
Criminal protection of electronic signatures from forgery in Jordanian and UAE legislation

Ashraf Fathi Al-Rai

Midocean University,
Fujairah, 51124, UAE
Email: Ashrafraie@gmail.com

Nayel Musa AlOmran*

Department of Legal Studies,
Zayed University,
Abu Dhabi, P.O. Box 19282, UAE
Email: drnayel0@gmail.com

*Corresponding author

Abstract: This paper focuses on the importance of electronic signatures in civil and commercial transactions, especially considering the widespread use of the internet. It discusses the issue of electronic signature forgery, which has become one of the negative consequences of globalisation. The main problem addressed in this paper is the ease of forging electronic signatures and the lack of legal protection against these crimes in Jordanian laws. The paper used the descriptive, analytical, deductive, and comparative approaches. The authors found that the Jordanian laws related to crimes and electronic transactions do not explicitly stipulate the act of forging electronic signatures and that the protection contained therein is for data, credit information, and electronic space only, and this is a clear deficiency. To address this problem, the paper recommends approving a special text criminalising the forgery of signatures and electronic documents in the Jordanian cybercrime law, like UAE legislation.

Keywords: criminal; forgery; electronic; protection; signature; legislation; UAE; Jordan.

Reference to this paper should be made as follows: Al-Rai, A.F. and AlOmran, N.M. (2024) 'Criminal protection of electronic signatures from forgery in Jordanian and UAE legislation', *Int. J. Electronic Governance*, Vol. 16, No. 2, pp.246–262.

Biographical notes: Ashraf Fathi Al-Rai is an Assistant Professor of Criminal Law in Midocean University, UAE. He holds two Master's degrees in Criminal Law and Electronic Crimes, and Media. Academic achievements are a part of his experience concluded in writing and publishing more than a book on criminal laws with gaining the privilege to consider these books as a reference in different universities. He works in his private office to provide legal advice in the UAE, and he was an Assistant Professor at Applied Science University, Jordan. He worked as Legal Consultant with different companies in UAE and Jordan.

Nayel Musa AlOmran is currently an Associate Professor of Constitutional and Administrative Law in Legal Studies at Zayed University, UAE. Previously, he worked at the College of Law, Al Ain University, as an Assistant Professor for four years. In addition, he worked at the Department of Management, University of Malaya, Malaysia, for three years as an Assistant Professor. His experience teaching undergraduate and graduate courses in constitutional law, administrative law, business law and ethics, and many other legal courses. As a researcher, he has an excellent track record of publishing in highly qualified and widely-read peer-reviewed international journals. He has more than 35 publications in high-ranking journals (Scopus).

1 Introduction

The world is currently witnessing remarkable technological progress and development in various sectors, supported by the widespread use of the internet. Many commercial and social activities now use modern methods, including cloud computing, artificial intelligence systems, and digital platforms for transactions and contracts. Hence, it is necessary to adhere to appropriate legal protocols when conducting transactions, using advanced technologies and systems that keep pace with the latest developments in this field. With the emergence of the electronic signature, there are concerns about the extent of its exposure to fraudulent activities, because it replaces the traditional handwritten signature and raises questions about its legal protection, especially in light of the lack of legal texts to achieve criminal protection for it in Jordan, especially in the Jordanian Cybercrime Law. The electronic signature has become crucial in civil and commercial transactions due to the advancements in technology. However, legal disputes have arisen among professionals in these fields regarding its validity. This has led to the question of whether forging an electronic signature is considered a crime in the legal sense, especially when considering the challenges presented by the internet and information transmission mechanisms. Despite the internet's ability to connect people globally, it has also made it easier to forge electronic signatures. Electronic signatures are essential for facilitating efficient and trustworthy transactions, particularly in the rapidly growing field of e-commerce. They help streamline the contract process, saving time, effort, and money for all parties involved. Many countries have recognised the significance of electronic signatures and have updated their legal regulations accordingly. In this paper, we will explore the current laws related to electronic signatures in Jordan and UAE.

Electronic signatures have become a popular tool for signing documents and conducting business transactions. However, one of the major concerns associated with this practice is the ease with which these signatures can be forged. This raises concerns about the safety and security of electronic signatures, especially in terms of criminal protection. In the context of Jordanian legislation, there is a lack of clear guidelines regarding the use of electronic signatures. This contrasts with the more advanced legislative framework of UAE, which has established comprehensive regulations and guidelines for electronic signatures. The Jordanian Cybercrime Law did not stipulate the protection of electronic signatures from forgery, but rather stipulated the protection of electronic data, information, and electronic space, and this is a large text. Given the potential risks associated with the use of electronic signatures, it is important for policymakers and legal experts to carefully consider the best practices and regulatory

frameworks that can help ensure the safety and security of these important tools. By doing so, we can help promote the widespread adoption of electronic signatures while also protecting the interests of individuals and businesses alike.

The significance of criminal protection for electronic signatures cannot be overstated, particularly considering the numerous technological advancements that have emerged in recent years. With the internet, information networks, cloud computing, digital platforms, and social media becoming increasingly prevalent, electronic signatures have become the norm for commercial and civil contracts. However, this has also led to a proliferation of forgeries, which has raised questions about the level of criminal protection that should be afforded to electronic signatures. As such, it is crucial that we examine this issue in greater depth and take the necessary steps to ensure that electronic signatures are adequately protected in order to achieve this goal, the authors employ a descriptive approach to explain the concept of electronic signatures and their characteristics. The authors also use an analytical approach to classify legal texts in a systematic way that clarifies the legal aspects of electronic signature validity. Additionally, the authors utilise the deductive approach to establish clear concepts of legal terms discussed in this study and highlight them. Furthermore, the authors compare Jordanian and Emirati legislation regarding the criminal protection of electronic signatures. The study proposes several questions it endeavours to answer as:

- 1 What is the concept of electronic signature and its characteristics?
- 2 What is the authority of an electronic signature as evidence in commercial and civil contracts?
- 3 What criminal protection is imposed for electronic signatures against the crime of forgery?
- 4 What are the types of electronic signature in the era of artificial intelligence?
- 5 What are the shortcomings in the Jordanian cybercrime law?
- 6 What are the proposals to stipulate the crime of forging an electronic signature in Jordanian criminal legislation?

2 Research plan

- What Is an Electronic Signature?
- Authenticity of Electronic Signatures
- Conditions for an Authentic Electronic Signature
- The Evidential Strength of The Electronic Signature and its Applications
- The Crime of Forging an Electronic Signature
- Conclusion.

3 What is an electronic signature?

The emergence of digital platforms and websites can be traced back to the launch of the internet in 1969. At that time, the US Department of Defense established a specialised team to integrate computers for the purpose of exchanging military information. Over time, the uses of the network expanded, and by 1986, supercomputer centres were being used in a variety of commercial, industrial, and media fields. It was during this time that the concept of electronic signatures began to take shape (Abdel Dayem, 2014).

Even with efforts from the legal and judicial systems to explain the electronic signature, advancements in technology have made it difficult to clearly define its nature. Additionally, some countries' commercial and civil legislation have not yet accepted the use of electronic signatures (Abdel-Rida and Hadi, 2012). In legal terms, some people view it as a means of proof that follows the same guidelines as a conventional signature (In Majdoub, 2015). Meanwhile, others see it as a unique identifier associated with a particular individual. Legally, it is referred to as digital data that takes on a specific format, which came about after the advent of the internet (Al-Abasiri, 2003).

In order to provide an accurate definition of the concept of electronic signature, it is essential to examine its legal and jurisprudential definitions. Despite being a relatively new term with distinct characteristics, we will explore these aspects in two separate sections.

3.1 Definition of electronic signature

A signature often reflects the personality of its owner and can convey their commitments (as stated by Al-Ghanami (2019)). Each state has the right to establish its own regulations and procedures for electronic signatures based on its internal laws (as explained by Buraidat (2006)). The definition of electronic signature has been a topic of debate in the legal and judicial communities, resulting in differing opinions as previously mentioned.

However, Article (2/A) of the UNCITRAL Model Law on Electronic Signatures (2001) stipulated a clear definition regarding the electronic signature, which was followed by many other legislations, which stated that "An electronic signature refers to data in electronic form that is either included in a data message or logically related to it. Its purpose is to identify the signatory in relation to the data message and to signify their agreement with the information contained in it".

Following Jordan's accession to the World Trade Organisation and the signing of numerous international agreements related to global and free trade, it became necessary to remove obstacles hindering commercial operations that required speed, accuracy, and security in the electronic field. To achieve this, The Jordanian Electronic Transactions Law No. 15 of 2015 stipulates that an electronic signature is an information in the form of letters, numbers, codes, symbols, or other and which is electronically, or in any other similar mean, included in, affixed to, or associated with an electronic record. It is used to authenticate the identity and unique usage of the signatory and differentiate him from others.

The definition of an electronic signature was clearly outlined in Article 1 of the Emirati legislator's Federal Decree Law No. (46) of 2021 on electronic transactions and trust services. This law replaced Federal Law No. (1) of 2006 on transactions, electronic commerce, and trust services. According to the definition, an electronic signature is made up of letters, numbers, symbols, voice, fingerprint, or a processing system in electronic

form. It is attached to or logically linked to an electronic document, and it serves to verify the identity of the person who signs it and their acceptance of the content of the associated data.

It is noted that the Emirati legislator included the use of voice or fingerprint as an electronic signature, while the Jordanian legislator only specified text “or any other similar means in the information message... that has a character that allows identifying the person who signed it”.

All legislations require electronic signatures to verify the signer’s identity, in accordance with advancements in recognising electronic signatures and documents. These signatures hold the same authority as traditional signatures and documents for proof. However, the process of proof can be problematic due to the possibility of electronic signature manipulation and forgery by criminal networks abroad, leading to difficulties. The United Nations Commission on International Trade Law created legal rules related to electronic commerce and developed the UNCITRAL Model Law on electronic signatures in 1996 to prevent conflicts between electronic commerce laws. The Model Law also establishes the validity of electronic signatures.

The electronic signature can take various forms, including signing with an electronic pen, through email, using artificial intelligence systems, or via text messages. Nowadays, smart applications have become prevalent in our modern world and offer another way to sign electronically.

In the era of artificial intelligence, electronic signatures have evolved to offer more security, efficiency, and convenience like advanced electronic signatures (AES) which offer higher levels of security and are often backed by cryptographic techniques to ensure authenticity, integrity, and non-repudiation and Biometric Signatures which signatures authenticate individuals based on unique biological characteristics such as fingerprints, facial recognition, iris scans, or voice recognition, and these are highly secure and difficult to forge and also, Blockchain-based Signatures which ensures the immutability and traceability of electronic signatures by storing them in a decentralised and tamper-proof ledger this enhances trust and security, especially in sensitive transactions, and remote online notarisation (RON) which allows signers to electronically sign documents in the presence of a notary public via audio-video technology (Chau, 2021).

The emergence of e-commerce and online transactions were a natural progression of mobile phone technology. Nowadays, it’s possible to conduct all commercial transactions through smart applications, which are an advanced and convenient alternative to traditional brick-and-mortar stores. Additionally, an electronic signature can be defined as an electronic mark that identifies its owner and can be used as evidence.

3.2 Characteristics of electronic signature

In order to delve into the distinguishing traits of electronic signatures, it is essential to first differentiate between these modern signatures and their traditional counterparts. This differentiation should be based on both their form and function. By doing so, we can better understand the unique features that set electronic signatures apart from traditional signatures.

A person’s traditional signature is a one-of-a-kind symbol, design, or mark that sets them apart from others. It represents their individuality and demonstrates their accountability for the content of any document they sign. The signature is also viewed as an expression of their character and typically features their given or family name. The

main objective of a traditional signature is to connect the signature to the individual who affixed it, confirming that the signer did so voluntarily and knowingly in their physical presence.

An electronic signature refers to data in electronic form, which can be in the form of letters, symbols, signs, numbers, or sounds. It serves the same purpose as a traditional signature in verifying the identity of the owner of the signature (Buraidat, 2006).

The electronic signature serves as a confirmation of an individual's agreement and acknowledgement of the information presented in an electronic document. It provides a modern and advanced way for individuals to express their intentions, keeping up with the technological advancements in the world, particularly in the realm of electronic commerce and documentation. Despite these advancements, the primary aspect that remains consistent between traditional and electronic signatures is the individual's association with the signature, which must be made freely, by their own will and choice, and with a commitment to the content of the document (Khattabi, 2020–2021).

The creation of an electronic signature involves utilising advanced electronic devices that possess exceptional electromagnetic, electrical, or optical capabilities. Conversely, the traditional signature involves manually writing on paper supports. It is worth noting that despite the dissimilarity in their form and function, both types of signatures serve the same purpose and are globally recognised and approved by international bodies. These signatures are characterised by their high level of trust and security, and they have been extensively used in US for a period of over four decades since the 1980s (Al-Saqqqa, 2008).

The most prominent characteristics of an electronic signature are:

- 1 In order for an electronic signature to be valid, it must be linked to a single individual whose appointment has been authorised. The signature must also be completed using electronic means that are under the direct control of the signer. This helps to demonstrate the signer's connection to the content and objectives of the signature (Khadija, 2014–2015). It is important to note that electronic signatures are unique to each individual and cannot be replicated by anyone else.
- 2 Using an electronic signature can save time and effort while ensuring speedy transaction completion. It does not require the signatory to be present in person. This means that it can be done from anywhere in the world (Hegazy, 2006). The world's technical revolution and progress in this field have led to the widespread use of the internet. This has made it possible to conduct trade, civil transactions, and buying and selling from anywhere in the world. As a result, the form of offer and acceptance issued in traditional sales operations has changed, as was the case in the past (Khattabi, 2020–2021).

Electronic signatures are known for their security and confidentiality. Only in cases of hacking and privacy breaches, which are considered crimes under the Jordanian Cybercrime Law, can someone gain access to them. While these occurrences may not be common in Arab societies, it's important to acknowledge them as a potential danger in the digital world that could be exploited by activists, pirates, or hackers (Al-Nawaisa, 2017). Article 5 of the European Electronic Signatures Directive of 1999 regulates the legal effects of electronic signatures. It stipulates that, "Member States must ensure that electronic signatures that rely on qualified certificates and that are created by means of a secure signature creation tool fulfil the legal requirements for a signature. It relates to

data in electronic form in the same manner as signatures and is acceptable as evidence in legal proceedings...”

Article 6, paragraph 3, of the UNCITRAL Model Law on Electronic Signatures stipulates “the conditions that must be met in an electronic signature, which are:

- The method used to create the signature must be linked to the site and not to any other person.
 - The means used to create the electronic signature must be subject to the control of the signatory at the time of signing and not any other person.
 - Any change in the electronic signature made after the signature occurs shall be discoverable...”
- 3 There are numerous ways to express an electronic signature, including images, letters, and numbers. Unlike traditional signatures that are restricted to hand signatures, fingerprints, or stamps, electronic signatures are a product of advanced technology. Unlike traditional signatures, electronic signatures do not fade away or disappear over time since they are stored on electronic mediums. As a result, they can be easily accessed whenever needed.

Once the characteristics of an electronic signature have been explained, it is important to note that certain conditions must be met in order for it to be considered valid proof. Article 6, paragraph 3 of the UNCITRAL Model Law on Electronic Signatures outlines the “specific requirements that must be met for an electronic signature to be deemed valid”.

In Section 2 of this study, we will address two requirements. The first requirement pertains to the conditions necessary for an electronic signature to be considered authentic. The second requirement deals with the probative strength of the electronic signature and its various applications.

4 Authenticity of electronic signatures

In the early days of electronic signatures, there was much debate among legal scholars regarding their validity. Specifically, there were concerns about whether electronic signatures could be reliably attributed to a specific individual and if they could be forged in the same way that traditional signatures can. Unlike traditional signatures, which typically feature unique writing styles or other distinct markings that allow them to be easily distinguished from forgeries, electronic signatures do not have any such features. This lack of distinctiveness was a significant point of contention for legal scholars who were concerned about the potential implications of electronic signatures in the world of law (Khadija, 2014–2015).

In jurisprudence, it is believed that a signature serves the purpose of identifying the person who signed it. This is particularly important in the technical and electronic world, such as in automated financial teller machines and open web networks like the internet. Even in the field of intranets, where identity authentication is not always required, an electronic signature can still be useful if it achieves its goal. Essentially, an electronic

signature serves the same function as a traditional one (Alwan, 2000). However, it is important to note that electronic signatures can be forged, which is why it's crucial to use the correct electronic signature to prevent identity theft and unauthorised access to the World Wide Web.

To determine the authenticity of an electronic signature, it is crucial to consider the specific requirements that must be met. These requirements establish the signature's legitimacy while also addressing the possibility of forgery. First, we will examine the conditions that must be satisfied for an electronic signature to be considered genuine. Then, we will discuss the signature's probative power and practical applications.

5 Conditions for an authentic electronic signature

Most modern electronic commerce laws require specific conditions to be met by electronic signatures in order for them to have authority in evidence and be acceptable for adoption and protection against forgery. Article 6 of the UNCITRAL Law specifies these conditions and confirms the complete authority of electronic signatures when they are met. These conditions include linking the electronic signature to the person who signed it, ensuring that it distinguishes its owner from anyone else, having the electronic signature system under the control of the signatory, and the ability to detect any changes in the signature. We will discuss these conditions in detail below:

1 The identity of the signatory:

For an electronic signature to be authentic, it must clearly and specifically identify the person who signed it, just like a traditional signature. If an electronic signature fails to do so, it cannot be trusted or used as evidence. The purpose of a signature is to express the personality of the signer, and an electronic signature serves this purpose just as well as a traditional one. It cannot be forged or claimed as such, since it reflects the unique identity of the signer. Article 260 of the Jordanian Penal Code defines forgery as "an artificial distortion of the truth in the facts and data that are intended to be proven by an instrument or manuscript that is used as evidence or that could result in material, moral, or social harm". It is defined by Article 216 of UAE Federal Penal Code No. 3 of 1987 as "tampering with documents, whether official or unofficial, by inserting an addition to the content of the document or a deletion from the content of the document...". The Jordanian Electronic Transactions Law does not stipulate forging an electronic signature as a crime, although it stipulates many other crimes that require it to be returned. It is noteworthy that the Penal Code and the Electronic Crimes Law have general regulations that have been criticised for their surprising nature. However, Article 15 of the Electronic Crimes Law outlines the necessary conditions for electronic signatures to be safeguarded.

"The electronic signature is considered protected if the following conditions are met together: A. If it is unique to the owner of the signature to distinguish it from others, B. If it identifies the owner of the signature, C. If the private key is under the control of the owner of the signature at the time the signature is made, D. If it is linked to the electronic record in a way that allows making an amendment to that electronic record after it is signed without causing change to that signature".

2 *Not affected by time*

One crucial requirement for an electronic signature is its ability to remain unaltered by time and accessible for retrieval at any given moment. The unique technological tools employed in electronic signatures distinguish them from traditional signatures, which are susceptible to the effects of time, as previously noted.

3 Acknowledgement of what was signed:

If a signature is an acknowledgement of what was signed, it is considered an electronic signature and can be relied upon. This is similar to a traditional signature and is connected to the personality of the person who signed it. However, if it does not constitute an acknowledgement, it cannot be relied upon to acknowledge what was signed through electronic data. Researchers believe that a signature is a free and frank expression of the signer's will, which leads to the conclusion of legal transactions.

4 The electronic signature and editor are closely related, forming a single unit.

6 **The evidential strength of the electronic signature and its applications**

In modern commerce, electronic signatures have become an essential aspect of conducting business. It is crucial to bear in mind that customary documents, although significant, are usually not accepted as evidence unless they have been appropriately signed. Such is the mandate put forth by Contractual and Commercial Obligations Article 28, which stipulates that unsigned documents hold no weight as evidence. This particular rule also expounds on what is permissible and impermissible for proof by testimony, taking into account certain provisions. It is important to understand and abide by these regulations to ensure the credibility and validity of all business transactions: "A. If the value of the contractual obligation in non-commercial matters exceeds 100 dinars or if the value is not specified, then testimony is not permissible in proving the existence of the obligation". Or acquittal of it unless there is an agreement or text stipulating otherwise. B. Taking into account the provisions of any special law, proof may be given by testimony in commercial obligations, regardless of their value, and in civil obligations if their value does not exceed 100 dinars...", as stipulated in Article 29 that "it is not permissible to prove by testimony regarding contractual obligations, even if the value of what is requested does not exceed 100 dinars:

- 1 What is contrary to or adjacent to what is included in written evidence.
- 2 Whether what is requested is the remainder or is part of a right not It may be proven by testimony.
- 3 If one of the litigants in the case demanded an amount whose value exceeds 100 dinars, then amends his request to an amount that does not exceed this value".

For the judiciary to accept electronic contracts, they must acknowledge the authenticity of the electronic signature and its reliability as evidence in disputes. This acknowledgement is dependent on whether the signature fulfils the terms and conditions previously discussed. If the authenticity cannot be proven, then any forgery cannot be relied upon (Al-Janabihi and Al-Janabihi, 2004).

In today's world, with the rapid advancement of technology and the rise of digital platforms, websites, social media sites, and artificial intelligence systems, traditional methods of implementing contracts for commercial and civil transactions are no longer feasible. Electronic signature systems have become more common due to the interconnected network in which the world operates.

In order to ensure the validity of electronic signatures, it is crucial to prevent any modifications or alterations to them, including deletion, addition, or any other changes. This will help establish a connection between electronic and traditional signatures, which will enhance the accuracy and reliability of legal proceedings, as well as commercial and civil contracts, whether they have been signed or will be signed in the future. Any manipulation or misrepresentation of electronic signatures must be avoided to maintain their integrity.

When it comes to electronic signatures, there is a potential issue with their authenticity. Unlike traditional signatures, which are considered to be absolute, electronic signatures may not be fully trustworthy without the presence of a third-party verification of the signer's identity. Researchers have even gone as far as to suggest that electronic signatures may not be as reliable as their traditional counterparts when it comes to authenticity. It is important to ensure that precautions are taken to verify the identity of the signer when using electronic signatures to avoid any potential issues.

The researchers strongly suggest implementing strict regulations on electronic signatures with legal consequences. This is due to the rapid advancements in technology that make it difficult for individuals to keep up with and increases the risk of tampering with commercial documents and contracts in the digital world. As more transactions become electronic, it is essential to have extensive information and personal data to ensure the authenticity of electronic signatures. The digital revolution brought about by the Global Communications Network and the global revolution of consumers and shoppers via the internet have made electronic signatures easily accessible (Al-Rai, 2022).

7 The crime of forging an electronic signature

The Jordanian legislature has not provided a precise definition for electronic forgery or forgery of an electronic signature. However, it has outlined the procedure for modifying or altering electronic data in accordance with the Cybercrime Law (Baara, 2015). Unlike the Emirati legislature, it has not explicitly identified electronic signature forgery.

Jurisprudence tried to define electronic forgery as "a criminal activity that aims to manipulate the electronic document directly or indirectly to achieve the intended criminal goal" (Al-Dabaiba, 2016). Some jurisprudence also defined information forgery as "changing the truth in automatically processed documents and information documents with the intention of using them" (Al-Qahwaji, 2000).

Jordanian law outlines the process for amending or altering electronic data in Articles 3 and 4 of the Electronic Crimes Law, and addresses forgery in general in Article 260 of Penal Code No. 16 of 1960 and its amendments. However, this is viewed as a legislative deficiency by researchers. To address this, we will examine the elements of this crime in the Jordanian Penal Code, Cybercrimes Law, and Electronic Transactions Law, and compare them with relevant UAE legislation. In each of the three demands, we will discuss the material element, the moral element, and the stipulated penalty.

7.1 The physical element of the crime of forging an electronic signature

The act of forging an electronic signature is addressed in the Jordanian Penal Code's Article 260 and Electronic Crimes Law's Articles 3 and 4. The physical aspect of the crime is considered by the Penal Code as "an artificial distortion of the truth in the facts and data that are intended to be proven by an instrument or manuscript that is used as evidence or that could result in material, moral, or social harm".

Article 3 of the 'Cybercrime Law' also stipulates in paragraph (a) that

"Anyone who intentionally accesses an information network or an information system by any means without authorisation or in a manner that violates or exceeds the authorisation shall be punished by imprisonment for a period of not less than one week and not more than three months or a fine of not less than 100 dinars and not more than 200 dinars, or both of these two penalties".

Paragraph (B) stipulates an aggravating circumstance if the entry stipulated in Paragraph (A) of this Article is for

"cancelling, deleting, adding, destroying, disclosing, destroying, blocking, amending, or changing, or transferring or copying data or information, or stopping or disrupting the operation of the information network or the information system of the information network. The perpetrator shall be punished by imprisonment for a period of not less than three months and not exceeding one year and a fine of not less than 200 dinars and not exceeding 1000 dinars".

Paragraph (c) also stipulates that

"Anyone who intentionally accesses the cartoon website to change it, cancel it, destroy it, modify its contents, occupy it, impersonate it, or impersonate its owner shall be punished by imprisonment for a period of not less than three months and not more than one year and a fine of not less than 200 dinars and not more than 1000 dinars".

According to the text of paragraphs (b) and (c) of Article 3, accessing an information system with the intention of changing or modifying is punishable, even though the Jordanian legislator did not use the term forgery, as is the case with the Emirati legislator. Article 14 of Federal Decree Law No. 34 of 2021 regarding combating rumours and electronic crimes stipulates that "anyone who forges an electronic document from the federal or local government or authorities shall be punished by temporary imprisonment and a fine of not less than 150,000 dirhams and not more than 750,000 dirhams". Or federal or local public institutions. The penalty shall be imprisonment and a fine of not less than 100,000 dirhams and not more than 300,000 dirhams, or one of these two penalties, if the forgery occurs in the documents of an entity other than those stipulated in Clause 1 of this paper, and the same penalty shall be imposed. The penalty prescribed for the crime of forgery, according to the circumstances, is "whoever uses the forged electronic document with knowledge of its forgery". This is a commendable approach suggested by the Emirati legislator, where the researchers recommend implementing forgery laws for electronic documents through the Electronic Crimes Law or the Jordanian Electronic Transactions Law.

Therefore, it is apparent that under UAE legislation, the material offence involves the creation of a falsified electronic document, which is considered as an act of forgery. This act of forgery is defined in Article 216 of UAE Penal Code as "introducing a real change to an instrument by performing operations on it, whether by addition, deletion, or change

in the writing of the instrument, numbers, marks, or images existing in or on it, with the aim of changing its reality...”.

Article 4 of the ‘Jordanian Cybercrime Law’ also stipulates that

“anyone who intentionally enters, publishes, or uses a programme via the information network or using an information system to delete, delete, add, destroy, disclose, damage, block, modify, change, or transmitting, copying, capturing, enabling others to view data or information, obstructing, disrupting, stopping or disabling the operation of an information system or accessing it, or changing a website”.

The perpetrator commits a crime by publishing or using electronic programmes to modify or alter electronic data or information, including electronic signatures. This crime applies to natural persons, companies, large institutions, individual institutions, social entities, or organisational associations, as well as public institutions. According to Al-Nawaisa (2017), the crime of forgery defined in the Penal Code also applies to the act of forging an electronic signature under Article 15 of the Electronic Crimes Law.

The act of forging an electronic signature can be done through various methods, with the most common being the use of an electronic pen to create a copy of the signature and paste it onto another document (Al-Ghalabi, 2012). This makes it difficult to prove in some cases, according to criminal jurisprudence (Rabadi, 2009). Another way this crime can occur is through obtaining the password from the owner and using it to forge the electronic signature (Al-Ghalabi, 2012). However, the burden of proof falls on the person making the claim, as per the general rule.

According to Article 260 of the Penal Code, in order for an act to be considered forgery, there must be evidence of harm that has been caused or could potentially be caused. Additionally, there must be a clear connection between the act and the harm. This requirement is not specified in Articles 3 and 4 of the Cybercrime Law but is determined as “an artificial distortion of the truth in the facts and data that are intended to be proven by an instrument or manuscript that is used as evidence or that could result in material, moral, or social harm”.

7.2 The moral element of the crime of forging an electronic signature

Regardless of how they are categorised, whether it be under Articles 3 or 4 of the Cybercrime Law or Article 260 of the Jordanian Penal Code, these offences are deemed premeditated. They require only knowledge and intent to be committed. Specifically, the offender must possess an understanding of their actions and consciously decide to engage in them.

Article 14 of Federal Decree Law No. 34 of 2021 on combating rumours and electronic crimes stipulates that “the perpetrator must have the intention to commit the criminal act of forgery” in order for the crime to occur.

A recent decision by the Amman Penal Magistrate Court stated:

“Criminal intent, as defined in Article (63) of the Penal Code, is the will to commit the crime as defined by the law. Criminal intent consists of two elements: knowledge and will, so that the will of the perpetrator is directed toward committing the act. Despite his knowledge that this act is punishable by law and that committing it would enable the crime to be achieved by achieving its result, his will nevertheless directs him to commit the act and achieve the result...” (Judgement No. 5337 of 2022, Amman Penal Court)

7.3 *Penalty for forging an electronic signature*

Article 3 of the 'Cybercrime Law' stipulates in paragraph (A) that

"Anyone who intentionally accesses an information network or an information system by any means without authorisation or in a manner that violates or exceeds the authorisation shall be punished by imprisonment for a period of not less than one week and not exceeding three months or a fine of not less than 100 dinars and not more than 200 dinars, or both of these penalties".

Paragraph (B) stipulates an aggravating circumstance if the entry stipulated in Paragraph (A) of this Article is for

"cancelling, deleting, adding, destroying, disclosing, destroying, blocking, amending, or changing, or transferring or copying data or information, or stopping or disrupting the operation of the information network or the information system of the information network. The perpetrator shall be punished by imprisonment for a period of not less than three months and not exceeding one year and a fine of not less than 200 dinars and not exceeding 1000 dinars."

Paragraph (C) also stipulates that

"Anyone who intentionally accesses the cartoon website to change it, cancel it, destroy it, modify its contents, occupy it, impersonate it, or impersonate its owner shall be punished by imprisonment for a period of not less than three months and not more than one year and a fine of not less than 200 dinars and not more than 1000 dinars."

Article (4) of the Jordanian 'Cybercrime Law' stipulates that the penalty for the crime of modifying data or information is "imprisonment for a period of not less than 3 years and not more than one year and a fine of not less than 200 dinars and not more than 1000 dinars".

The penalty for committing this act while on the job or by exploiting work shall be doubled, as stated in Article 8 of the same law, "The penalty for the crimes stipulated in Articles (3) to (6) of this law shall be doubled against every person who commits any of them by performing his job or work or by exploiting any of them".

The accomplice and instigator shall receive the same punishment as the perpetrator, as stated in Article 14 of the law: "Anyone who intentionally participates, intervenes, or incites to commit any of the crimes stipulated in this law shall be punished with the penalty specified therein for their perpetrators".

The penalty is also increased in the event of repetition in accordance with the text of Article 16 of the law, which states that "the penalty stipulated in this law shall be doubled in the event of repetition of any of the crimes stipulated in it".

The punishment for forgery, as stated in the Penal Code, varies depending on the type of document forged. If the document is an official one, it is considered a felony, and the perpetrator can be sentenced to temporary labour for a period of 5 to 15 years. If the perpetrator is an employee and forges a document related to their work, the minimum term is 7 years. Those who instigate or aid in the forgery will receive the same punishment. If the document is not official, the charge is a misdemeanour, and the punishment is imprisonment for one to three years and a fine of at least 50 dinars.

Attempting to commit the misdemeanour crimes outlined in Articles 3 and 4 of the Cybercrime Law is not possible without a provision in the law, as stated in Article 71 of the Jordanian Penal Code. It is important to distinguish between the criminal act and

misdeemeanour in the crime of forgery, according to the provisions of the Jordanian Penal Code. While attempting to forge official documents is punishable, there is generally no punishment for attempting to forge private documents as a misdemeanour, unless otherwise specified by the law.

According to the findings of the researchers, it is highly recommended to institute strict penalties for any type of forgery, regardless of whether the falsified documents are of an official or private nature. This is primarily due to the potentially hazardous repercussions that these counterfeit documents can have on society. As such, it is imperative that significant measures be taken to deter individuals from engaging in such deceptive and dangerous acts.

According to Article 14 of Federal Decree Law No. 34 of 2021 on combating rumours and electronic crimes in UAE, forging an electronic document from a federal or local government or authority can result in temporary imprisonment and a fine ranging from 150,000 to 750,000 dirhams. The same penalty applies for forging documents from federal or local public institutions. If the forgery occurs in documents of an entity other than those specified in Clause 1 of this paper, the penalty is imprisonment and a fine ranging from 100,000 to 300,000 dirhams, or one of these two penalties. The punishment for the offence of forgery varies based on the situation. If someone knowingly uses a forged electronic document, they may face severe penalties, including fines and imprisonment under UAE law. This strictness is commendable since it protects both official and unofficial electronic documents from forgery, including electronic signature forgery. It's important to note that this applies to all aspects of electronic documents, including forging signatures or altering information in electronic documents.

7.4 Judicial rulings

The Jordanian judiciary addressed signature forgery in general, as stated in one of its judgements:

“The plaintiff filed a complaint stating that the defendant, when he authenticated the signature of his client, was abroad. It was revealed during the investigation that the lawyer indeed did not meet his client, and he admitted that his client did not sign the power of attorney in his presence but sent it to him with her father. The Criminal Court considered the defendant's actions as forgery and the use of forged documents, sentencing him to three years of hard labour in its decision number (204/2016), Qastas Publications. However, in its decision number (12660/2018) M. Qastas, the Court of Appeal acquitted the defendant of the charges attributed to him, considering that the role of the lawyer was limited to authenticating the validity of the signature attributed to his client without her presence, and there was no evidence indicating his distortion of the truth and committing forgery. In its decision number (1093/2019) M. Qastas, the Court of Cassation affirmed the direction of the Court of Appeal, summarising its decision by stating that the crime of forgery, if proven, requires criminal intent on the part of the forger in terms of the physical element represented by distortion and alteration of the truth, and the forger's intention to use the forged document to harm the complainant, which negates the mere authentication by the lawyer of his client's signature in her absence constituting the crime of forgery”.

In comparison, the Public Prosecution in UAE clarified in one of its rulings that according to Article 14 of Federal Decree-Law No. 34 of 2021 concerning combating rumours and electronic crimes, imprisonment, and a fine ranging from AED 150,000 to

AED 750,000 shall be imposed on anyone who forges an electronic document from the documents of the federal or local government, authorities, or public federal or local institutions. The penalty shall be imprisonment and a fine ranging from AED 100,000 to AED 300,000, or one of these two penalties, if the forgery occurs in documents from an entity other than those specified in paragraph (1) of this paper. The same penalty prescribed for forgery shall be imposed, as appropriate, on anyone who uses the forged electronic document with knowledge of its forgery.

8 Conclusion

This study discussed the significance of electronic signatures in relation to the current technological advancements and concerns over forgery, particularly due to the increasing use of online platforms for commercial transactions. The study yielded a number of findings and recommendations which are summarised as follows:

- 1 Electronic signatures play a crucial role in facilitating swift transactions and building trust among customers, especially within the realm of e-commerce. Their ability to expedite contract agreements while saving time, effort, and resources has led many countries to update their legal frameworks accordingly.
- 2 The current legislation in Jordan lacks clear provisions addressing electronic signature forgery under both the Electronic Crimes Law and Electronic Transactions Law. Recommendations: Building on these findings, it is recommended that relevant authorities consider revising existing laws or implementing new regulations to explicitly address issues surrounding counterfeit electronic signatures, and The inability of Jordanian law to specify the types and forms of electronic signature compared to UAE law.
- 3 To ensure the protection of electronic space, Article 15 of the Cybercrimes Law allows for the application of relevant provisions regarding forgery as outlined in the Penal Code. Additionally, Articles 3 and 4 of the Cybercrimes Law serve to provide comprehensive protection for electronic transactions.

9 Recommendations

- 1 The study recommends adding a special text that criminalises the forgery of an electronic signature due to its seriousness, or the forgery of an electronic document, following the example of UAE legislator.
- 2 The study suggests that all forms of forgery should be punished due to their significant negative impact on society, regardless of whether the forged documents are official or private. Whether the crime of forgery is categorised as a misdemeanour or a felony under the Electronic Crimes Law or as a misdemeanour under the Jordanian Penal Code, it still warrants punishment.

- 3 The researchers suggest implementing a measure to penalise individuals who knowingly use a falsified electronic document. This can be achieved through the Electronic Crimes Law or the Jordanian Electronic Transactions Law, similar to the Emirati legislation.

Conflict of Interest

The authors declare that they have no conflicts of interest.

Funding

The authors did not receive support from any organisation for the submitted work.

Compliance with ethical standards

This paper does not contain any studies involving animals performed by any of the authors. This paper does not contain any studies involving human participants performed by any of the authors.

Data availability statement

Research data are not shared.

References

- Abdel Dayem, S. (2014) 'The nature of new media and its means – a theoretical study', *Journal of Public Relations Research in the Middle East*, Egyptian Society for Public Relations, Cairo, Arab Republic of Egypt.
- Abdel-Rida, A-R. and Hadi, M.J. (2012) 'The legal concept of electronic signature', *Al-Muhaqiq Al-Hilli Journal of Legal and Political Sciences*, First Issue, Fourth Year, University of Babylon, Iraq.
- Al-Abasiri, F. (2003) *Subscription Contract in Electronic Information Bases, An Applied Study of Internet Contracts*, Dar Al-Nahda Al-Arabiya, Cairo, Egypt.
- Al-Dabaiba, S.M. (2016) *Substantive and Procedural Provisions for the Crime of Electronic Forgery in Jordanian Legislation*, Master's Thesis, Amman Arab University, Amman, Jordan.
- Al-Ghalabi, R.A.K. (2012) *The Crime of Forging an Electronic Signature*, Imam Jaafar Al-Sadiq University, Baghdad, Iraq.
- Al-Ghanami, N.B.N. (2019) 'The electronic signature and its validity in proof by application to the Saudi system', *Journal of Sharia and Regulations*, Regulations Department, Taif University, Kingdom of Saudi Arabia.
- Al-Janabihi, M.M. and Al-Janabihi, M.M. (2004) *The Electronic Signature and Its Validity in Proof*, Dar Al-Fikr Al-Jami'i, Alexandria, Egypt.
- Al-Nawaisa, A-I. (2017) *Information Technology Crimes, Explanation of the Substantive Provisions in the Cybercrime Law*, 1st ed., Dar Wael for Publishing and Distribution, Amman, Jordan.
- Al-Qahwaji, A.A.Q. (2000) 'Criminal protection of electronically processed data', *Research Presented to the Conference on Law, Computers and the Internet*, Qustas Publications.

- Al-Rai, A. (2022) *Criminal Protection of the Sanctity of Private Life Through the Media in Jordanian Legislation – a Comparative Study*, Doctoral Thesis, International Islamic Sciences University, Amman, Jordan.
- Al-Saqqa, I.F. (2008) *The Crime of Forgery in Electronic Documents*, New University House, Alexandria, Egypt.
- Alwan, R.M. (2000) *Expressing Will Online*, Research Submitted to the Jordanian Bar Association, Amman, Jordan.
- Baara, S. (2015) *Cybercrime in Algerian Legislation*, Master's Thesis, Mohamed Khudair University, Biskra, Algeria.
- Buraidat, M.A. (2006) Electronic Signature: A Study of the Jordanian Temporary Electronic Transactions Law No. 85 of 2001', *Jerash Journal of Research and Studies*, Vol. 10, No. 2, Jerash University.
- Chau, D. (2021) *Anti – Money Laundering Transaction Monitoring System Impleentaions: Funding Anomalies*, John Wiley & Sons, London.
- Hegazy, A.F.B. (2006) *Electronic Government and Its Legal System*, Dar Al-Fikr University, Alexandria, Egypt.
- In Majdoub, A. (2015) *Electronic Signature*, *Journal of Law and Human Sciences*, No. 23, Zayan University, Ashour, Djelfa, Joan, Algeria.
- Khadija, G. (2014–2015) *Electronic Signature*, Master's Thesis, Kasdi Merbah University – Ouargla, Algeria.
- Khattabi, F. (2020–2021) *'Criminal Protection of Electronic Signatures*, PhD thesis, University of Batna, Lahj Lakhdar, Algeria.
- Rabadi, I.G. (2009) *Rules for Electronic Signature*, *Dar Al-Thaqafa for Publishing and Distribution*, Amman, Jordan, Second: Scientific theses.