional and electronic documents. And above mentioned provides a basis for the exceptional and cautious treatment of electronic evidence by investigative bodies and the judiciary.

3.3. Persistence

We have talked about several features of computer data and electronic documents, but persistence is another distinguishing quality from written documents. By comparing material and electronic documents, it becomes clear that electronic documents are more difficult to dispose of than

---

51 *Diana J. A., Esteban A. A., Guglielmo P. J., Hiser S. T., Kuckelman D., Mandel P. E., Opstnick M. T., Ragan R. C., Sharp C. D., Tully T. M.,* The Sedona Principles, Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 3rd ed., The Sedona Conference Journal, Vol. 19, №1, 2018, 208.

52 *AMP v. Persons Unknown*, [2011] EWHC 3454 (TCC).

53 Back up Data, Nonprofit Technology Collaboration, 2013, 1, <https://www.baylor.edu/content/services/document.php/192120.pdf> [23.02.2021].

54 *Schafer B., Mason S.*, The Characteristics of Electronic Evidence, Electronic Evidence, 4th ed., Institute of Advanced Legal Studies, *Mason S., Seng D. (eds.)*, London, 2017, 26.

55 Ibid, 25.

paper ones. Paper documents can be destroyed by shredding or burning, whereas it is not relevant for electronic documents.[56]

The term 'Deletion' can be misleading in the context of electronic data because it does not equate to the "destruction" of data from storage devices.[57] To better understand the issue, the examination of the electronic data storage principle is a leading option. Whenever a file is stored on a computer system, it keeps an index of the location and when a user retrieves the file, the computer looks up the location of the file in the index and knows from which sector to obtain the file. And when a user "deletes" the file, the computer system only removes the file reference from the index, not expunge data. Therefore, if the old data is not overwritten by a new one, the 'deleted' data is still able to be retrieved by a computer forensics expert.[58] Except for overwriting, the only way to effectively destroy electronic evidence is through applying heat or by magnetic destruction.[59]

Thus, it is obvious that electronic documents are durable and their destruction is related to certain difficulties, which emphasizes the need for peculiar treatment by law enforcement agencies.

3.4. Dynamic and Changeable Content

Dynamic and changeable content is one of the fundamental characteristics of electronic data. Electronic documents, unlike paper ones, have content that is designed to change over time even without human intervention.[60] For example computer systems that automatically update files and transfer data from one location to another. Also, an email that automatically and periodically updates information about notifications and destroys old data.[61]

It is noteworthy that electronically stored information can be modified in numerous ways that are sometimes difficult to detect without computer forensics expertise. To give an example, the act of moving an electronic document from one location to another may change creation or modification dates and it can be found in the metadata.[62]

To sum up, we can conclude that examination of computer data requires special care and computer forensic is inevitable for determining its reliability. Besides, in response to its dynamic and changeable nature, the Convention on Cybercrime provides legal tools like Expedited Preservation of

---

56 *Stanfield R. A.,* The Authentication of Electronic Evidence, Queensland University of Technology, Australia, 2016, 65.

57 *Diana J. A., Esteban A. A., Guglielmo P. J., Hiser S. T., Kuckelman D., Mandel P. E., Opstnick M. T., Ragan R. C., Sharp C. D., Tully T. M.,* The Sedona Principles, Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 3rd ed., The Sedona Conference Journal, Vol. 19, № 1, 2018, 209.

58 *Stanfield R. A.,* The Authentication of Electronic Evidence, Queensland University of Technology, Australia, 2016, 65-66.

59 Ibid.

60 *Diana J. A., Esteban A. A., Guglielmo P. J., Hiser S. T., Kuckelman D., Mandel P. E., Opstnick M. T., Ragan R. C., Sharp C. D., Tully T. M.,* The Sedona Principles, Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 3rd ed., The Sedona Conference Journal, Vol. 19, № 1, 2018, 209.

61 Ibid.

62 Ibid.

Stored Computer Data and Expedited Preservation and Partial Disclosure of Traffic Data,[63] which are not yet reflected as independent investigative actions in the Criminal Procedure Code of Georgia.

3.5. Environment-Dependence

If good eyesight and knowledge of the language are sufficient to read material documents, it is not enough in the case of electronic records. This deficiency is due to its dependence on hardware and software. Moreover, a user cannot read or create, with nothing to say about alteration or damage.[64]

To illustrate electronic document obsolescence, sending Microsoft office word documents to a third party is a good option. In most cases, the shared document does not function properly or at all. The diverse software is the main cause for that. The pace of hardware and software development has an impact on the legal process. In particular, it is difficult to follow in the footsteps of development. As noted in the legal literature, a lawyer and expert must receive constant training, which is more important than experience in this field.[65]

We also face challenges in the investigation. For example, due to the rapid change in the development of technology, it is difficult to obtain relevant evidence for an investigation. This can be caused by two reasons: first, the tools have yet to be devised, and second, because such tools can be expensive.[66]

Thus, it is obvious that hardware and software are constantly evolving, and for computer data to become perceptible to humans, it requires the use of a range of technologies. Therefore, it can be said that the existence of electronic data without computer systems and software is excluded.

3.6. Dispersion

Due to the nature of electronic data, it is possible to create lots of copies. Thus, each of them may be located in different places. It could be Ram or a Hard drive and data storage facilities, such as compact disc, memory cards, and network servers.

Despite their locations, they look identical. Therefore, it is difficult to distinguish between the copy and the original. Besides, it may seem incredible to deal with large volumes of information, but automated methods allow you to quickly and accurately search for greater volumes of electronically stored data than any paper documents.[67]

Consequently, due to the dispersion of the electronic document, the only way to identify the original one among the documents with identical content is computer forensics.

---

63 Convention on Cybercrime, Budapest, 23.11.2001, Art. 16-17.

64 *Schafer B., Mason S.*, The Characteristics of Electronic Evidence, Electronic Evidence, 4th ed., Institute of Advanced Legal Studies, *Mason S., Seng D. (eds.)*, London, 2017, 21.

65 Ibid, 23.

66 Ibid, 24.

67 *Diana J. A., Esteban A. A., Guglielmo P. J., Hiser S. T., Kuckelman D., Mandel P. E., Opstnick M. T., Ragan R. C., Sharp C. D., Tully T. M.,* The Sedona Principles, Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 3rd ed., The Sedona Conference Journal, Vol. 19, № 1, 2018, 213.

4. Authentication of Computer Data

According to criminal procedure law, the alleging process consists of obtaining evidence, affixing it to the proceedings, examining and evaluating it.[68] The importance of each of them is special, but we will mainly focus on evaluating the process of electronic evidence.

It is noteworthy that the evaluation process of evidence lasts at all stages of proceedings, although ultimately, only the court can determine its true value. [69] To some extent parties, but the court is authorized to cumulatively assess the evidence with relevance, admissibility, and reliability.[70] Evidence is relevant if it has any tendency to prove something material to the case.[71] Based on the principle of negative enumeration, the evidence is admissible if there are no grounds for excluding them.[72] As for the reliability of evidence, it includes trustworthiness and authentication.[73] And the authentication is the capacity to prove that the evidence is what it purports to be.[74]

In the legal literature, the authentication of computer data is compared with material documents. Some scientists believe that rules which have developed concerning the authentication of evidence, particularly documentary evidence are to electronic data,[75] but others consider that due to its features stricter foundation or new rules are essential.[76]

The best way to comprehend the diversity of opinions existing in scientists and challenges facing the authenticity of electronic documents is by comparing national legislation to foreign ones. It should be noted that the legislation on the electronic evidence of the United States of America and Canada is similar. According to the Federal Rules of Evidence and Canada Evidence Act, witness testimony, indirect evidence, and proof that indicates the integrity of the data are the means of establishing authenticity.[77] A party who decides to use electronic evidence in court must provide the court with information about the nature, source, and integrity of the record.[78] The source of electronic documents affects its authenticity as reliability. Data storage facilities, whether it is the hard drive or

---

68 *Tumanishvili G.,* Criminal Process – Overview of General Part, Tbilisi, 2014, 225-226 (in Georgian).

69 *Papiashvili L.,* Commentary on the Criminal Procedure Code of Georgia, Tbilisi, 2015, 288 (in Georgian).

70 Criminal Procedure Code of Georgia, LHG, 03/11/2009.

71 Federal Rules of Evidence, Article IV, Rule 401, 20/11/1972.

72 Decision of July 31, 2015 № 2/2/579, Constitutional Court of Georgia on the case: "Citizen of Georgia Maia Robakidze against the Parliament of Georgia", 12 (in Georgian).

73 *Mason S.*, *Stanfield A.,* Authenticating Electronic Evidence, Electronic Evidence, 4th ed., Institute of Advanced Legal Studies, *Mason S., Seng D. (eds.),* London, 2017,193.

74 *Gonzales R. A., Schofield B. R., Hagy W. D.,* Digital Evidence in the Courtroom – A Guide for Law Enforcement and Prosecutors, NIJ, USA, 2007, 28.

75 *Mason S.*, *Stanfield A.,* Authenticating Electronic Evidence, Electronic Evidence, 4th ed., Institute of Advanced Legal Studies, *Mason S., Seng D. (eds.),* London, 2017, 193.

76 *Johnson A. M.,* Computer Printouts as Evidence: Stricter Foundation or Presumption of Reliability, Marquette Law Review, Vol. 75, Issue 2, 1992, 445.

77 Federal Rules of Evidence (USA), Rule 901(b) (1, 4, 9), (Amendment 1/12/2019). See also. Canada Evidence Act, 1985, Section 31.1-31.7.

78 *Gregory D. J.,* Authentication Rules, and Electronic Evidence, The Canadian Bar Review, Vol. 81, № 3, 2001, 531.

compact disc, or any other storage media is inherently unstable. Some data may be lost or altered over time with or without human intervention.[79] Therefore, a proponent must convince the court that the evidence is authentic and is obtained from reliable sources.[80] Precisely, the changeable content and other features of computer data are the reasons for some scholars to redefine legislation related to electronic documents.

The form of data creation is crucial for the authentication of digital evidence. Particularly, whether it is generated by a computer system or if it is produced by the user.

To determine the authenticity of electronically stored information, it is essential to identify an author and the integrity of the content. It is a little bit challenging in the case of electronic documents. To illustrate, an email is sent from the account of a specific person, although this does not mean that its author is the owner of the account. Possibly, third parties have access to the account. It is appropriate to examine the metadata, which is an integral part of an electronic record and contains data about creation, location, and methods. And this allows us to determine as the users who have access to this document,[81] as the integrity of the record. Just as great importance has an integration of evidence. Documentation is essential at all stages of handling and processing digital evidence and it should include the followings: what types of digital evidence have been collected, who handled the evidence, which tools or methods were used to collect the evidence, who had access to the digital evidence, was information password protected or not, when was evidence collected, etc.[82] Thorough and accurate documentation of the evidence will help parties to confirm the integrity and reliability of evidence. Consequently, with the documentation, where the investigative actions are described in detail and the testimonies of those involved in the process of obtaining information, it is possible to establish the integrity of electronic evidence.

Proper functioning of a computer is decisive for authentication of electronically stored information, including data recorded automatically by a computer system without human intervention. It is also noteworthy that the proper functioning of devices does not guarantee the authenticity and accuracy of the electronic evidence.[83] Possibly, the computer system does not fully function properly, but such a defect cannot affect the integrity of the document. Therefore, it is essential to provide the court with evidence describing a proper functioning of a computer system or shows that it was not operating properly, but it did not affect the production of the document or the accuracy of its contents.[84]

---

79 Ibid, 537.

80 *Capra D.,* Authenticating Digital Evidence, Baylor Law Review, № 1, 2017, 3.

81 *Outerbridge D., Siller E.,* The Admissibility of Electronic Evidence, 2015, 11, < https://www.lawinsider .com/documents/1tYTXnzcs2u> [23.02.2021].

82 *Gonzales R. A., Schofield B. R., Hagy W. D.,* Digital Evidence in the Courtroom – A Guide for Law Enforcement and Prosecutors, NIJ, USA, 2007, 28.

83 *Outerbridge D., Siller E.,* The Admissibility of Electronic Evidence, 2015, 11, <https://www.lawinsider .com/documents/1tYTXnzcs2u> [23.02.2021].

84 *Gonzales R. A., Schofield B. R., Hagy W. D.,* Digital Evidence in the Courtroom – A Guide for Law Enforcement and Prosecutors, NIJ, USA, 2007, 44.

Besides theoretical reasoning, judicial practice is interesting. In the case of *R v. Morgan*, [85] The defendant was accused of violating the terms of the fishing license. The prosecutor presented to the court the copy of an electronic permit as evidence. When establishing the authenticity of the document, the court relied upon the witness testimony, the characteristics of the document, and the lack of objection by the defendant.[86]

Also in the case of *R v. Nichols*, [87] based on Canada Evidence Act, emergency calls made by the citizen are considered as electronic documents, and for challenging its authenticity the court had drawn attention to the proper functioning of the communications and telephone systems. According to the testimony of the operator, the system was technically in order. Besides, the supervisor of the employees was at work and declared that there were no obstacles during the work. That's why the electronic record was considered authentic by the court.

As we can see, in both cases the court relied upon the testimony of the witness instead of experts' conclusions. To some extent, witness testimonies may help us to get information about the proper functioning of computers, but in the same way, it is vital to know how accurate and reliable data was presented before the court. When it comes to information automatically processed by the system itself, where no human is involved, this kind of electronic document as a final result is more accurate than the data entered by the user into the computer system. Despite this fact, we believe that this cannot be correct and in some cases, expert evidence will be required for determining the authenticity of electronic documents. The same can be said for electronically stored information.

As well, the authentication of the printout is significant. Its authentication and uniqueness like other forms of computer data are concerned with the reliability of processing and output functions. Unlike other electronic documents, the printout is presented before the court, not in digital form, but material. Thus, they are unable to examine the document in its original form. We face difficulties when examining the authenticity of unofficial documents because unlike official documents it does not have any requisites. With the help of these requisites determining the authenticity of the document requires less effort, but the printout that does not have the hallmarks and the party submits it to the court an expert evaluation will be essential to supply the court with the information on the source of evidence, the proper functioning of the device and its compliance with the original document.

To some extent, we talked about the legislation of the United States and Canada, but just as important is the approach of criminal procedure legislation of Georgia on the issue of document authentication. Even though Georgian procedural law does not contain rules about authentication, it provides the regulation on the admissibility and probative value of documents. In particular, according to article 78(1) of the Criminal procedure Code, a document has probative value if its origin is known and it is authentic. Besides, it is admissible, if a party may interrogate as a witness a person which has acquired, produced, or which held it before its submission to the court. Also, according to article 248(1) during the main hearing, only the evidence the authenticity of which can be proven shall be considered admissible.

---

85 *R. v. Morgan,* (2002), N.J., № 15, (NLPC).

86 Ibid, §22.

87 *R. v. Nichols,* (2004), № 6186, CarswellOnt 8225, (Ont. C.J.).

The origin and source of a document have an impact on its probative value as authentication. It helps us to get information about the time of creation, location, author, alteration, and other important circumstances.[88] Thus, by questioning the owner, who can provide the court and investigation with information about the origin of the document, it is feasible to establish its accuracy and authentication. Besides, the procedural law includes the rules of authentication by the testimonies of the persons who obtain and preserve it. Of course, it should be conditioned with objective circumstances.[89]

Also, its authenticity can be established by direct evidence, expert-witness testimony/report, and plenty of other methods, which are impossible to list exhaustively.[90]

Despite the different legal systems, significant similarities were identified between the means of establishing the authenticity of the document. Under all above-mentioned legislation witness testimony, forensic reports, direct and circumstantial evidence are preferred for document verification.

Besides, the case law has shown us that the rules developed for the authentication of written documents are pertinent to electronic evidence. However, it is necessary to pay attention to the features of computer data that affect its integrity. Particularly, for assessing its authenticity, it is vital to identify the author, the source of record, methods of how it is created and obtained, and also to determine the integrity of the document.

If in the course of the proceedings, the above-mentioned features are properly and thoroughly investigated, it will be possible to apply the existing rules to electronic documents, regardless of their inconstant nature.

5. Conclusion

Given the ubiquity of digital devices and our near total reliance on them, in this modern age, it is hard to imagine a crime that does not have a digital dimension.[91] The digital world, like many other fields of activity, has had an impact on the law, too. Consequently, making aware of specific issues of technology is a great of importance for lawyers.

Regarding that electronic evidence and computer data are relatively recent additions to the means of proof in legal proceedings. Its specific and technical characteristics has become a significant challenge for the legal community. So comprehending its content, demonstrating the distinction between material and electronic documents, and determining the authenticity of electronic data were main issues of the article.

As a result of analyzing foreign legal literature and experience of various countries and its comparative legal studies revealed that the definitions of the computer data and the electronic evidence are numerous but the content is mostly common. In particular, computer data is any information entered by the user into the computer system, then automatically processed, stored, or transmitted by an electronic device. And electronic/digital evidence is – computer data available in computer systems

88 *Papiashvili L.,* Commentary on the Criminal Procedure Code of Georgia, Tbilisi, 2015, 276 (in Georgian).
89 Ibid, 275.
90 Ibid, 277.
91 *Casey E*., Foundations of Digital Forensics, Digital Evidence and Computer Crime, 3rd ed., USA, 2011, 3.

that are valuable to the investigation or to a party to the proceedings to prove important circumstances in court.

Herewith, analyzing the characteristics of computer data allowed us to perceive the distinction between material and electronic evidence, which in turn showed us the need for additional procedural tools, like Expedited Preservation of Stored Computer Data to respond the dynamic and changeable content of computer data.

The importance of the characteristics of computer data increases when examining the authenticity of it, but also crucial is the form of data creation. Particularly, whether the evidence is generated by a computer system or if it is produced by the user. The authenticity of Printout is a challenging, too. We face difficulties when examining the authenticity of unofficial documents because unlike official documents it does not have any requisites. With the help of these requisites determining the authenticity of the document requires less effort, but the printout that does not have the hallmarks and the party submits it to the court an expert evaluation will be essential to supply the court with the information on the source of evidence, the proper functioning of the device and its compliance with the original document.

Despite the complexity of the issue, a study of different legislation and case law assured us that the use of rules developed concerning the authentication of written documents are fully justified with electronic evidence.

Bibliography:

1. Criminal Procedure Code of Georgia, LHG, 03/11/2009.
2. Federal Rules of Evidence (USA), 01/12/2019.
3. Acts Interpretation Act 1901, 14/01/2019.
4. Evidence Code of California, 18/05/1965.
5. Convention on Cybercrime, 23/11/2001.
6. Data Protection Act, 16/07/1998.
7. Evidence Act, 1995.
8. Canada Evidence Act, 1985.
9. Federal Rules of Civil Procedure, 20/12/1937.
10. Federal Rules of Criminal Procedure, 26/12/44.
11. Back-Up Data, Nonprofit Technology Collaboration, <https://www.baylor.edu/content/services/document.php/192120.pdf> [23.02.2021].
12. *Brenner W. S., Frederiksen A. B.,* Computer Searches and Seizures: Some Unresolved Issues, Michigan Telecommunications and Technology Law Review, Vol. 8, Issue 1, 2002, 60-63, 80-82.
13. *Capra D.,* Authenticating Digital Evidence, Baylor Law Review, №1, 2017, 3.
14. *Casey E.,* Digital Evidence and Computer Crime, 3rd ed., USA, 2011, 3, 7, 26.
15. *Clancy K. T.,* The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and A Primer, Mississippi Law Journal, Vol. 75, 2005, 193.
16. Council of Europe, Cybercrime Training for Judges, 2010, 35, <https://rm.coe.int/16802fa028> [23.02.2021] (in Georgian).

17. *Diana J. A., Esteban A. A., Guglielmo P. J., Hiser S. T., Kuckelman D., Mandel P. E., Opstnick M. T., Ragan R. C., Sharp C. D., Tully T. M.,* The Sedona Principles, Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 3rd ed., The Sedona Conference Journal, Vol. 19, №1, 2018, 207-209, 211, 213.
18. *Gonzales R. A., Schofield B. R., Hagy W. D.,* Digital Evidence in the Courtroom – A Guide for Law Enforcement and Prosecutors, NIJ, USA, 2007, 2, 28, 44.
19. *Gonzales R. A., Schofield B. R., Hagy W. D*., Investigations Involving the Internet and Computer Networks, National Institute of Justice, USA, 2007, 2.
20. *Goodison E. S., Davis C. R., Jackson A. B.,* Digital Evidence and U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence, NIJ, USA, 2015, 3.
21. *Gregory D. J.,* Authentication Rules and Electronic Evidence, The Canadian Bar Review, Vol. 81, № 3, 2001, 531.
22. *Johnson A. M.,* Computer Printouts as Evidence: Stricter Foundation or Presumption of Reliability, Marquette Law Review, Vol. 75, Issue 2, 1992, 445.
23. *Kerr S. O.,* Searches and Seizures in a Digital World, Harvard Law Review, Vol. 119, 2006, 1.
24. *Mason S., Weir R. S. G.,* The Sources of Electronic Evidence, 4th ed., Institute of Advanced Legal Studies, *Mason S., Seng D. (eds.),* London, 2017, 1, 4.
25. *Mason S., Stanfield A.,* Authenticating Electronic Evidence, Electronic Evidence, 4th ed., Institute of Advanced Legal Studies, *Mason S., Seng D. (eds.),* London, 2017, 193.
26. *Meurmishvili B*., Georgian Criminal Procedure Law, Special part, Tbilisi, 2017, 534 (in Georgian)
27. *Mukasey B. M., Sedgwick L. J., Hagy W. D*., Electronic Crime Scene Investigation: A Guide for First Responders, National Institute of Justice, USA, 2008, 9.
28. *Otkhozoria V., Tsiramua Z., Svanishvili Sh*., Supporter Specialist of Information Technology, Tbilisi 2015, 8 (in Georgian).
29. *Otkhozoria V., Tsiramua Z.,* Information Technology, Tbilisi, 2015, 226 (in Georgian).
30. *Outerbridge D., Siller E.,* The Admissibility of Electronic Evidence, 2015, 11, <https://www.lawinsider.com/documents/1tYTXnzcs2u> [23.02.2021].
31. *Papiashvili L.,* Commentary on the Criminal Procedure Code of Georgia, *Giorgadze G. (eds.),* Tbilisi, 2015, 288 (in Georgian).
32. *Riley J.*, Understanding Metadata, National Information Standards Organization, Baltimore, MD, 2017, 1.
33. *Schafer B., Mason S.,* The Characteristics of Electronic Evidence, Electronic Evidence, 4th ed., Institute of Advanced Legal Studies, *Mason S., Seng D. (eds.),* London, 2017, 18, 20-21, 26-28.
34. Scientific Working Group on Digital Evidence (SWDGE), SWGDE Digital and Multimedia Evidence Glossary, 2016, 7, < https://www.swgde.org/documents/published> [20.02.2021].
35. *Stanfield R. A.,* The Authentication of Electronic Evidence, Queensland University of Technology, Australia, 2016, 61, 64-65.
36. *Tumanishvili G.,* Criminal Process – Overview of the general part, Tbilisi, 2014, 225-226 (in Georgian).
37. The Explanatory Report to the Convention on Cybercrime, European Treaty Series – № 185, Budapest, 23.11.2001, 5.

38. Decision of July 31, 2015, № 2/2/579, Constitutional Court of Georgia on the case: "Citizen of Georgia Maia Robakidze against the Parliament of Georgia", 12.
39. *AMP v. Persons Unknown,* [2011] EWHC 3454 (TCC).
40. *R. v. Nichols,* (2004), CarswellOnt 8225, (Ont. C.J.).
41. *R. v. Morgan,* (2002), N.J., №15, (NLPC).