Pak. j. life soc. Sci. (2024), 22(2): 21018-21030 E-ISSN: 2221-7630;P-ISSN: 1727-4915

Pakistan Journal of Life and Social Sciences
www.pjlss.edu.pk

https://doi.org/10.57239/PJLSS-2024-22.2.000198

RESEARCH ARTICLE

The Status of Electronic Evidence and Its Role in Proving Criminal Cases

Raddam Azawi Dawas[1], Siamak Jafarzadeh[2*], Reza Nikkhah Saranghi[3]

[1,2,3] Faculty of Literature and Humanities, Urmia University, Urmia

ARTICLE INFO

Received: Oct 27, 2024

Accepted: Dec 22, 2024

Keywords

Electronic Evidence

Proof of Criminal Cases

Law

***Corresponding Author:**

s.jafarzadeh@urmia.ac.ir

ABSTRACT

The objective of this study is to examine the status of electronic evidence and its role in proving criminal cases. The research methodology is descriptive and library-based. The acceptance of electronic documentation or data messages as evidence depends on meeting the legal conditions of such evidence in an electronic environment, particularly when the confrontation with the judge or the objective supervision of a third party is a formal requirement for the evidence. In such cases, the electronic environment cannot fulfill these conditions. However, when evidence is stipulated to be written and signed, a data message, provided it is technically reliable, is considered equivalent to written and manually signed documents. By recognizing and accepting electronic documentation as evidence, such documents gain probative value.

Electronic evidence comprises valuable data and information stored or transmitted via electronic devices. Such evidence becomes admissible only when sufficient assurance exists regarding the technical conditions necessary to ensure their authenticity for various authorities. In other words, for criminal courts, the identity of the creator of the electronic evidence must first be established, and the evidence must possess attributes of authenticity (such as accuracy, integrity, validity, non-repudiation, etc.). Additionally, judicial officers and forensic experts must adhere to a protective chain of custody, employing standardized tools and methods at all stages of identifying, discovering, collecting, documenting, analyzing, preserving, and presenting digital evidence to ensure its acceptance by the court.

INTRODUCTION

Long before the enactment of the Electronic Commerce Act, electronic evidence—such as audio recordings, videos, photographs, and data messages generated by water and electricity meters—was admissible in courts. However, the absence of a coherent legal framework in this area led to inconsistent judicial rulings and subjective approaches by judges in recognizing the validity of such evidence. The Electronic Commerce Act, enacted in 2003 (1382 AH), formally acknowledged electronic evidence as a new category of proof and even granted it the highest probative value when deemed reliable, considering it indisputable and irrefutable.

Despite the passage of several years since the enactment of the Electronic Commerce Act, this type of evidence is still overlooked in certain contexts, such as the course on evidence law taught to law students. Furthermore, the law itself remains unfamiliar to many judges, lawyers, and legal scholars.

This lack of awareness among the legal community extends to the technical infrastructure of electronic evidence, including secure information systems and digital signatures. The prevailing assumption is that electronic evidence is easily falsifiable or modifiable, that information systems are not sufficiently reliable, and that data derived from such systems are prone to errors. Consequently, lawyers are often hesitant to rely on electronic evidence to prove their claims, and judges occasionally refrain from accepting it.

Moreover, assessing the credibility of such evidence in court requires experts proficient in both the technical underpinnings and legal principles of electronic evidence. These experts play a critical role in retrieving, safeguarding, and verifying the reliability of electronic evidence, thereby aiding the judicial process.

Before the advent of information and communication technologies, evidence was predominantly presented in its traditional forms, such as confessions, written documents, testimony, presumptions, and oaths, with paper being the primary medium for conveying information. However, the past century has witnessed remarkable advancements in information and communication technologies. Innovations such as the telegraph, telephone, fax machine, microfilm, computer, and internet introduced new methods of communication, significantly enhancing efficiency and accessibility. These tools rapidly gained popularity for both commercial and everyday purposes, ultimately giving rise to electronic commerce—a new mode of conducting business that facilitates the exchange of commercial information without reliance on paper.

In addition, computer-based tools have become so precise and intelligent that, beyond their role as instruments for storing and transmitting information, they can autonomously generate and process data without direct human intervention.

Problem Statement

Proof-of-Stake (PoS) cryptocurrencies represent an innovative approach within the cryptocurrency ecosystem, enhancing both security and efficiency. Unlike Proof-of-Work (PoW) systems, PoS cryptocurrencies contribute to transaction validation by holding stakes in the network. This mechanism not only reduces energy consumption but also opens new opportunities for investors. Consequently, PoS cryptocurrencies play a crucial role in advancing the sustainability and security of the crypto ecosystem. The Proof-of-Stake algorithm, widely known as PoS, is recognized as a prominent consensus mechanism in the blockchain domain. It is the second most commonly used method after the Proof-of-Work algorithm (Mousavi, 2022).

A digital currency is a form of payment that exists solely in electronic form, intangible and lacking any physical presence. Digital currencies can be transferred between individuals using technologies such as computers, smartphones, and the internet. While sharing several similarities with physical currency, digital money facilitates fee-free and rapid transfers for users. Digital currencies can be used for purchasing goods and services. Currently, hundreds of digital currencies exist worldwide, offering advantages such as:

- Reduced risk of fraud
- Fast transactions
- Lower transaction costs
- Decentralization

Among these, certain cryptocurrencies, such as Bitcoin, Ethereum, Ripple, and Litecoin, are particularly popular with users (Siah Beidi, 2018). For this study, Bitcoin has been selected as the basis for comparisons due to its focus by domestic and international policymakers, central banks, and currency exchanges.

Money laundering, although seemingly distinct, is closely tied to the issues discussed above. It is a process by which criminals or organized groups disguise the origins and nature of illicitly obtained wealth, integrating it into the formal economy. Money laundering serves as a bridge connecting the criminal underworld with broader society. Recent definitions highlight its role as the connecting link between the formal, legal economy and the informal, illegal economy. In essence, money laundering is a method of introducing the proceeds of drug trafficking, gambling, prostitution, and other illicit activities into the economic cycle through multiple layers of concealment (Fallahi, 2018).

In the evolution of monetary systems, digital currencies have emerged, revolutionizing financial and currency exchanges. Like any human advancement, this nascent phenomenon comes with its strengths and weaknesses, attracting the attention of opportunists and disruptors of the economic system. This necessitates a thorough examination of digital currencies from their inception to their issuance and exchange, ensuring they are utilized responsibly and not exploited, as has been the case with traditional currencies.

Notably, digital currencies like Bitcoin transfer computational and operational responsibilities from humans to machines, where the impartiality and calculative precision of computers over humans can be considered a basic advantage. However, this is not the sole benefit of digital currencies. Among the numerous advantages, the following points stand out:

- Peer-to-peer transactions
- No need for intermediaries
- Decentralization
- Independence from banks

Despite these advantages, digital currencies pose challenges to society. These challenges have not yet been adequately addressed by domestic legislators or international authorities, and, at best, the existing laws on the matter are incomplete or ineffective. For instance, blockchain technology, which underpins many digital currencies, enables the distribution of data across multiple systems. This distributed ledger ensures that all users have access to a copy of the data. However, a critical issue arises: users are often unaware of the origins and purposes of the transactions and data being recorded and transferred.

A significant concern is the entry, circulation, and exit of illicit money through these systems. While the entry and exit of such funds may involve physical processes, their circulation is entirely digital. This means that money derived from illicit activities, such as money laundering, must be integrated into and removed from the network, a process requiring meticulous examination. A crucial, yet ambiguous, aspect involves tracking and identifying the flow of these currencies within networks.

Money laundering allows economic disruptors to evade taxes and enables criminals involved in other illegal activities—such as human trafficking, arms dealing, and drug trafficking—to exploit this emerging financial phenomenon for their transactions. Such individuals take advantage of legal loopholes to facilitate their operations effectively (Pouladvand, 2015).

This might raise the question of whether digital currencies have facilitated opportunities for profiteers or increased challenges for them. To date, no comprehensive research has been conducted on this issue, and references are often limited to a few short articles. Consequently, this study seeks to examine money laundering, which is more prominently manifested in digital currencies compared to other forms of cybercrime (Abhari, 2017, p. 34). Initially, we will discuss the legal approach in Iran, followed by a focus on preventive measures.

Public interest in cryptocurrencies has surged recently, and the global cryptocurrency market continues to flourish. Cryptocurrencies are often portrayed as significant competitors to the current financial system, promising enhanced security, speed, transparency, increased financial transactions,

the creation of a more equitable economy, privacy protection, and the elimination of bureaucratic processes.

Even if we accept all these claims, the world of cryptocurrency is not without its downsides. Governments, regulatory organizations, central banks, and other financial institutions are working hard to address the decentralized nature of cryptocurrencies, especially concerning the legal, economic, and technical challenges they present. Despite these efforts, significant challenges persist, including:

- The difficulty of determining the competent court and applicable law
- Violations of mandatory regulations
- Tax evasion
- The commission of crimes
- Disruptions to economic order

These issues demand serious consideration. Based on the above, the aim of this study is to investigate digital currencies and their role in proving criminal cases.

RESEARCH BACKGROUND

Matsura (2018):

Matsura examined digital currency systems, which utilize secure distributed computing networks encrypted to exchange economic value and support a wide range of applications. The nature of these computing platforms and their application domains raises critical issues regarding legal compliance. Many jurisdictions worldwide are evaluating how existing laws and regulations apply to digital currency systems and to what extent these laws need modification or new regulations to address the growth of digital currencies. Presently, it is evident that a diverse range of laws and regulations are applicable to digital currencies and their applications in various jurisdictions. In this complex legal landscape, developers, distributors, and users of digital currencies and their associated systems face significant compliance challenges. Understanding existing and potential legal requirements is essential for the successful use of digital currency platforms and applications.

Jalali Farahani (2007):

In a study titled "The Admissibility of Electronic Evidence in Criminal Cases," Jalali Farahani stated:"In the new millennium, almost nothing remains unaffected directly or indirectly by technological advancements. This emerging condition has influenced various fields of modern information and communication technologies, including the legal system. Among these, perhaps no branch has been impacted as significantly as the system of evidence in legal proceedings, as digital data fundamentally differs from physical-world documents and information. This concern is even more pressing in the realm of criminal evidence. The standardization of law enforcement practices when dealing with cybercrime cases or those linked to cyberspace is imperative. Without such measures, not only would justice fail to be served, but human rights principles would also be violated."

Matsura(2019):

National currency regulators have generally not had direct jurisdiction over virtual currencies because they are not national fiat currencies. However, regulators influence the development of digital currencies through several indirect methods. By exercising their authority to protect the value and integrity of national fiat currencies, they implement measures that affect digital currencies, claiming these actions are necessary to safeguard their national currency. Additionally, regulators often control the activities of banks and other key financial institutions, limiting their ability to use or accept virtual currencies. Regulators also typically have authority over foreign exchange

transactions and frequently use this role to restrict the ability to convert digital currencies into traditional fiat currencies. Furthermore, national currency regulators have issued significant consumer warnings about the risks of using digital currencies. They also regulate capital transfers and money transfers, often applying these controls to virtual currency transactions. Some governments are currently exploring state control over digital currencies and the possibility of participating in blockchain platforms for existing virtual currencies.

Baghani (2020):

With technological advancements, financial and banking services, like other industries, are undergoing changes. The impact of modern technologies has increased the profitability of banks and financial institutions, accelerated service delivery, and enhanced customer satisfaction. Although the banking industry in the country has made some progress, there have not been significant changes in business platforms. Hence, regulators and senior banking system managers must adopt a different perspective toward modern financial technologies, viewing them as drivers of transformation for new banking business platforms. Technologies such as financial technology (FinTech) and digital currencies can serve as the beginning of a new era in technology-based financial services. This article provides a general framework for these technologies, examines common regulatory methods in other countries, and offers recommendations for overseeing FinTech and digital currencies. With the support of domestic banks, the establishment of regulations and frameworks by the Central Bank, and a conducive environment, FinTech and digital currencies have the potential to transform the banking ecosystem to benefit customers.

METHODOLOGY

To collect the data and information required for this research, in addition to library studies and using articles and journals for the purpose of obtaining prior research, internet websites will also be used to find research conducted both inside and outside the country. The researcher will also use available theses from universities in the country that are related to the research topic, and additionally, reputable legal websites such as Magiran, Noormags, IranDoc, and the Comprehensive Portal of Humanities will be utilized.

Definition of Electronic Evidence

Electronic evidence is evidence that has the characteristic of being "electronic," meaning that "electronic evidence" is a more specific concept of evidence. However, this does not mean that this type of evidence possesses all the features of traditional evidence; rather, its electronic nature leads to effects that distinguish it from traditional evidence. For instance, electronic evidence cannot be categorized into the eight traditional forms. Some have considered it as a ninth category of evidence, suggesting that a new title, such as "electronic evidence" or a broader term, should be added to the section on fundamental principles of evidence in the Civil Code or under the topic of documents, as advancements in information technology may introduce other intermediaries with similar effects (Abdollahi, 2012, p. 22).

The concept of "electronic evidence" includes not only the evidence generated by electronic tools but also all types of evidence created by other modern technologies, including digital, magnetic, optical, and electromagnetic tools, as well as evidence produced by other tools that may be invented in the future. However, the common feature is that electronic evidence is in the form of "data messages."

Although the legislator has not provided a definition of electronic evidence, based on the aforementioned aspects, it can be defined as: "Electronic evidence is a data message to which the parties refer in order to prove or defend their case."

According to the definition of a data message in section (a) of Article 2 of the Electronic Commerce Law, "electronic evidence" is any information, concept, or symbol of an event that is produced, sent,

received, stored, or processed through electronic, optical, or modern information technologies, and to which the parties refer in order to prove or defend their case (Abdollahi, 2012, p. 23).

Features of Electronic Evidence

By examining the nature of electronic evidence, certain features can be identified that distinguish it from other types of evidence, leading to various effects. These features include:

1. The most important feature of an electronic version is that it may not be identical to its printed copy. This means that only by examining the electronic version can important hidden information become visible. Therefore, having an electronic version of a document or record may provide more information compared to its printed copy (Soltani, 2005).
2. Computers typically store information in locations such as log files or document headers, which are generally not accessible to users. Many people are unaware of the types of information that are tracked and stored by computer systems (Soltani, 2005).
3. Electronic data can be stored in highly compressed formats, which makes transferring and deleting electronic data easier compared to paper-based records.
4. Electronic data is more vulnerable than paper documents, and it is easier to forge and manipulate this data (Soltani, 2005).
5. An electronic document can be stored in various forms. These documents are readable only through the software that created them. Even in this case, some useful information may remain in the documents and may not be easily accessible (Soltani, 2005).
6. Electronic documents have a faster replication ability compared to regular documents (Soltani, 2005).
7. Electronic evidence may exist in forms of which the user may be unaware, as it can be stored by a computer without the user's knowledge (Soltani, 2005).

The Importance of Electronic Evidence

With the widespread adoption of computer technology in information management and the increasing reliance on computerized systems in place of traditional paper-based records, substantial repositories of valuable information are being created in the virtual domain. The discovery and utilization of this information, often referred to as the discovery of electronic media, hold critical importance.

Many software applications generate files known as log files, which record various types of information without the user's explicit knowledge. Furthermore, within virtual networks, even when data is deleted, it does not vanish entirely, as copies often remain stored in other network nodes.

Electronic evidence extends beyond computers and encompasses all retrievable data from electronic devices such as mobile phones, fax machines, and pagers. It is essential to note that the substantiation of claims in judicial proceedings requires the presentation of evidence to the court. Unlike conventional evidence, electronic evidence is more susceptible to destruction. For legal practitioners involved in advanced litigation, disregarding electronic data is tantamount to compromising the outcome of the case (Soltani, 2005).

Requests for the discovery of electronic evidence can also serve as a strategic tool in legal negotiations. The advent of information technology has facilitated the generation and storage of vast amounts of data. Moreover, electronic evidence provides access to informal records, which often possess greater persuasive value compared to conventional forms of evidence. For instance, an audio or multimedia message retrieved from an electronic messaging system may encompass both visual and auditory elements, features absent in traditional evidence (Soltani, 2005).

Conditions for the Validity of Electronic Evidence (Documents)

Can all electronic documents and records be presented as evidence in court? Generally, the admissibility of such evidence is contingent on convincing the judge presiding over the case. Given the characteristics of the digital environment—such as the ease of manipulation, alteration, duplication, and deletion of electronic data—it is natural for courts to approach the validity of electronic evidence with great caution. Ordinarily, such evidence may be considered only as supporting evidence rather than definitive proof.

Under Iran's Commercial Code, the admissibility and evidentiary value of electronic data messages are specified in Articles 52 to 54 as follows (Soltani, 2005):

Article 52: Electronic data messages may be presented as evidence in claims or defenses. No court or government authority may deny the evidentiary value of such data messages merely because of their form or format.

Article 53: Electronic data messages may be presented as evidence in claims or defenses. Their evidentiary value is equivalent to that of documents addressed in Book Two of the Civil Code's Volume Three on Evidence of Claims, enacted on October 13 and November 18, 1935.

Article 54: The evidentiary value of electronic data messages is determined based on the security measures used for their creation, storage, and transmission, as well as measures ensuring the integrity of the data message and other relevant factors.

The Electronic Commerce Law specifies the evidentiary value of data messages and outlines two possible scenarios:

Data Messages with Evidentiary Value:

If the data message meets security requirements, as indicated in the relevant provision, its evidentiary value is determined based on factors such as the adequacy of security methods used in the exchange process. The law also provides a definition for "secure methods."

Data Messages Lacking Security Conditions:

If a data message does not meet the required security standards or reliable factors, it will not possess evidentiary value. This interpretation is derived from the contrary implication of Article 54.

It is evident that under the aforementioned regulations, there may be instances where a data message has no evidentiary value and, therefore, cannot be considered valid evidence (Soltani, 2005).

Furthermore, some may object to recognizing electronic messages as documents based on Article 1284 of the Civil Code, which defines a document as "any writing that can be cited as evidence in claims or defenses." Since written form is a principal condition for a document under this article, and electronic messages are not traditionally written, their acceptance as documents might be disputed (Soltani, 2005).

Types of Electronic Evidence

The differences between electronic evidence and traditional evidence often lead to uncertainty about the reliability of the former. In traditional evidence systems, paper is typically used as a durable medium for recording information, and the handwriting and signature of the issuer ensure the attribution of the document to them. Moreover, due to the physical nature of traditional documents, forgery or alteration can be more easily detected. These characteristics provide confidence in the validity of paper documents, which are commonly used in commercial transactions. However, electronic documents differ significantly. These documents exist as data messages and lack a tangible, physical basis, making them less stable and susceptible to modification without leaving a physical trace (Abdollahi, 2012, p. 51).

Electronic evidence is often created in the online environment and is used to substantiate electronic contracts. In this setting, the parties are typically unaware of each other's real identities due to the absence of physical presence. Additionally, as information is exchanged over the internet, it lacks sufficient security. For instance, a hacker could infiltrate the network, access the document, alter it, or impersonate others to send documents. Consequently, a document created simply, without advanced technologies, and in an insecure environment is prone to denial, doubt, and forgery. There is no certainty regarding the attribution of the document to its issuer, the identity of the issuer, or the integrity of the document.

However, not all electronic evidence suffers from these vulnerabilities. Modern technologies have been developed to ensure the reliability of such evidence. These technologies primarily manifest in two forms: **electronic signatures** and **information systems** (Abdollahi, 2012, p. 52).

Challenges in Accepting and Admissibility of Electronic Evidence

The collection of electronic evidence in cybercrime investigations and trials is of significant importance. If such evidence is properly collected, preserved, and presented, it can facilitate the administration of justice. Conversely, if it is not gathered, stored, or presented in accordance with accepted technical and legal principles, it can disrupt judicial proceedings and prevent the realization of individual and societal rights. Consequently, challenges in accepting electronic evidence can hinder its admissibility in legal contexts.

CONCLUSION

The admissibility of electronic documentation or data messages as evidence depends on fulfilling the legal conditions required for such evidence in the electronic environment. When direct interaction with the judge or third-party supervision is a formal requirement for evidence, the electronic environment cannot satisfy those conditions. However, if the requirement pertains to the equivalence of writing and signature, data messages that meet technical reliability standards are considered equal to handwritten documents and signatures. By accepting and recognizing electronic documentation as valid evidence, such documentation gains evidentiary value.

In general, when dealing with the emerging phenomenon of electronic evidence, lawmakers must adopt four fundamental principles:

Admissibility of Electronic Evidence: The mere electronic nature of evidence should not prevent its acceptance.

Equivalence to Handwritten Documents: The equivalence of data messages to handwritten documents should be conditional upon the reliability of the data.

Presumption of Reliability: Data encrypted with codes issued by competent authorities should be presumed reliable.

Equal Evidentiary Value: The evidentiary value of electronic evidence should be treated as equivalent to that of other forms of evidence.

The acceptance of electronic documents or data messages as evidence depends on meeting the legal requirements for such evidence in the electronic environment. When confrontation with the judge or third-party oversight is a formal condition for evidence, the electronic environment cannot fulfill such conditions. However, when writing and signing are stipulated as conditions for evidence, data messages, provided they are technically reliable, will be equivalent to handwritten documents and signatures. By recognizing and accepting electronic documents as evidence, these documents gain evidentiary value.

Electronic evidence comprises valuable research data and information stored on or transmitted through electronic devices. Such evidence is admissible when there is sufficient confidence in the presence of necessary technical conditions to ensure the validity of these documents for various authorities. In other words, for criminal courts, the identity of the creator of the electronic evidence must be established, and the evidence must possess characteristics of authenticity (accuracy, integrity, credibility, non-repudiation, etc.).

Furthermore, judicial officers and court experts must observe a chain of custody by employing standard tools and methods during the stages of identification, discovery, collection, documentation, analysis, preservation, and presentation of digital evidence, ensuring compliance with these standards in practice.

In addition, Iran's judicial system and criminal procedure follow the open evidence system. In judicial proceedings, the court's confidence in the validity and authenticity of evidence is largely based on reports from judicial officers and opinions from official judiciary experts. Certain provisions from the Electronic Commerce Act and the Computer Crimes Act (or provisions of the Islamic Penal Code) are referenced, and topics such as confessions, documents, judicial presumptions, and the judge's knowledge also play significant roles.

Ultimately, after understanding electronic evidence and its admissibility, it must be emphasized that the existing laws, in some cases, have shortcomings and deficiencies. In certain areas, there is a need to draft new laws and complementary regulations, and in some cases, existing rules require amendment. It is incumbent upon lawmakers to take action in this regard. The proposed solutions, based on theoretical and field research, are as follows:

1. When discussing electronic litigation in Articles 49, Clause 2 of Article 204, Item "ch" of Article 217, and Article 448 of the Criminal Procedure Code of 1392, one of the topics to be addressed is electronic evidence. The question raised in this regard is whether the necessary prerequisites for its implementation have been established. Is the mere existence of certain judicial bodies or portals, such as the well-known electronic judicial complex, sufficient? Does simply scanning petitions and the parties' pleadings or sending SMS notifications for trial dates imply electronic litigation? To answer these questions, we are waiting for the courts or lawmakers to have enough time to familiarize themselves with technologies and new professional activities. In other words, the challenge of balancing the need for the claimant to access relevant information to prove the claim with the responsibilities imposed on the provider creates a fair equilibrium.

2. The necessity of drafting and formulating general procedural laws for cyber and specific environments means that, with regard to the procedural aspects of cybercrimes, it is surprising that the legislator has included procedural issues related to evidence in the substantive law, known as the Islamic Penal Code. While procedural and substantive laws each have their own specific legal consequences, the need to review traditional laws and draft new ones is essential and necessary.

3. In the research conducted, the draft regulation of Article 54 of the Computer Crimes Act (Article 782 of the Islamic Penal Code) concerning the collection and admissibility of electronic evidence was mentioned. However, this regulation, which was passed by the judiciary after approximately five years from the approval of the law in 1388, still lacks a clear definition of concepts such as traffic data, content data, and some technical terms. Additionally, it refers the implementation of certain articles to other instructions and regulations, and it would have been more appropriate to issue a complete and comprehensive regulation after this period. What is more noticeable in the regulation is the reference to the Computer Crimes Act, which has now been integrated into the Islamic Penal Code, and it appears that insufficient attention has been given to this matter.

4. The necessity for greater familiarity and expertise of judicial officers and judges with technical and electronic issues, although currently, the Cyber Police (FATA) plays a major role in the collection and

documentation of evidence, it is important to note that the experts in this center were initially selected from ordinary police officers who lacked the necessary technical knowledge. To address this shortcoming, experts and employees familiar with computers were brought in to solve the issue. However, this method faced a serious flaw in that these employees were not police officers and lacked expertise in police matters. It seems that, in the future, necessary measures must be taken to coordinate both specializations.
Another issue concerns the shortage of specialized judges. The judges currently handling these cases are law graduates who are not familiar with computer science, and simply having an ICDL certificate is insufficient. It is essential to organize specialized training sessions and further education. It should be noted that, at present, the Cyber Crimes Prosecution Office in a large city like Tehran has two investigative branches and two prosecution branches, and the orders issued by the prosecution regarding conviction and indictment are processed and issued at the Government Employees Judicial Complex. Certainly, the current situation is not suitable, and the mere allowance by the 1392 Criminal Procedure Code to establish specialized prosecution offices, including for cybercrimes, is not sufficient. Therefore, these judges are forced to accept the documents and evidence presented by judicial officers and forensic experts, which contradicts the research argument that judges must ensure the authenticity and validity of the evidence.

5. Since some cybercrimes are committed on social networks like Facebook, whose central servers are located abroad, collecting evidence is difficult due to the lack of access to the central website. Therefore, court-appointed experts resort to alternative methods, such as examining the records stored by computer service providers, to provide their opinion to the court. In this regard, international cooperation and mutual legal assistance in discovering electronic evidence and establishing a rapid response group for cybercrimes to combat, detect, and track cybercrimes are among the most crucial steps. This group must be equipped with the latest software and hardware for discovering and tracking cybercrimes and collecting electronic evidence.

REFERENCES:

Al-Bouali, Amir. Jurisdiction of Courts in Cyber Crimes. Jangal Publications, First Edition, 2013.

Al-San, Mustafa. Internet Banking Law. Monetary and Banking Research Institute, Second Edition, 2013.

Emami, H. (2006). Civil Law, Vol. 6. Tehran: Eslamiyeh Publications, 540 pages.

Ulrich Sieber. Computer Crimes. Translated by Nakhjavani, Noori, Bakhtiarvand, Rahimi Moghaddam. Ganj Danesh Publications, Second Edition, 2011.

Ashouri, M. (2001). Criminal Procedure, Vol. 2. Tehran: SAMT Publications, 600 pages.

Ashouri, Mohammad. Criminal Procedure, Vol. 2. SAMT Publications, Fourth Edition.

Allen Gatton. (2004). Discovery of Electronic Evidence. Translated by M. Ramazani. Secretariat of the Supreme Council of Information, Tehran: Tous Publications, 240 pages.

Babakhani, R. (2012). "A Study on the Evidentiary Value of Electronic Documents in Iranian Law." Islamic Law Research Journal, 1(35), 157–188.

Baghani, Elaheh. (2020). "Examining the Oversight Mechanisms for New Financial Technologies: FinTech and Cryptocurrency." Investment Knowledge Journal, 9(35), 153–168.

Bakhtiarvand, M. (2004). "Electronic Signature and the Revolution of Rules on Evidence." Informatics Newsletter, No. 91.

Pour Ahmadi, Mahsa. Master's Thesis, Islamic Azad University, Mashhad Branch, "The Role of Electronic Evidence in Legal Proceedings."

Pouladvand, Nastaran. (2015). "Criminalization in the Light of Societal Values." First National Conference on New Research in Law and Social Sciences.

Tadian, Abbas. Evidence Collection in Criminal Procedure. Mizan Publications, Second Edition.

Sarvati Bi-Niaz, Morteza, & Jafari, Fereydoun. (2020). "Jurisdiction over Currency Smuggling Crimes in Iranian Law." Legal Research Journal, 19(43), 29–43.

Javidnia, Javad. Further Studies in E-Commerce Crimes. First Edition, Khorsandi Publications, 2011.

Electronic Evidence Training Manual. Committee on Combating Cyber Crimes, Judiciary of Iran, Translated by Mosaib Ramazani.

Jalali Farahani, Amir Hossein. "Admissibility of Electronic Evidence," Jurisprudence and Legal Journal, Winter 2007, No. 15.

Jalali Farahani, Amir Hossein. Search and Seizure of Computers and Collection of Electronic Evidence in Criminal Investigations. Judiciary Legal and Development Deputy, Second Edition, 2011.

Jalali Farahani, Amir Hossein. Introduction to Criminal Procedure for Cyber Crimes. Judiciary Legal and Development Deputy, Khorsandi Publications, Second Edition, 2011.

Khordmand, Mohsen. (2019). "A Jurisprudential Study of Cryptocurrency Mining and Exchange with a Focus on the 'Bitcoin' Network." Islamic Economics Knowledge Journal, 2(20), 109–124.

Secretariat of the Supreme Council of Informatics. (1997). Computer Crimes. Tehran: Agah Publications, 340 pages.

Dr. Khazani. Criminal Procedure Course Notes, Academic Year 1994–1995.

Zwina Linen Doubelphon. E-Commerce Law. Translated by Dr. Sattar Zarkalam, Shahr Danesh Publications, Second Edition, 2011.

Rahimi, Ali, & Amini Nia, Atefeh. (2021). "Cryptocurrencies: Challenges and Crimes Surrounding Them." Qanoon Yar Journal, 5(18), 78–98.

Zarkalam, Sattar. (2003). "Electronic Signature and Its Role in Evidence Law." Modares Journal of Humanities, 7(28), 56–87.

Zarkalam, Sattar. Electronic Commerce Law. Shahr Danesh Publications, Second Edition, 2011.

Zarrin Kalki, B. (2008). "Electronic Documents and Their Management." Archive Quarterly, Issue 70.

Zandi, Mohammad Reza. Preliminary Investigations in Cyber Crimes. Jangal Publications, First Edition, 2010.

Souri, Parviz. (2022). "Cryptocurrency and Challenges Facing Legal Systems." Legal Research Journal, 2(25), 113–142.

Siyah Bidi Kermanshahi, Saeed. (2018). "Overview of Cryptocurrency Regulations and Their Legal Implications." Fars Law Research Journal, Year 1, Issue 1.

Shams, Abdullah. Evidence Law (Substantive and Procedural). Drak Publications, Sixteenth Edition, 2013.

Shams, A. (2006). Evidence Law, Third Edition. Tehran: Drak Publications, 456 pages.

Shams, A. (2007). Civil Procedure, Fourth Edition, Tehran: Drak Publications, 543 pages.

Shirzad, Kamran. Computer Crimes in Iranian and International Criminal Law. Behineh Faragir Publications, First Edition, 2009.

Sadeghian, Nadi Ali. "Electronic Documents: The Most Astonishing Communication Media." Hoghoughdan Website.

Abdollahi, M. (2012). Electronic Evidence in the Evidence System. First Edition, Tehran: Khorsandi Publications, 379 pages.

Askarzadeh, Gholamreza, & Rouhi, Amin. (2022). "Herding Behavior in the Cryptocurrency Market." Journal of Financial and Behavioral Research in Accounting, 4(7), 123–135.

Fallahi, Mohammad, & Momeni, Alireza. (2018). "Financial and Tax Laws in Anti-Money Laundering Relating to Virtual Currencies." National Conference on Modern Approaches in Management, Economics, and Accounting, Tehran.

Fazeli, Mehdi. Criminal Responsibility in Cyberspace. Judiciary Legal and Development Deputy, Khorsandi Publications, Second Edition, 2012.

Ghajar, S. (2001). "E-Commerce and Related Crimes." Collection of Articles from the First Specialized Symposium on Computer Crimes, Tehran: Police Intelligence Deputy.

Ghajar, S. (2002). "Introduction to Public Key Infrastructure." Informatics Newsletter, 85, 57–89.

Ghorbani, Farhad, & Mousavi, Zahra Sadaat. (2021). "The Impact of Cryptocurrency, Bitcoin, and Digital Currency on Financial Interactions in Modern Businesses." International Conference on Management and Humanities Research in Iran, 2(9), 210–223.

Casey Owen. Digital Evidence and Computer Crimes. Translated by Amir Hossein Jalali Farahani and Ali Shayan. Judiciary Legal and Development Deputy, Salsabil Publications, 2011.

Katouzian, N. (2001). Evidence and Proof, Vol. 1. Tehran: Mizan Publications, 356 pages.

Katouzian, Nasser. Evidence and Proof. Mizan Publications, Sixth Edition, 2011.

Casey Owen. (2007). Digital Evidence and Computer Crime (Forensic Science, Computers, and the Internet). Translated by A. Jalali Farahani and A. Shayan. Judiciary Legal and Development Deputy (Judicial Development Studies Center). Tehran: Salsabil Publications, 360 pages.

Matsura, Jeffrey H. (2019). "The Impact of Cryptocurrency on Traditional Currency Regulations." Civilization Law Journal, 1(2), 123–153.

Matsura, Jeffrey H. (2018). "Overview of Cryptocurrency Regulations and Their Legal Implications." Civilization Law Journal, 1(2), 149–167.

Madani, Seyed Jalal Al-Din. Criminal Procedure One and Two. Paydar Publications, First Edition, 2008.

Parliament Research Center. (2005). Cybercrime Convention and Its Explanatory Report. No. 7646.

Maryam Esmaeili. Compilation of Laws and Regulations on Computer Crimes. Harir Publications, 2011.

Moeini Far, Mohaddeseh. (2022). "Requirements for Recognizing and Restoring Rights in Digital Space." Public Law Knowledge Journal, 11(36), 45–68.

Nouri, B. (2011). "Ordinary and Reliable Data Messages." www.vekalatnoori.ir.

Varasi, Ghazal. (2021). "Criminal Policy and Preventive Aspects of Crimes in the Domain of Cryptocurrencies." Qanoon Yar Journal, 5(19), 117–128.

Yazdi Nejad, Amir, & Dehghan, Abdolmajid. (2021). "A Blockchain EOSIO-Based Framework for Central Bank Digital Currency (CBDC)." Journal of Financial Knowledge and Securities Analysis (Financial Studies), 14(50), 187–200.

Department of Justice of the United States. 2002. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.

Gahtan A M. 1999. Electronic Evidence. Carswell.

Hill J. 2003. "The future of Electronic Contracts in International Sales", Journal of Technology Intellectual Property.

Hofman J. 2006. Electronic Evidence In South Africa. London: Lexisnexis Butterworths.

Kairab S. 2004. A Practical Guide to Security Assessments, CRC Press Company, London.

Kent T S, Millett L I. 2003. Who Goes There? Authentication Through the Lens of Privacy. National Academy Press.

Sarukkaia S, David Z. 2003. Biometric Solutions for Authentication in an E- World. USA, pp 163.

Sgarlata C, Christine D. 1998. The Electronic Paper Trail: Evidentiary Obstacles to Discovery and Admission of Electronic Evidence. Journal of Science and Technology Law.

UNCIRAL. 2001. Model Law on Electronic Signatures with Guide to Enactment, 12: 230-240.

UNCITRAL. 1996. Model Law on Electronic Commerce with Guide to Enactment.

Volonio L. 2003. Electronic Evidence and Computer Forensice, Communications of The Association for Information Systems, 12: 278-289.

Wilding E, Computer E. 1997.A Forensic Investigations Handbook, London: Sweet & Maxwell.

Wolfe H. 2001. Forensics and the Emerging Importance Evidence Gathering, available at:http://nzcs.org.nz/Site-Default-files/4915.pdf.

Young D. 2001. Advising the Corporate Client on the Duty to Preserve Electronic Evidence. aa: www.fbm.com.