Int J Ethics Soc 2025; 7(2): 13-24

10.22034/ijethics.7.2.13

INTERNATIONAL JOURNAL OF Ethics & Society

Review Article

Ethical Dimensions of Forgery and Comparative Analysis of Computer Forgery and Traditional Forgery in Iranian and Iraqi Law

Salah Habib Yasser[1], Siamak Jafarzadeh[2*], Reza Nikkhah Saranghi[2]

1. Ph.D. Student of Criminal Law and Criminology, Department of Jurisprudence and Islamic Law, Faculty of Literature and Humanities, Urmia University, Urmia, Iran.
2. Department of Jurisprudence and Islamic Law, Faculty of Literature and Humanities, Urmia University, Urmia, Iran.

Corresponding Author: Siamak Jafarzadeh, Department of Jurisprudence and Islamic Law, Faculty of Literature and Humanities, Urmia University, Urmia, Iran. E-mail: s.jafarzadeh@urmia.ac.ir

Received 15 Mar 2025 **Accepted** 08 Apr 2025 **Online Published** 13 Aug 2025

Abstract

Introduction: Forgery is a reprehensible and immoral behavior that usually aims at financial gain, but may be done to influence the opinion of one person, deceive another, or simply to cause harm. Given the technological developments and the expansion of the use of digital tools, computer forgery has become one of the serious challenges in legal systems. Therefore, the aim of the present study is to examine the ethical dimensions of forgery and comparative analysis of computer forgery and traditional forgery in Iranian and Iraqi law.

Material and Methods: This study used reliable sources and international scientific articles in the field of ethical consideration of forgery and comparative analysis of computer forgery and traditional forgery.

Conclusion: Since the emergence of writing and the beginning of the use of writing to convey intentions and thoughts, distortion and alteration of lines and words have been recognized as immoral, undesirable and criminal acts. In Islamic law, forgery is recognized as one of the examples of Ta'zir crimes, and the Holy Quran has also considered this act immoral and reprehensible and has included it among the sins. With the comparative analysis presented regarding computer forgery and electronic documents in Iranian and Iraqi law, general and practical conclusions can be reached. This study showed that both legal systems, despite similarities in the main concepts and objectives of the laws, have different approaches in formulating and implementing regulations related to forgery and electronic documents.

Keywords: *Computer forgery, Electronic evidence, Iranian law, Iraqi law, Proof of crime, Digital evidence, Comparative analysis*

How to Cite: Yasser SH, Jafarzadeh S, Nikkhah Saranghi R. Ethical dimensions of forgery and comparative analysis of computer forgery and traditional forgery in Iranian and Iraqi law, Int J Ethics Soc. 2025;7(2): 13-24. doi: 10.22034/ijethics.7.2.13

INTRODUCTION

Forgery is when someone creates or alters a document, signature, item of value, or other type of object without permission in order to deceive others. It is an act of fraud and is considered a white-collar crime. The purpose of forgery is usually financial gain, but it may be done to influence one person's opinion, deceive another, or simply to cause harm.

Computer forgery crimes are one of the most important and challenging issues in today's digital world. Given the rapid development of information and communication technology, the form and nature of crimes, especially forgery, have undergone fundamental changes [1]. Computer forgery, as a type of forgery, refers to the creation or alteration of electronic data with the aim of deceiving others and gaining illegal

gain [2]. In the Iranian legal system, the Islamic Penal Code of 1996 and the Computer Crimes Law of 2009 specifically examine and define these crimes. Article 6 of the Computer Crimes Law clearly refers to the alteration of reliable data and interference in data processing, and specific penalties are provided for it [3].

In contrast, the Iraqi legal system also faces similar challenges in the field of computer forgery. The laws of this country have also addressed the category of forgery and crimes related to information technology and, given specific cultural and social considerations, propose different legal approaches [4]. According to Article 29 of the Iraqi Cybercrimes Law, any fraudulent act in the field of electronic information will be subject to penalties including imprisonment and fines [5]. This contrast in approaches and laws, especially in the two neighboring countries, makes the present study necessary to compare computer forgery crimes in these two legal systems.

In view of the above, the purpose of the present study is to examine the ethical dimensions of forgery and to conduct a comparative analysis of computer forgery and traditional forgery in the laws of Iran and Iraq. By comparative examination of computer counterfeiting crimes in Iran and Iraq, a better understanding of the legal structure, shortcomings, and challenges in each of these systems can be achieved.

MATERIAL AND METHODS

This is a review article that used reliable sources and international scientific articles in the field of ethical consideration of forgery and comparative analysis of computer forgery and traditional forgery.

DISCUSSION

Historical Course and Ethical and Islamic Aspects of the Crime of Forgery

Since the advent of writing and the beginning of the use of writing to convey intentions and thoughts, distortion and change in lines and words have been recognized as an immoral, undesirable and criminal act. In a way, this issue has been mentioned in the Code of Hammurabi, which is the oldest code of human law. Also, in Roman law, the term "falsum" was used to refer to forgery. In the old French legal system, forgery was also used in a broader sense and referred to any type of fraudulent act whose purpose was to hide the truth and deceive others [6].

In Islamic law, forgery is recognized as one of the examples of penal crimes, and the Holy Quran has also condemned this act and included it among the sins. For example, in Surah Al-Baqarah it is stated: "So whoever substitutes what is not heard, his sin is upon those whom he substitutes. Indeed, Allah is Hearing, Knowing."

Forgery and forgery have been discussed in jurisprudential texts. For example, Sheikh Tusi states that whoever takes people's property through deceit, fraud, and forgery in writings is liable to be punished and disciplined, and he must return what he has taken in full, and it is right for the ruler to punish him publicly so that others will learn a lesson and not engage in such immoral acts in the future [7].

Some other jurists have considered forgery and the use of a forged document to be immoral and un-Islamic and have issued fatwas for it. For example, Mohaghegh Ardabili states: The popular theory among Imamiyeh jurists is that a document is not valid, meaning that it cannot be ruled on as authentic because there is a possibility of forgery and forgery in it. Of course, in the case of forgery, since the property is taken without a battle, the battle ruling does not apply and ta'zir is imposed. Shahid Sani states that three groups are not subject to the punishment of being cut off:

1. The embezzler
2. The inventor
3. The forger [8]

Computer Forgery

The historical evolution of computer crimes from the invention of the computer to the early 2000s can be divided into three generations. The first generation, which was prevalent until the late 1980s, was known as computer crimes. These crimes mostly included theft, copying of programs, and invasion of the privacy of computer users. With the expansion of technology and international communications in the 1990s, the second generation of crimes became known as data crimes. During this period, crimes related to information technology, satellite communications, and international networks were defined as data crimes. In the mid-1990s, with the development of international networks and satellite communications, the third generation of computer crimes emerged as cyber or virtual crimes. The history of these crimes, based on the global development and developments in information technology, dates back to the 1960s, when the first cases referred to as "computer crimes" were reflected in the press and scientific publications of that era. These included espionage, computer sabotage, and illegal abuse of computer systems. Since the mid-1970s, empirical studies on computer crimes began, and in the 1990s, with the rapid growth of computer technology and the Internet, these crimes took on new forms and dimensions. In addition to well-known crimes, new crimes such as Internet password smuggling and multimedia crimes also emerged during this period. Today, transnational activities in the field of computer and Internet crimes have assumed broader dimensions and are constantly increasing [9]. Given that the use of computers in Iran has been limited since its introduction in 1962 until the 1990s, computer crimes do not have much history in our country. If any crimes have occurred during this period, no reports have been published. The occurrence of computer crimes in Iran began gradually in the 1990s, but there are no accurate statistics on this matter. Unauthorized use of computers to commit traditional crimes, the spread of viruses, and financial abuse were among the crimes that occurred on a small scale in the 1990s and were dealt with by conventional criminal laws. From the second half of the 1990s, especially with the beginning of the 2000s and the increase in the use of personal computers in private organizations and institutions and greater access to Internet services, the commission of computer crimes also increased sharply. Publishing immoral images and content, creating ethnic and racial divisions, publishing confidential documents, and literary theft were among the crimes that occurred after wider access to the Internet. The first legal response in Iran to some of these crimes appeared in the 1990 Press Reform Law, which was approved by the Guardian Council that same year. The second legal action was the 1990 Law on the Protection of the Rights of Computer Software Creators. Subsequently, the Armed Forces Crimes Punishment Law was passed in 2003, which criminalized the falsification of information and the misuse of computer data by the military. Finally, in 2009, the Computer Crimes Law was passed [10].

New Ethical and Legal Challenges in the Digital Age

Cybercrime and digital security: With the expansion of the Internet and cyberspace, new crimes such as hacking, data theft, phishing, and ransomware attacks have increased dramatically. Legal systems in different countries are faced with these crimes and must provide solutions to combat these types of crimes and protect data security [11].

Privacy and personal data: Maintaining privacy in the digital world has become one of the most important legal challenges. With the widespread collection and use of user data by large technology companies, issues such as user

consent, the right to be forgotten, and the responsibility for data protection have become particularly important [12].

Intellectual property and digital rights: New technologies have led to new challenges in the field of intellectual property. Questions have been raised about the ownership of content generated by artificial intelligence, copyright infringement in the online space, and how to protect digital works [13].

Artificial Intelligence and Liability: The use of AI in decision-making (such as self-driving cars, medical algorithms, and judicial systems) raises new issues of liability in the event of errors or damages. Determining who is liable in these cases is a major legal challenge [14].

Cryptocurrencies and Blockchain: The emergence of cryptocurrencies such as Bitcoin and blockchain-based technologies has raised many legal challenges in the areas of regulation, money laundering, financial crimes, and property rights [15].

E-commerce and Online Contracts: With the increase in e-commerce and online transactions, traditional contract laws have lost their effectiveness in some cases. This requires a review of regulations and the creation of laws that can protect the rights of customers and sellers in the online environment [16].

Virtual and Augmented Reality: These technologies have also led to new legal challenges, including in the areas of intellectual property, privacy protection, and liabilities arising from the use of these technologies [17].

Labor and human rights in the digital space: With the emergence of freelance and remote working platforms, new challenges have arisen in the field of labor rights. Issues related to contracts, the rights of digital workers, and the guarantee of their social rights have not yet been fully clarified [18].

These challenges require a review of existing laws and the development of new regulations to keep pace with the pace of technological change.

Aspects of Difference between Material and Spiritual Forgery

According to the sum of the above-mentioned matters regarding material and spiritual forgery, their distinctions and differences can be briefly stated as follows [19]:

a) Spiritual forgery occurs simultaneously and during the preparation of the writing or document, while material forgery occurs after the issuance of the document or document.
b) In spiritual forgery, no change is made in the material and body of the document or document, and therefore it does not leave a physical and tangible mark on the appearance of the document or document, while in material forgery, this is the opposite.
c) The heart of the truth in spiritual forgery appears in the form of changing and distorting the meaning and concept of the content of the document or document, while in material forgery, this occurs in addition to changing the concept or existing situation in the form of changing and distorting the letters, numbers, words and phrases contained therein, and ultimately the material and body of the document or document.
d) Spiritual forgery often occurs in official documents in a specific sense, but material forgery may occur routinely in any writing, whether official or unofficial.
e) The variety of examples of material forgery and the number of crimes committed and cases filed in this field in the judicial system are greater than spiritual forgery.

Methods of the Heart of Truth in Computer Forgery

The heart of truth, in both material and substantive dimensions, is the most important component of the material element of this crime.

It means changing and distorting reality in such a way as to violate a right or prove an injustice. This act may be carried out noticeably through a material act on the message data, such as when a false message data is created or existing message data is accompanied by fundamental changes through actions such as insertion, deletion, and stopping, thereby materially forging a message data that has financial and evidentiary value. Or the perpetrator's act may be carried out without any external effects, in such a way that no change is made in the appearance of the message data and a material distortion occurs. In this case, its contents and conditions are distorted and something false, correct, or the opposite is made to appear to be correct. For example, if tax officials or officials in charge of official offices commit forgery while performing their duties in entering information related to data messages and enter and process false information in the text of data messages that they are legally required to create or delete part of the existing facts and remove the data from the processing path, they will thereby violate a right or prove injustice. In such cases, the act of committing forgery is considered material and will be subject to punishment.

Therefore, although the legislator has used the general term forgery in relation to computer forgery and has not distinguished between material and moral forgery, as stated above, computer forgery may also be committed in both material and moral ways [3].

Elements of Computer Forgery

The legal element of this crime is stated in Article 6 of the Computer Crimes Law, approved on 2009/03/05, which states: "Anyone who commits the following acts without authorization shall be considered a forger and shall be sentenced to imprisonment for one to five years or a fine of twenty to one hundred million rials, or both. (a) Changing credentialed data or fraudulently creating or entering data. (b) Changing data or symbols on memory cards or processable in computer or telecommunications systems or chips or fraudulently creating or entering data or symbols into them.

Before the adoption of the Computer Crimes Law, Article 68 of the Electronic Commerce Law was active in this regard. This article states: "Anyone who, in the context of electronic exchanges, enters, changes, erases, and stops message data, interferes with the processing of message data and computer systems, or uses tools applied to cryptographic systems to produce a signature - such as a private key without the signatory's authorization, or produces a signature that has no record of registration in the electronic document registry, or does not match the name of the holder in the aforementioned list, or obtains a forged certificate, etc. - shall be considered a forger and sentenced to imprisonment for one to three years and a fine of fifty million rials [20].

Article 56 of the Computer Crimes Law states that laws and regulations that contradict this law will be repealed. In the initial version of this law, it was specifically stated that Articles 67 and 68 of the Electronic Commerce Law on computer fraud and forgery were repealed. However, the final text was limited to the general version of Article 56, and this action caused the validity of Articles 67 and 68 of the Electronic Commerce Law to be discussed and disputed among scholars. Some believe that Article 68 has been repealed because it covers virtually all computer counterfeiting, while others believe that Article 68 of the Electronic Commerce Law regarding computer counterfeiting in the context of electronic transactions remains in force and Article 6 of the Computer Crimes Law has not repealed the above article.

Also, the Cybercrime Convention and the Council of Europe Minimum List have also defined computer counterfeiting. The Cybercrime Convention states in its Article 7:

"Each State Party shall adopt such legislative and non-legislative measures as may be necessary to establish as criminal offences under its domestic law.

When acts such as entering, altering, deleting and blocking computer data are committed intentionally and without right, resulting in the creation of incorrect data, with the intention that they be interfered with or used in the same way as correct data for lawful purposes; Regardless of whether the data is directly readable and understandable, a State Party may require fraudulent intent or similar improper intent before criminal liability can be established [21].

The definition of the Council of Europe's minimum list is as follows: "Computer forgery, the entry, alteration, erasure or suspension of computer data or computer programs or any other intervention in the processing of data in a manner or under conditions described in national law, constitutes the crime of forgery, provided that it is committed with regard to the customary purpose of such a crime."

It should be noted that the first legal text that paid attention to the commission of computer crimes in our country was the Law on the Punishment of Crimes by the Armed Forces, approved on 29/10/2003. Article 131 of this law stipulates that any unauthorized change or deletion of information, addition, submission or delay of date from the actual date, etc., carried out by military personnel in computer systems and related software, as well as actions such as submitting classified computer information to the enemy or individuals who do not have the authority to access that information, unauthorized disclosure of information, theft of objects of informational value such as disks or diskettes containing information or their destruction, or financial abuse committed by military personnel using computers, are considered crimes and are subject to the penalties set forth in the relevant articles of this law, as the case may be. Although Article 131 does not distinguish between types of computer crimes, in any case, changing or deleting information, addition, submission or delay of date from the actual date, etc. include computer forgery and financial abuse related to computer fraud.

Comparing the outcome of a crime in computer forgery with traditional forgery

The issue of harm in traditional forgery is a complex issue that has different opinions about it, and these differences of opinion have led to the emergence of various theories in this field. In this section, we intend to analyze the result of the crime by examining the different opinions of jurists and the issued opinions in order to take a small step towards clarifying this issue.

First, we will provide a brief definition of harm and then we will discuss its role in the crime of forgery. In fact, harm in forgery means harm to public trust in the credibility and value of documents. For the crime of forgery to be committed, harm must be to the public and the realization of harm in itself is not a condition [22]. Therefore, whenever there is a possibility of harm, the crime of forgery will be prosecuted, because judicial practice has concluded that forgery is punishable in itself, regardless of the result it produces [23].

The result of the crime of forgery means "the possibility of harm to another"; Therefore, if a person commits one of the instances of this crime, then it can be said that the crime of forgery has been committed if, due to this act, actual harm has been caused to a person or the act of the forger potentially contains harm to him. On the other hand, if there is no potential harm, the crime of forgery will not be committed [24]. One of the law professors has stated regarding the importance of the element of harm in the realization of the crime of classical forgery: "One of the elements of the crime of forgery is the possibility of harm; therefore, if the change of the

truth in a document or writing does not have the ability to cause harm to another, it is not considered a crime" [23].

Also, another professor has stated regarding the basis of the element of harm in the crime of forgery: "The basis of the element of harm is present in the law, but it is not explicitly and directly stated, and legal doctrine has extracted this concept from the law over time" [22]. At least potential harm is necessary for the realization of the crime of forgery, and there must be a causal relationship between it and the material act in the crime of forgery [25]. The Supreme Court has stated in one of its decisions that "immediate harm is not a condition for the commission of the crime (forgery), but the act of forgery, even if it potentially involves harm in the future, is included in the cases of forgery. Therefore, the intentional destruction of a forged document will not generally prevent the prosecution of the crime" [23]. If actual harm were required for the commission of the crime of forgery, this act should never have been considered a crime, because no harm is caused to anyone by committing forgery, but rather it is the subsequent use of the forged document that causes harm [25]. What has been mentioned above regarding the element of harm, both potential and actual, is the prevailing opinion of the country's jurists.

In traditional forgery, unlike computer forgery, the legislator has considered differences in the amount of punishment based on the status of a government employee or non-employee. This is while in the Computer Crimes Law, Article 7 of this law, by using the phrase "everyone", includes all real people and does not make any distinction between ordinary people and government employees.

In the use of a forged document, as in traditional forgery, the person's position has an effect on determining the amount of punishment, but in the use of fake data, as explained, based on Article 7 of the Computer Crimes Law, due to the mention of the phrase "everyone", the person's position will not have an effect on the amount of punishment.

Forgery is not only a material crime, but also requires a psychological element; so that without establishing this element, it is not possible to prosecute the perpetrator. For this reason, the Penal Code has added the clause "with the intention of fraud" at the end of Article 523, which describes the instances of forgery. For the mental element of the crime of forgery to be fulfilled, the first condition is that there must be an intention to make or change. Therefore, if a person commits these acts while asleep, under the influence of drugs, or in a state of madness, he will lack general bad faith. On the other hand, the perpetrator must have the intention to deceive others so that what is forged is accepted as the original and thereby causes harm. For this reason, the presence of an intention to cause harm is also mandatory. At the end of Article 523, it is stated that the intention to deceive also includes the intention to harm. Therefore, if the forger does not intend to harm or deceive, the crime of forgery will not be fulfilled.

The perpetrator's awareness of the matter is also important in classic forgery. This means that if a person makes a change in a document and is aware of his authority, but it is later determined that he did not have such authority, the crime of forgery is not fulfilled.

In the use of a forged document, the mental element depends on the intention and free will of the perpetrator in using it. Unlike the use of forged data, in the case of a forged document, the existence of ultimate intent and specific malice is mandatory, and the person must intend to cause harm, whether material or moral, to a natural or legal person; of course, this specific malice or intent to harm is hidden in the general malice.

In traditional forgery, the motive does not affect the nature of the crime and can only lead to a

reduction in punishment in some circumstances. In comparing the moral element of traditional and computer forgery, it should be said that in traditional forgery, the legislator has clearly specified the specific malice and the moral element of forgery by mentioning the clause "with the intention of fraud", while in computer forgery, after mentioning the clause of reliance, the word "fraudulent" has been included at the end of paragraphs a and b of Article 734 of the Criminal Procedure Code. This word does not specify whether it expresses specific malice or refers to the material element, and removing this clause seems more useful, because the existence of the clause of reliance alone is sufficient and adding another clause under the title of fraudulent increases the existing ambiguities.

Comparison of counterfeiting law in Iranian and Iraqi law

The Iraqi legislature, under the title “Chapter Five: Crimes that Violate General Conscientiousness,” has dedicated the first chapter to the imitation and counterfeiting of seals, signs, and stamps, the second chapter to the manipulation of money and financial papers, and the third chapter to the counterfeiting of documents and writings. In this division, the Iraqi legislature has collected all forms of counterfeiting in three chapters from Articles 137 to 171 and has mentioned the penalties related to different types of counterfeiting in these same sections. In contrast, the Iranian legislature has adopted a different approach. On the one hand, it has mentioned the crimes of counterfeiting not only in the Islamic Penal Code but also in other laws, and on the other hand, unlike the Iraqi legislature, it has not divided the crimes of counterfeiting into multiple laws [27]. This approach of the Iranian legislature makes it difficult to compare and contrast the two legal systems. In fact, the Iranian legislature has combined the crimes that are mentioned separately and in two chapters in the Iraqi law into a single article and has considered the same punishment for them. Therefore, if we want to proceed according to the order of Iraqi law.

The Iraqi legislator has divided this section into four types under the title of forgery of documents. The first type includes articles 181 and 187, which define forgery and the methods of committing it. The second type is dedicated to forgery of official documents and this issue is addressed in three articles 188 to 133. The third type refers to specific cases of the crime of forgery in writings, and the fourth type in articles 131 to 138 deals with forgery in ordinary documents. Therefore, the contents of this section will be examined in two topics:

According to article 188 of the Iraqi Penal Code, an official document refers to a document that is drawn up by a government official or a public service official according to existing documents or statements of people related to the subject and in compliance with legal conditions and within the limits of the official's authority. Based on the definition of Iraqi jurists, this definition seems broad, so some of them have added restrictions to this definition to make it more practical. These jurists believe that an official document must be prepared by a public service official and that the legal and local jurisdictional conditions must be observed in preparing it. After defining an official document, the Iraqi legislator states that any document that does not meet these conditions will be considered an ordinary document. The penalty for forgery of official documents is between one and fifteen years in prison according to Articles 183 and 133. According to Article 183, if a specific crime is not assigned to the perpetrator, the penalty will be between one and fifteen years in prison. In Article 133, if a government official prepares a document incorrectly or enters false information into the document, the penalty is between five and fifteen years in prison [28]. In Iranian law, according to

Article 1284 of the Civil Code, "a document is any writing that can be relied on in a lawsuit or defense." Also, according to Article 1287, an official document refers to a writing that has been prepared in the Department of Registration of Documents and Real Estate or Notaries or with government officials and within the limits of their jurisdiction in accordance with legal regulations. Unlike the Iraqi legislature, which directly addresses forgery of official documents, the Iranian legislature has devoted Articles 111 to 116 of Book Five of the Islamic Penal Code to various types of forgery of writings, documents, seals, and certificates.

This difference in approach makes it difficult to compare the two laws, as the Iraqi legislature has included general provisions on forgery of official documents in one section, while the Iranian legislature has stated these provisions in various and scattered articles. Therefore, in this section, we will first examine forgery of official documents in Iraq and then conduct a similar examination in Iranian law [29].

According to Article 131 of the Iraqi Penal Code, any person who, by using a false name or identity, succeeds in obtaining documents such as an official license, identification card, general election card, or driving and transportation license, will be sentenced to a penalty of three months to five years in prison and a fine of up to three hundred dinars, or both.

In order for this crime to be committed, the aforementioned documents must first be obtained by adopting a false name or identity. Therefore, if a person succeeds in obtaining these documents without using these methods, for example by paying a bribe, this act will not fall under the crime set forth in this article. In addition, the crime is committed when the person has obtained one of the documents mentioned in the article. If a document other than what is stated in the article is obtained by using a false name, this act will also not be in accordance with this article.

There is no article similar to this article in the Islamic Penal Code of Iran. Of course, Articles 523 and 526 of this law refer to the crime of forgery and fraud by government employees and public service officials. According to Article 523, "Any employee of government departments, judicial authorities, and public service officials who commit forgery or falsification in the preparation of documents and contracts related to their duties, whether by changing the subject or content thereof or distorting the words and writings of an official, or by making a false order appear true or a true order appear false, shall, in addition to administrative penalties and compensation for damages, be sentenced to imprisonment for one to five years or a fine of six to thirty million rials."

In accordance with Article 526, "Any employee and public official who commits forgery in official decrees, writings, and documents in the performance of their duties shall be sentenced to imprisonment for one to five years or a fine of six to thirty million rials."

A comparison of these two articles shows that the material element of these crimes is very similar. The difference is that in Article 523, the perpetrators of the crime are introduced as "employees of government departments and judicial authorities and public service officials," but in Article 526, these individuals are known as "employees and government officials."

Some legal writers see the difference between the two articles as being that Article 523 refers to government employees and officials in general, while Article 526 refers more to employees of the country's judicial systems. However, some other writers do not consider this difference correct and believe that Article 523 is sufficiently complete and that Article 526 is not needed [30].

Unlike Iraq, the Iranian legislature has defined the crime not only for government employees but

also for non-employees. According to Article 527, "Persons who are not government employees or officials and who commit the crimes mentioned in the previous article shall be sentenced to imprisonment for a period of six months to three years or a fine of three to eighteen million rials." One of the differences between these articles and Article 131 of the Iraqi Penal Code is that in Article 131, forgery must result in the receipt of official documents, but in Articles 523 and 526 of the Iranian Code, any type of writing is subject to the crime of forgery. Therefore, the scope of the crime in Iranian law is broader than in Iraqi law. Some Iranian legal writers believe that some of the instances mentioned in Article 523 also include moral forgery, while others believe that all instances of this article include material forgery [31].

CONCLUSION

Since the advent of writing and the beginning of the use of writing to convey intentions and thoughts, distortion and alteration of lines and words have been recognized as immoral, undesirable and criminal. In Islamic law, forgery is recognized as one of the examples of Ta'zir crimes, and the Holy Quran has also considered this act immoral and reprehensible and has included it among the sins.

With the comparative analysis presented regarding computer forgery and electronic documents in the laws of Iran and Iraq, general and practical conclusions can be reached. This study showed that both legal systems, despite similarities in the main concepts and objectives of the laws, have different approaches in formulating and implementing regulations related to forgery and electronic documents. The Iraqi legislator has addressed the crime of forgery and fraud in its laws in a more coherent and focused manner. In Iraq, the crime of forgery is divided into specific chapters and its different types are stated more precisely in the legal articles. This structure allows researchers, judges, and lawyers to more easily access legal interpretations and facilitate the process of handling cases.

In contrast, the Iranian legislature has adopted a more dispersed approach. The crimes of forgery and forgery are mentioned in various laws, including the Islamic Penal Code, the Civil Code, and other related laws. This dispersion may create legal complications and make it difficult to compare and contrast with other legal systems. Also, the Iranian legislature has in some cases defined the scope of criminalization more broadly than Iraq; for example, while Iraqi law focuses more on official documents, Iranian laws have extended the crime of forgery to unofficial documents and writings.

In terms of legal provisions, both countries have emphasized the difference between official and ordinary documents, but in Iraq this distinction is made more carefully and clearly. The definition of an official document in Iraqi law includes additional requirements, including compliance with legal conditions and the competence of the issuing officer. This is while Iranian law has a simpler approach to defining an official document and focuses more on the ability to cite documents as a claim or defense.

One of the notable points in comparing these two legal systems is their different approach to the crime of forgery by government officials. In Iraq, these crimes are defined specifically and with an emphasis on the role of government officials, while Iranian law is broader in this regard and has expanded the scope of criminalization to non-governmental individuals. Also, Iraqi law explicitly addresses the criminal liability of officials who enter false information into documents, but in Iran, this issue is expressed in more general terms and in the form of scattered regulations.

Overall, the findings of this study indicate that Iraqi law may be superior to Iran in terms of

enforceability in some cases due to its coherence and transparency. On the other hand, Iranian laws, with their broader criminalization, have been able to cover a wider range of crimes, but the fragmentation of regulations can create challenges in implementing these laws. As a result, it seems that a review of the structure of Iranian laws and a move towards greater coherence can help improve the legal situation in this area. This is especially important in the context of new crimes such as computer counterfeiting, because with the advancement of technology and continuous changes in cyberspace, the need for clear, transparent, and coordinated laws is felt more than ever.

ETHICAL CONSIDERATIONS

Ethical issues (such as plagiarism, conscious satisfaction, misleading, making and or forging data, publishing or sending to two places, redundancy and etc.) have been fully considered by the writers.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interests.

REFERENCES

1. Lali Farahani A. Preventing computer crimes. [M.A thesis] Tehran: Imam Sadeq University. 2005. (In Persian).
2. Bay H, Poorghahremani B. Jurisprudential and legal study of computer crimes. 1st ed. Tehran: Publications of the Islamic Jurisprudence and Law Research Institute. 2009.
3. Bagheri Asl, R, Rastegar N. Explaining the cybercrime law in mobile government services. Tehran: Parliment Research Center. 2009.
4. Al-Sulaimani R. Iraqi legislation in the field of cybercrimes. Baghdad: Dar Al-Fajr. 2024. (In Arabic).
5. Al-Jubouri A. Cybercrimes: A Study on Victims. Basra: Dar Al-Fikr. 2024. (In Arabic).
6. Azmayesh A. Special criminal law course notes. [M.A thesis]. Tehran: Tehran University. 1978. (In Prsian).
7. Khodadadi M, Dadash Nezhad D. The place of ethics in the criminalization of criminal offenses in iran's legal system. Ethics in Science and Technology 2024; 19 (2) :41-49. Doi: 10.22034/ethicsjournal.19.2.41
8. Javanmard B, Jafarzadeh S, Ghoreishi SM. Analysis of money laundering precautionary measures to establish an ethical market based on Iranian and international law. Ethics in Science and Technology 2023; 18 (2): 9-15. Dor: 20.1001.1.22517634.1402.18.2.2.1
9. Javidnia J. E-commerce crimes. 1st ed. Tehran: Khorsandi Publication. 2008. (In Persian).
10. Mehrpoor H, Madani Bajestani M, Hajbarkolaei SS. Role of principles of ethics in the legal function of computer. Ethics in Science and Technology 2020; 15 (3) :13-19. Dor: 20.1001.1.22517634.1399.15.3.3.3
11. Madih A, Rahmat M R, Arzhang A. Favorable social and moral consequences of organized crime management in society. Int. J. Ethics Soc 2023; 5 (2): 9-17. Doi: 10.22034/ijethics.5.2.13
12. Channak Z. Business Ethics in E-Commerce – Legal Challenges and Opportunities. Access to Justice in Eastern Europe, 2023; 6: 1-16. Doi: 10.33327/AJEE-18-6S007
13. Choraś, Michał & Pawlicka, Aleksandra & Jaroszewska-Choraś, Dagmara & Pawlicki, Marek. Not Only Security and Privacy: The Evolving Ethical and Legal Challenges of E-Commerce. 2024. Doi: 10.1007/978-3-031-54204-6_9
14. Atrey I. Cybercrime and its Legal Implications: Analysing the challenges and Legal frameworks surrounding Cybercrime, including issues related to Jurisdiction, Privacy, and Digital Evidence. International Journal of Research and Analytical Reviews, 2023; 10(3). Doi: 10.1729/Journal.35277
15. Taherdoost H. Legal, regulatory, and ethical considerations in E-Business. 1st ed. Canada: University Canada West. 2023. Doi: http://dx.doi.org/10.1007/978-3-031-39626-7_15
16. Lubis, Fauziah. (2022). Cyber Crime E-Commerce Business Transactions. SASI. 28(4): 589. Doi: 10.47268/sasi.v28i4.1068
17. Singh C, Journals C. Impact of cyber law on e-commerce and digital transactions. Global Journal of Current Research, 2024; 11(3): 44-48. Doi: 10.13140/RG.2.2.16689.19042
18. Mujtaba BG, Cavico F. E-Commerce and social media policies in the digital age: legal analysis and recommendations for management. Journal of Entrepreneurship and Business Venturing, 2023; 3(1). Doi: 10.56536/jebv.v3i1.37
19. Ong D, Kamaruddin A, Bulathsinhalage C, Seneviratne L. The influence of materialistic and ethical values on the purchase intention of counterfeit luxury goods: the case of Malaysian Undergraduates. Journal of Marketing Research and Case Studies, 2013; 2013: 1-17. Doi: 10.5171/2013.356704
20. Rostami H. Computer fraud; A reflection on the elements of crime and its effects. *Criminal Law Doctrines*, 2020; 16(18): 51-82. doi: 10.30513/cld.2020.558
21. Mohammadi Fardovi A. Criminal investigation of the elements of the crime of computer forgery in Iranian law. Ghanoonyar, 2018;2(8):459-476. (In Persian).
22. Salari M. Forgery and fraud. 1st ed. Iran/Tehran: Mizan Publication. 2007. (In Persian).
23. Poorbaferani H. Crimes against public safety and well-being. 1st ed. Tehran: Jungle Publication. 2011. (In Persian).
24. Mir Mohammad Sadeghi H. Crimes against public safety and well-being. 6th ed. Tehran: Mizan Publication. 2006. (In Persian).
25. Matin A. Collection of judicial procedures. Iran/Tehran: Hashemi Publication. 1951. (In Persian).
26. Zandi MR. Preliminary Research on Information Exchange Crimes. 1st ed. Tehran: Jungle Publications. 2010. (In Persian).
27. Al-Bazzaz M. Cybersecurity: Rights and duties. 1st ed. Najaf: Al-Huda Library. 2024. (In Arabic).
28. Al-Nasiri O. Cybersecurity in Iraq: Problems and solutions. 1st ed. Baghdad: Dar Al-Noor. 2024. (In Arabic).
29. Al-Obaidi I. The impact of cybercrimes on human rights in Iraq. 2nd ed. Najaf: Al-Jisr Library. 2024. (In Persian).

30. Al-Khazarji N. Cybercrimes: Methods and legislation. Basra: Dar Al-Kitab. 2024. (In Arabic).

31. Mosalaee A. Forgery and fraud in Iranian criminal law. 2nd ed. Tehran: Third Line Publication. 2008. (In Persian).