

Criminal Protection of the Electronic Document

Tarak QADRI ⁽¹⁾

⁽¹⁾ Lecturer, grade "A", faculty of law, Mouloud Mamery University, Tizi ouzou, Algeria.

Email: tarak.qadri@ummto.dz

Abstract :

Technological advancements in the field of electronic communications have enabled human interaction and the easy and convenient conduct of transactions. The use of such technologies has facilitated the efficient delivery of healthcare services, the development of intellectual property, and advancements in various other fields. Information networks and electronic data interchange systems represent an application of modern technological use in the realm of communications. However, this technology may be misused, thereby posing a threat to public safety and the national interest. While modern electronic means of communication allow for the swift and reliable execution of financial transactions, the use of these methods is not without risk. Some criminals may exploit these means to commit crimes through fraud or by infringing upon the privacy of users and the confidentiality of their transactions. Although technological progress has sought to combat crimes in the field of communications by resorting to encryption to maintain confidentiality, such measures have at times enabled perpetrators to exploit these procedures by using communication methods that are difficult to penetrate or monitor. This means that technological advancement has provided criminals with powerful and practical tools to perpetrate their offences.

Keywords:

Document, electronic, protection, cybercrime, legal framework.

Received: 10/08/2025 & Accepted :15/12/2025 & Edited :27/12/2025

Corresponding author: Qadri tarak, email: tarak.qadri@ummto.dz

الحماية الجنائية للمستند الإلكتروني

الملخص:

وفرت التكنولوجيا في مجال الاتصالات الإلكترونية إمكانية تحقيق التواصل الإنساني وإنجاز المعاملات في سهولة ويسر، وأتاح استخدامها حسن تقديم خدمات الرعاية الصحية وتنمية الملكية الفكرية، وغيرها من المجالات. وتعد شبكات المعلومات ونظم التبادل الإلكتروني للبيانات تطبيقاً للاستخدام التكنولوجي الحديث في مجال الاتصالات غير أن هذه التكنولوجيا قد يساء استعمالها ويصبح يهدد استخدامها السلامة العامة والمصلحة الوطنية، فإذا كانت وسائل الاتصال الإلكتروني الحديثة تتيح إنجاز المعاملات المالية بشكل سريع وموثوق؛ فإن استعمال هذه الوسائل لا يخلو من مخاطر، فقد يستغل بعض المجرمين هذه الوسائل في ارتكاب جرائمهم بطريق الاحتيال أو المساس بخصوصية هؤلاء المتعاملين وسرية معاملاتهم. وإذا كان التقدم التقني قد حاول مكافحة الجرائم في مجال الاتصالات ولجأ إلى تشفيرها بما يحفظ سريتها، فإن هذه الإجراءات قد أفضت إلى استغلال الجناة لهذه الإجراءات في ارتكاب جرائمهم باستخدام وسائل اتصال يصعب اختراقها أو الوقوف على محتواها، وهو ما يعني أن التقدم التقني قد أمد المجرمين بوسائل بالغة القوة والفاعلية في ارتكاب جرائمهم.

الكلمات المفتاحية:

وثيقة، الكترونية، الحماية، الجريمة الإلكترونية، الإطار القانوني.

Protection pénale du document électronique

Résumé :

La technologie des communications électroniques a permis la communication humaine et la facilitation des transactions. Son utilisation a permis la prestation efficace de services de santé, le développement de la propriété intellectuelle et d'autres domaines. Les réseaux d'information et les systèmes d'échange de données électroniques sont des applications des technologies modernes dans le domaine des communications. Cependant, ces technologies peuvent être utilisées à mauvais escient et menacer la sécurité publique et les intérêts nationaux. Si les méthodes de communication électroniques modernes permettent des transactions financières rapides et fiables, leur utilisation n'est pas sans risques. Certains criminels peuvent exploiter ces méthodes pour commettre leurs crimes par fraude ou en compromettant la vie privée et la confidentialité des utilisateurs. Si les progrès technologiques ont tenté de lutter contre la criminalité dans le domaine des communications et ont eu recours au cryptage pour préserver leur

confidentialité, ces mesures ont conduit les auteurs à exploiter ces procédures pour commettre leurs crimes en utilisant des méthodes de communication difficiles à pirater ou à déchiffrer. Cela signifie que les progrès technologiques ont doté les criminels de moyens extrêmement puissants et efficaces pour commettre leurs crimes.

Mots clés :

Document, électronique, protection, cybercriminalité, cadre juridique.

Introduction

The electronic document is connected to an important array of administrative, commercial, and financial systems that encompass both the state and individuals alike. An electronic document is one of the essential tools for realising the concept of “e-government,” which provides services to individuals, as well as public and private entities. The electronic document is also integral to the operations of bodies working in the fields of banking, insurance, medical services, and others, as these institutions conduct their activities by relying on this document.

The electronic document serves as a means for international trade to achieve its objectives. Through this document alone, transactions can be conducted, and dispositions and deals can be concluded, as necessitated by the concept of electronic commerce. Ensuring the protection of the electronic document facilitates the acceleration of commercial transactions and cost savings. The electronic document is closely linked to the right to confidentiality and privacy and is also related to the protection of consumer rights. This document embodies the rights of both parties to a contract, serving as a reference for what the parties have agreed upon and for determining their legal obligations. The protection granted to the electronic document, therefore, guarantees protection for the consumer as well.

The protection of electronic documents achieves legal stability and security. Protecting the electronic document, whether in terms of its content and signature or by safeguarding its confidentiality and preventing disclosure, provides individuals with assurance and ensures the stability of transactions. Moreover, it enables this document to stand as evidence, on an equal footing with paper documents, which ultimately leads to stability within the legal system and a reduction in disputes.

Accordingly, we have chosen to pose the following problem:

To what extent is the protection granted to the electronic document adequate in confronting criminal acts that target it?

Section I :The Nature of the Electronic Document

In this section, of the study, we address the concept of the electronic document and identify its elements, followed by an explanation of its forms in two subsections.

A)- Definition and Elements of the Electronic Document:

Electronic transactions are numerous and vary significantly from one another. On the one hand, these transactions may take place on open communication networks accessible to all without distinction, such as the internet, or on closed networks where dealings are limited to a restricted number of individuals or entities, such as in the case of networks belonging to companies, governmental institutions, and bodies providing services such as healthcare and insurance¹. New communication systems have contributed to increasing the significance and efficiency of electronic transactions; examples include private transaction networks (such as SWIFT), which are capable of executing transactions within moments, as well as means of remote communication and electronic data interchange systems².

The need arises to establish a precise definition of the electronic document to enable the identification of its forms and the acts that may affect it. The importance of defining this concept is highlighted by the varying approaches of legislations in their references to the electronic document and in the extent of the protection accorded to it.

Most legislations do not develop a general theory for the electronic document, nor do they set out general rules that apply to any document possessing an electronic nature. Instead, these legislations are limited in addressing the main applications of the concept of the electronic document, such as electronic signatures and records.

¹ "Are Your Financial Institution's Computer Systems Impenetrable?," *Cyber Security by Chubb SM for Financial Institutions*, 2003.

<http://businesses/industrygroups/index.html>.

² Hussein Shahada al-Hussein, "Electronic Documentation in Letters of Credit," study presented to the Third Scientific Conference of Egyptian Jurists, organised by the Egyptian Society for Political Economy, Statistics, and Legislation on the legal aspects of banking operations, Cairo, 19–20 December 2002, p. 1.

1- Definition of the Electronic Document:

Many legislations have not enacted provisions to define the concept of the electronic document, determine its evidentiary value, or penalise acts that affect it. As a result of this legislative deficiency, a jurisprudential dispute has arisen as to whether the punitive provisions that protect paper documents apply to electronic documents. One view in the legal literature holds that the term "document" in existing statutes should be interpreted broadly to include electronic documents, whereas another view does not support this approach.

a. Broad Definition of the Electronic Document:

This view holds that the term "document" can be extended to encompass both paper and electronic documents since the linguistic origin of the word "document" is not confined to a particular form. It includes writing on paper in its traditional sense, as well as other forms, including electronic writing. For the signature of a document, it is not required that it be of a specific type; rather, any form of signature that indicates the attribution of the document to its author, and any means that performs the function of identifying the signatory and expresses its definite intent to be bound by its content, is regarded as a signature³.

According to this view, it is necessary to abandon the traditional concepts of "document," "writing," and "signature" and to recognise the electronic document when it possesses technical safeguards equivalent to those prevailing in paper documents. This approach further holds that since the principle of freedom of evidence is the basis for proving commercial transactions, permitting the establishment of such transactions by all means of proof without the need for formal evidence, the application of this principle requires that the judge be left to assess the evidentiary strength of modern methods. This view concludes that equivalence between the meaning of the electronic document and that of the paper document can be achieved through a broad jurisprudential and judicial interpretation of existing provisions, thereby granting the concept of "document" a scope encompassing all forms that may fall under this definition⁴.

³ Muhammad Hossam al-Din Lotfi, "The Use of Modern Communication Means in Negotiating and Concluding Contracts," study presented to the Seminar on Methods for Settling Disputes in Banking Operations, Cairo Regional Centre for International Commercial Arbitration, June 1998, p. 8; and by the same author, *The Legal Framework for Electronic Transactions: A Study of the Rules of Evidence in Civil and Commercial Matters with Special Reference to Some Arab Countries' Laws*, Cairo, 2002, pp. 34–35.

⁴ Muhammad Hossam al-Din Lotfi, *Ibid.*, "The Use of Modern Communication Means in Negotiating," p. 41.

b. Narrow Definition of the Electronic Document:

The prevailing view in legal scholarship holds that the existing provisions were established to regulate matters related to paper documents and that it is not possible to reinterpret current statutes to extend their application to electronic documents. Instead, there is a need for the enactment of specific legislation governing the electronic document, taking into account the safeguards that must be provided to ensure its effectiveness and acceptance in transactions⁵.

The basis for this view is that the meaning of the document protected by criminal statutes is necessarily linked to “instruments and papers.”⁶ Proponents of this view argue that forgery committed in electronic documents falls outside the concept of forgery in traditional documents. The rationale is that forgery in a document requires that the document expresses human thought and has a tangible, physical existence that can be seen with the naked eye, which is not the case for electronic data, as such data cannot be perceived except through technical means that enable its visualisation⁷.

2- Elements of the Electronic Document:

The question arises as to the distinguishing elements of the electronic document. These elements serve, at the same time, as criteria by which the features and scope of the electronic document can be determined, and thus, the acts that affect and infringe upon it can be identified. Applying such criteria also makes it possible to distinguish electronic documents from other forms that may be confused with them.

In our estimation, the electronic document is characterised by three elements:

- The first element is that it contains an expression of coherent human meanings and ideas;
- The second element is that this expression possesses legal value;
- The third element is that the document is characterised by its electronic nature.

⁵ For example, in Egyptian law: Ghanam Muhammad Ghanam, *The Inadequacy of Traditional Rules in Combating Computer Crimes*, p. 34; and Medhat Abd al-Halim Ramadan, *Criminal Protection of Electronic Commerce*, p. 31.

⁶ For a critique of this jurisprudence, see Omar al-Faruq al-Husseini, No. 46, p. 82.

⁷ Muhammad Sami al-Shawa, p. 161.

The expression of coherent meanings implies that what the document contains serves as a means for communication and the exchange of ideas. This affirms the social role of the document as a means for conducting legal transactions⁸.

The legal significance of the document means that any infringement upon it results in harm, as established in the offences relating to the forgery of ordinary documents⁹. For example, such infringement may affect information for which the document was created to provide proof, such as the electronic signature, or it may involve information that could serve as evidence or legal proof, even incidentally. An example of this would be forgery of the date of an electronic document, even though the date may not have been included for evidentiary purposes. This approach has been adopted in many comparative legislations; for example, German law, in the offence of falsifying electronic records, requires that the electronic record concern “a fact of legal value”¹⁰.

For the electronic nature of a document, various operations related to the document, such as its creation, storage, retrieval, transmission, or copying, are carried out via technology that involves electrical, digital, magnetic, wireless, optical, electromagnetic, or other similar elements¹¹.

It must be capable of identifying its user, allowing the user to retain the signature’s code under their exclusive control, and making it possible to detect any subsequent alteration of the signature’s data¹².

Some legal scholars have considered the use of credit and magnetic withdrawal cards as an application of the electronic signature¹³. In our view, however, this opinion is questionable, as these cards do not constitute electronic documents, and all legislations have required that the electronic signature be linked to an

⁸ Mahmoud Najib Hosni, No. 356, p. 247.

⁹ For this element, refer to general jurisprudential writings on the crime of forgery, for example: Mahmoud Najib Hosni, No. 370, p. 259 and following.

¹⁰ “Zum Beweis einer rechtlich erheblichen Tatsache bestimmt ist,”

¹¹ “*Electronic*” means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.”

The Electronic Signatures and Records Acts of the states of Kansas and Connecticut adopted this definition. Kansas Statute No. 16-1602, 2001–200

<http://www.kslegislatures.org/currenthappenings/index.html>.

An Act Concerning the Connecticut Uniform Electronic Transactions Act, op.cit.

¹² Draft of a Law on the Framework Conditions, 2 (2), p. 4.

¹³ Tharwat Abd al-Hamid, *The Electronic Signature: Its Nature, Risks, Means of Addressing Them, and Its Evidentiary Value*, Al-Jalaa Al-Jadida Library, Mansoura, 2001, No. 90, p. 100 and following.

electronic record, whether by being integrated with it or logically associated with it. This does not appear to be the case with such cards.

B)- Forms of the Electronic Document:

In this part of the study, we address various forms of electronic documents, such as electronic contracts, electronic credit letters, and, finally, electronic payment orders.

1-The Electronic Contract:

The electronic contract is an agreement concluded by offer and acceptance, similar to ordinary contracts that are executed and signed in writing; however, the offer and acceptance are accomplished by electronic means without the need for a written document¹⁴. An example of this is when the offeror sends their offer to the other party by e-mail, where the recipient, whether an individual or a legal entity, signs the offer electronically to indicate acceptance and returns it to the sender. In this way, the contract is concluded and acquires its legal force¹⁵. It makes no difference whether acceptance is communicated in a separate message sent to the offeror or within the same document containing the offer. This can be achieved by the recipient of the offer clicking a button on the document's page that signifies acceptance, after reviewing the contract's terms, or by placing an electronic signature in a designated field and returning the document to the offeror¹⁶.

2- The Electronic Letter of Credit:

When a buyer wishes to import goods, they conclude a contract of sale with the seller, agreeing that payment will be made by means of a letter of credit. The buyer then approaches their bank, requesting the opening of a letter of credit in favour of the seller, specifying all the details of the sale transaction. The bank then notifies the seller of the letter of credit opened in their favour, either directly or

¹⁴ On distinguishing the electronic contract, see Osama Abu al-Hasan, "The Particularities of Contracting via the internet," study presented to the conference held by the College of Sharia and Law, United Arab Emirates University, on "Law, Computers, and the internet," held in Al Ain, 1–3 May 2000, p. 37. He considers the distinguishing feature of this contract to be its conclusion via the internet. In our view, this definition narrows the concept of the electronic contract, which is not limited to contracts concluded solely over the internet but extends to other electronic means such as private networks or electronic data interchange systems.

¹⁵ Cummings, *E-Sign Act Raises the Speed Limit on the Information Superhighway*, op.cit.; *New Law Makes E-Signatures Valid, Contracts Created Online Are Now as Legal as Those on Paper*, op.cit.

¹⁶ *New Law Makes E-Signatures Valid*, op.cit.; Cummings, op.cit.

through a corresponding bank in the country of origin. This latter bank may confirm the letter of credit; if so, it becomes obligated to pay the beneficiary in addition to the obligation assumed by the issuing bank¹⁷. Suppose that the issuing bank is satisfied that the goods' documents conform to the terms of the credit letter. In that case, it will reimburse the corresponding bank for the amount paid to the beneficiary. If the documents do not comply with the terms, the issuing bank will notify the corresponding bank of the rejection of the documents within a reasonable period.

Technological advancements have led to the emergence of the “electronic letter of credit,”¹⁸ whereby the abovementioned procedures are carried out through electronic means of communication. The importer sends the application to open the letter of credit electronically, and the bank responds in the same manner; if accepted, the text of the letter of credit is sent electronically to the beneficiary. Before the expiration of the letter of credit, the beneficiary sends the required shipping invoices electronically. The beneficiary also sends electronic messages to the parties involved in the sale, such as the shipper, insurer, and preshipment inspector, requesting that they send their documents electronically to the issuing bank. The issuing bank then forwards the received electronic messages to the corresponding bank¹⁹.

The electronic letter of credit enables transactions to be completed with great ease, convenience, and speed, granting its users a competitive advantage over those who use traditional methods. It also reduces the cost of sending documents and allows parties to benefit from electronic exchange in resolving problems arising from goods arriving before the relevant documents.

Regulation 500 does not contain provisions governing the electronic letter of credit. Nevertheless, Article 20(b) of this regulation considers documents produced by modern technological means, such as computers, to be accepted as original documents unless the letter of credit contract provides otherwise, on the condition that they are marked as original and, when necessary, appear to be signed.

¹⁷ Hussein Shahada al-Hussein, *Ibid.*, p. 1.

¹⁸ “Electronic Documentary Credit.” And Ismat Abdel Majeed Bakr, *The Role of Scientific Techniques in Developing the Contract*, Dar Al-Kotob Al-Ilmiyah, Beirut, 2015.

¹⁹ Hussein Shahada al-Hussein, *Ibid.*, pp. 1–2. And Brahimi Hanan, *The Crime of Forgery of Official Administrative Documents of Informational Nature*, PhD Thesis, Criminal Law, University of Mohamed Khider, Biskra, 2015.

3- Electronic Payment Order:

Payment methods have evolved such that creditors can now fulfil their obligations by electronic means. Some countries have established national payment systems, and there are also several international payment systems, most notably the SWIFT network, which is a widely used global system for affecting payments via electronic means. This may be accomplished either by the debtor instructing their bank to settle a debt electronically in favour of the creditor or by instructing their bank to collect a sum from the creditor's account on the basis of prior electronic authorisation²⁰.

The first form, known as credit transfer, occurs when the creditor undertakes the necessary banking procedures to transfer a specified sum to the beneficiary, whether the beneficiary holds an account at the same bank or another bank. This may involve either the advance payment of the amount to the transferring bank or authorising the bank to debit the sum from the creditor's account. The creditor may instruct the bank to do so by means of an electronic message. Upon receiving the instruction, the bank verifies its authenticity and checks other conditions for the transfer, such as the sufficiency of funds, and then executes the transaction.

The second form, referred to as the debit transfer, is carried out by authorising the beneficiary's bank to collect the transfer amount from the debtor or the debtor's bank. In this process, the beneficiary submits the transfer request along with authorisation from the transferor (the debtor) to their bank, instructing the bank to transfer the amount to the beneficiary's account and to debit the corresponding value from the debtor's account²¹.

The transfer order constitutes an electronic document and may be subject to acts of forgery.

Section II: Offences against the Electronic Document

A question arises concerning the legal nature of the electronic document, whether it should be considered a movable object and thus subject to the protection afforded by the provisions that protect movables under the Penal Code,

²⁰ Fayyad Malfi al-Qudah, "The Liability of Banks Resulting from the Use of Computers as a Means of Payment," study presented to the conference held by the College of Sharia and Law, United Arab Emirates University, on "Law, Computers, and the internet," Hilton Al Ain Hotel, 1–5 May 2000, p. 16.

²¹ Hussein Shahada al-Hussein, *Ibid.*, p. 10. And Muhammad Nafi' Rashdan Al-Adwani, The Validity of Electronic Evidence as a Means of Proof in Criminal Matters, Master's Thesis, Public Law, Middle East University, Jordan, 2015.

such as the offences of sabotage, impairment, and destruction²². Alternatively, whether it possesses a distinct nature that excludes it from such protection, the significance of this debate is evident in legal systems that have not yet established criminal provisions addressing harm to electronic data in general or to electronic documents in particular, such as Egyptian law. Suppose that the essence of destruction lies in damaging the object or diminishing its utility by rendering it unusable or inoperative. In that case, this is the case regardless of whether the destruction is total or partial.

A) -Acts affecting the content of the electronic document:

The forms of harm to the content of the electronic document are varied. However, they can generally be categorised into two groups: the first is the forgery of the electronic document, and the second is its destruction.

1-Forgery of the Electronic Document:

There is an important distinction between the electronic document and the paper document in terms of interference with their content. Tampering with and altering the content of the electronic document can occur at any time and may not be detectable or provable. Furthermore, a far greater number of individuals can access and interact with electronic documents than with paper documents. Finally, tampering with the content of an electronic document tends to be easier than tampering with a traditional document. For example, forgery of a signature on a paper document often leaves traces that indicate its occurrence. In contrast, the forgery of an electronic signature composed of a code that identifies the signatory can be subject to manipulation or erasure. Forging such a code may be easier than forging a handwritten signature, and detecting and identifying the perpetrator can, in many cases, prove to be more difficult²³.

The forgery of an electronic document is no less significant than the forgery of a paper document. This significance is apparent in several respects. First, electronic documents have replaced paper documents in many commercial transactions; therefore, tampering with the content of such documents may result in defects in consent, such as mistakes or fraud, leading to numerous disputes and threatening the stability of such transactions.

²² For example, see Article 361 of the Egyptian Penal Code. It is also possible to view Omar Abdul Salam Al-Jabouri, *The Crime of Electronic Forgery in Jordanian Legislation*, Master's Thesis, Public Law, Middle East University, Jordan, 2017.

²³ Gibbs and Mazan, *op.cit.*

Second, reliance on printed versions of original electronic documents and their acceptance in transactions leads to the consequence that any tampering with the content of the electronic document will necessarily affect the identical paper version of that document²⁴. If official and private documents serve to establish legal facts with evidentiary authority and if such documents now exist in electronic form, then altering their content would compromise the probative value of the facts they contain. Finally, the importance of criminalising forgery in electronic documents becomes clear in light of the previously discussed distinction between the concept of the document in traditional forgery offences and that of the electronic document, which makes such criminalisation necessary for the protection of the electronic document.

Comparative legislation differs in its approach to criminalising the forgery of electronic documents. The first approach establishes general provisions criminalising such forgery, thereby extending these provisions to cover all forms of electronic documents, as seen in French and German law. The second approach criminalises only specific forms of electronic document forgery; Egyptian law is an example of such legislation.

a. Criminalisation of Electronic Document Forgery by General Provisions:

French and German legislators criminalise the forgery of electronic documents through general provisions in their penal codes. The following is a study of these two legislations.

According to French law, the criminalisation of forgery in electronic documents can be traced back to a proposal submitted by a member of the French parliament²⁵. On August 5, 1986, amendments aimed to introduce amendments to the offense of forgery in documents provided for in the Penal Code to include the alteration of the truth in electronic data²⁶. However, this proposal was not adopted, and the Senate considered the forgery of electronic documents as an offense distinct from the forgery of traditional documents. Law No. 88-19 of January 5, 1988, was then enacted, which criminalised two forms of conduct: the first is forgery of computer-processed documents of any form where such forgery is

²⁴ Hassan Abd al-Basit Jumai, *Proof of Legal Acts Concluded via the internet*, Dar al-Nahda al-Arabiya, 2000, p. 63 and following.

²⁵ The French deputy Jacques Godfrain, after whom this Legislation was named, had previously submitted a draft law, which was not enacted at the time. Ali Abd al-Qadir al-Qahwaji, p. 39.

²⁶ The approach of this draft law was to adapt traditional criminal offences such as theft, fraud, breach of trust, and forgery to include electronic data. Ali Abd al-Qadir al-Qahwaji, *Ibid.*, p. 39.

prejudicial to others (Article 462--5), and the second is the use of such forged documents (Article 462--6)²⁷.

Upon the replacement of the old French Penal Code with the new Code in 1994, the French legislature repealed the aforementioned articles and adopted the proposal to amend the principal provision on forgery to encompass electronic documents. This was done by amending Article 441-1 of the Penal Code to state: "Forgery is any fraudulent alteration of the truth that is likely to cause harm and is committed by any means, whether in writing or by any other instrument for expressing thought, where the purpose or result of such alteration is to establish a right or a fact with legal consequences."²⁸⁻²⁹ This approach was also adopted by the Electronic Commerce Law of the Grand Duchy of Luxembourg, enacted in June 2000, which amended Article 196 of the Penal Code criminalising forgery by adding electronic writing and signatures to the subject matter of the offense in its traditional form³⁰.

In application of this provision, it is considered forgery to alter the record of a university student's results stored on the university's computer, even if they have not been printed in paper form. The new wording of Article 441-1 mentioned above allows the provision to encompass all forms of expression of thought, including those in electronic form and even those that may be developed in the future, provided that they are relevant to establishing a right or a fact with legal consequences³¹. Moreover, the French legislature, by this provision, did not limit the methods of altering the truth to specific means but instead left the provision unrestricted as to how forgery may occur.

According to German law, Article 268 of the Penal Code, which appears under the section on forgery, criminalises the "forgery of computer-processed records." Paragraph one of this article, in its first clause, criminalises the act of "anyone who, by means of deception, creates a fictitious computer-processed record or

²⁷ Omar al-Faruq al-Husseini, *Ibid.*, p. 86.

²⁸ Constitue un faux toute altération frauduleuse de la vérité de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques.

²⁹ Marco, Estelle De, *Le Droit Pénal Applicable sur internet*, Mémoire de D.E.A. Informatique et Droit, under the supervision of Professor Michel Vivant, Université de l'Information Juridique, 1998, no. 12. <http://www.juriscom.net/universite/memoire6/penal/html>.

³⁰ Medhat Abdel Halim Ramadan, *Criminal Protection of Electronic Commerce*, Dar Al-Nahda Al-Arabia, Cairo, 2001, p. 72.

³¹ Medhat Abdel Halim Ramadan, *op.cit.*, p. 30.

alters the truth in such a record.” The second clause penalises the use of such a record³².

The German legislature equated the creation of a fictitious electronic record with the act of altering the result produced by such a record, using the perpetrator, who caused a disruptive effect on the operation of the record³³. The German legislature has also criminalised certain specific forms of offenses related to the electronic document after establishing the general framework for criminalising such documents in Article 268 mentioned above. Among the most important of these is the forgery of data, which has evidentiary value³⁴ (Article 269 of the Penal Code).

b-Egyptian Law:

Egyptian legislators criminalised the forgery of electronic records related to civil status. As previously mentioned, the Egyptian legislature has, in Civil Status Law No. 143 of 1994, equated paper and electronic records in the application of its provisions. The legislature considers data recorded on computers at civil status information centres to be data contained in official documents. Article 72 of the aforementioned law provides that “for the purposes of applying the provisions of this law and the Penal Code, data recorded on computers and their accessories at civil status information centres and their associated issuance stations, used for issuing documents and identity cards, are considered data contained in official documents. If forgery occurs in the above documents or any other official documents, the penalty shall be temporary hard labor or imprisonment for a period not less than five years”³⁵.

³² “Falsification of Technical Records.

1. Whoever, with the intent to deceive in legal transactions, (1) produces a false technical record or falsifies a technical record, or
2. uses a false or falsified technical record,”
3. — *Criminal Code, Special Section*, 2002.
4. <http://www.gesetze-xxl.de/gesetze/stgb.htm>.

³³ “... (3) The creation of a false technical record is equivalent to when the perpetrator, through disruptive interference with the recording process, influences the result of the record.”
—*Criminal Code, Special Section*, 2002.

<http://www.gesetze-xxl.de/gesetze/stgb.htm>.

³⁴ 629 “Falsification of Evidence-Relevant Data”—*Criminal Code, Special Section*, 2002.

<http://www.gesetze-xxl.de/gesetze/stgb.htm>.

³⁵ The first paragraph of this article stipulates that “For the purposes of applying the provisions of this law and the Penal Code, the data recorded by computers and their accessories at the Civil Status Information Centers and their dedicated issuance stations used in issuing documents and identity cards shall be regarded as data contained in official documents.”

Article 74 of the aforementioned Civil Status Law provides that, without prejudice to any harsher penalty prescribed by the Penal Code or other laws, anyone who accesses, attempts to access, obtains, or attempts to obtain the data or information contained in the records, computers, or attached storage media, or alters such data by addition, deletion, cancellation, destruction, or otherwise interferes with it in any way, or disseminates or discloses it in cases other than those specified by law and, according to the procedures prescribed therein, shall be punished by imprisonment for a period not exceeding six months, a fine not exceeding five hundred Egyptian pounds, or either of these penalties. If the offense concerns aggregated data, information, or statistics, the penalty should be imprisonment.

2- Destruction of the Electronic Document:

There is no direct criminalisation of the destruction of the electronic document; rather, protection for this document from acts constituting its destruction can be achieved indirectly in two ways. First, acts of destruction may be directed at the operating system that contains the electronic document, thereby resulting in the destruction of the document as a consequence. Second, destruction may be directed at the data contained within the document, in which case the protection generally applies to electronic data but extends by implication to the electronic document in its precise sense.

a. Destruction of Data Processing Systems:

The French legislature criminalised the offence of disrupting or turning off the operation of a data processing system (Article 323--2). This offense may be committed in different ways: the means of disruption may be physical, such as acts of violence, sabotage, or severing communication means affecting the devices and causing their malfunction, or it may be nonphysical, such as introducing a virus into the operating system.³⁶ This is equivalent to sabotaging if the perpetrator corrupts the stored information in such a way that it becomes unusable. Impairment does not cause the devices to cease functioning entirely but instead causes them to operate abnormally, thereby affecting their performance. For example, the offense is established if perpetrators send many electronic messages to a particular site, causing disruption and interruption of its operation.³⁷ Notably, turning off a computer storing electronic documents and records does not fall under the concepts of sabotage or impairment as defined in Article 323-2

³⁶ Ali Abdelkader Al-Qahwaji, *Previous Reference*, p. 56. here, the issue of Case C-746-18, the Court of Justice of the European Union ruled on the need to respect the rights of individuals when collecting such information.

³⁷ Jamil Abdelbaki Al-Saghir, *The internet and Criminal Law*, p. 63.

of the French Penal Code. Instead, it is considered a form of material destruction punishable under Article 322-1 of the French Penal Code.

The German legislature has also criminalised, in Article 270 of the Penal Code, any person who, using deception, causes an effect that disrupts the operation of an electronic data system.³⁸ Notably, in this case, destruction does not affect the data contained in the data processing system but rather affects the system itself. Thus, the protection provided here for the document is, in reality, indirect, as the legislator's primary aim is not to protect the document itself but rather to safeguard the data processing systems and their functioning, and the protection of the document follows as a consequence.

b. Interference with Data Contained in the Data Processing System:

Interference with the data of a processing system, whether by inputting or erasing data, does not necessarily constitute a form of forgery of such data; rather, the effect of such interference is the destruction of the system and its inability to perform its function. An example is the deletion of specific operating commands, which results in system failure. Therefore, the proper legal characterisation of this act is that it falls under the offense of destruction. The French legislature has provided punishment for anyone who "fraudulently inputs data into a data processing system, or fraudulently erases or modifies the data contained in the system" (Article 323--3)³⁹. This provision does not protect the system in a physical sense but instead protects the data contained within the system against criminal activity.⁴⁰ This offense comprises three forms: inputting, erasing, and modifying. All three forms do not need to be present; the offense is established if any one of them occurs. The subject matter of the offense is electronically processed information, which means that it encompasses all the data contained in electronic documents. The act of inputting refers to the addition of new data to the system, regardless of whether existing data are supplemented or the area of addition was previously empty⁴¹.

The offense of forgery requires an alteration of the truth and presupposes, among its elements, that such alteration causes harm. In contrast, the offense of

³⁸ "Deception in Legal Transactions Involving Data Processing:

Deception in legal transactions is equivalent to the intentional manipulation of data processing in legal transactions."—*Criminal Code, Special Section*, 2002. <http://www.gestze-xxl.de/gesetze/stgb.htm>.

³⁹ "The act of fraudulently introducing data into an automated data processing system, or fraudulently deleting or modifying data contained therein, is punishable by three years' imprisonment and a fine of 300,000 francs."

⁴⁰ Medhat Abdel Halim Ramadan, *Criminal Protection of Electronic Commerce*, p. 55.

⁴¹ Ali Abdelkader Al-Qahwaji, *Previous Reference*, p. 59.

interference with data, as stipulated in Article 323-3, is constituted by the mere act of inputting, modifying, or erasing, even if no harm results, and even if there is no alteration of the truth in the strict sense. The French legislature has regarded this offence as one of endangerment⁴².

This offense is intentional, as is evident from the legislator's requirement that it be committed fraudulently; this means that the requisite intent is absent if the perpetrator deletes or modifies the system's data by mistake.

c. Criminalisation of Preparatory Acts:

The French legislature has provided for the punishment of participation in a group or agreement among several persons to prepare for the commission of one or more crimes of disrupting, impairing, or interfering with data in a data processing system by carrying out one or more material acts (Article 323--4). This provision departs from general criminal law principles by criminalising preparatory acts. The rationale for this departure is the legislator's desire to ensure preventative protection for information systems and electronic data. The French legislature prescribes for such activity the same penalty as for the principal offence. Notably, if the crime prepared for is committed and the perpetrators participate in its commission, this constitutes a material concurrence of offenses that cannot be separated. In such cases, a causal link must exist between the preparatory acts and the offence committed.

The French legislature also prescribes that, for the attempt to commit the offence, the same penalty applies to the principal offence (Article 323--7).

d. Liability of Legal Persons:

The French legislature has permitted the prosecution of legal persons for committing the two forms of destruction provided in Articles 323--2 and 323--3 of the Penal Code by the general provisions establishing the criminal liability of such persons (Article 323--6). A legal person may be held liable for these offences as a principal perpetrator, an accomplice, or an accessory and may be liable for either the completed offence or the attempt. However, for such liability to be established, it must be proven that the offense was committed by one of the members or representatives of the legal person and that it was committed in the name or on behalf of the legal person (Article 121--2 of the French Penal Code). The establishment of the liability of the legal person does not preclude the

⁴² Merco, op. cit., no. 113.

criminal liability of natural persons, whether as perpetrators, accomplices, or accessories in the same offense (Article 121--2, paragraph 3, of the Penal Code).⁴³

B)- Acts affecting the confidence of the document

Various forms of acts compromise the confidentiality of the document, as stipulated by comparative legislation. Such acts may take the form of unauthorised access to electronic records or the copying or printing of the information and data contained in the document.⁴⁴ The following will outline the approach of comparative legislations in addressing these acts, followed by a discussion of the common elements of these offences.

1-Analysis of the Approach of Certain Comparative Legislations to Offences Affecting the Confidentiality of the Electronic Document:

a. Egyptian Law:

Egyptian legislators have not enacted provisions specifically criminalising unauthorised access or interference with stored electronic data. Instead, the legislature has included, in various separate articles, certain forms of such protection⁴⁵. Among the most important provisions is that set out in the previously

⁴³ Ali Abdelkader Al-Qahwaji, *Previous Reference*, p. 47.

⁴⁴ "Are Your Financial Institution's Computer Systems Impenetrable," *op.cit.*

⁴⁵ Among the other examples stipulated by the Egyptian legislator is what is provided by Law No. 35 of 1960, as amended by Law No. 28 of 1982, concerning statistics and census, regarding penalties for breaching the confidentiality of statistical or individual data. Article 3 of this law states that individual data related to any census or survey is confidential and may not be disclosed to any person or public or private entity, nor may it be used for purposes other than statistical ones, or published about individuals except by written permission from the concerned parties. Article 4 of the law imposes a stricter penalty in cases of breach of the confidentiality of statistical data or disclosure of individual data or any industrial, commercial, or other trade secrets learned through work in statistics or census. The law also increases the penalty for obtaining, or attempting to obtain, confidential data or information about statistics or census by fraud, threat, or deception by any means. It should be noted that these individual data concern the number of family members and are related to statistics and census, not to the private lives of individuals, it was issued as an amendment to this law the Law No. 15 of 2004 regulating electronic signatures and establishing the Egyptian Information Technology Industry Development Agency, Official Gazette of the Arab Republic of Egypt, Issue No. 17 issued on 4/22/2004 ;In addition to this , it was published later Executive Regulations of the Electronic Signature Law, Decision of the Minister of Communications and Information Technology No. 109 of 2005 dated 5/15/2005 published in the Egyptian Gazette No. 115

—Tarek Sorour, no. 39, pp. 70–96.

mentioned Civil Status Law No. 143 of 1994, which stipulates that data and information related to civil status contained in “registers, records, computers, or attached storage media” are confidential and may not be accessed or disclosed except in the cases specified by law (Article 13, paragraph one).

The legislature further considers that data, information, or aggregated statistics contained in the aforementioned electronic records and registers constitute a “national secret” that may not be accessed or published except for national or scientific purposes and with written permission from the director of the Civil Status Authority or their delegate (Article 13, paragraph two).

An analysis of these two provisions suggests that the legislator's intention was not to protect electronic data as such but rather to protect secrecy itself. However, by conferring the attribute of secrecy to all stored data, the legislature, in our view, has created a form of protection with a mixed character.

Article 74 of the aforementioned Civil Status Law provides that, without prejudice to any more severe penalty stipulated in the Penal Code or other laws, anyone who accesses, attempts to access, obtains, or attempts to obtain the data or information contained in the records, computers, or attached storage media... or disseminates or discloses them in cases other than those specified by law and, according to the procedures prescribed therein, shall be punished by imprisonment for a period not exceeding six months, a fine not exceeding five hundred pounds, or either of these penalties. If the offense concerns aggregated data, information, or statistics, the penalty should be imprisonment.

Article 76 of the same law provides that anyone who breaches or attempts to breach the confidentiality of data, information, or aggregated statistics in any manner shall be punished by temporary hard labor. If the offense is committed in time of war, the penalty should be permanent hard labor.

b. French law:

The French legislature, under Article 323-1 of the Penal Code, punishes the mere act of fraudulently accessing all or part of an information system or unlawfully maintaining a connection with it⁴⁶. The penalty is increased if the perpetrator's

⁴⁶ “The act of fraudulently accessing or remaining in all or part of an automated data processing system is punishable by one year's imprisonment and a fine of 10,000 francs.”

activity results in the deletion or alteration of data contained in the system or in the modification of the operation of that system⁴⁷.

The French legislature has increased the penalty if unauthorised access to, or unlawful presence in, the system, or the deletion or modification of data contained within it, results in the system being rendered inoperative. For this aggravating circumstance to apply, there must be a causal link between the act of unauthorised access or presence in the system and the deletion or modification of data or the disruption of the system's operation. However, if the deletion or modification is due to other causes, such as force majeure or unforeseen incidents, the causal connection is considered absent, and the perpetrator is not liable for the aggravated circumstance in this case⁴⁸. The French legislature also protects the confidentiality of the electronic document through Articles 226--16--226--24 of the Penal Code, which criminalises interference with the confidentiality of stored information. Previously, this protection was provided by Law No. 87--17 of January 6, 1978, on information technology, files, and civil liberties⁴⁹.

This law criminalised the use of information recorded on computers for purposes other than those for which it was intended and criminalised the disclosure of such information. Law No. 19 of 1988 further criminalised the deletion or alteration, whether in whole or in part, of electronic data⁵⁰. The French legislature repealed these two provisions and incorporated their content into the current Penal Code enacted in 1994 and then added further offences, including obtaining information relating to a person by fraudulent means or entering such information by the same means despite that person's legitimate objection (Article 226--18) and entering information into computer memory concerning a person's racial origins, political, philosophical, or religious views, trade union affiliations, or behaviour (Article 226--19).

⁴⁷ "When this results in either the deletion or modification of data contained in the system, or an alteration of the operation of that system, the penalty is" and it was issued in this regard the Law No. 2000-230 of 13_3_2000 adapting the law of evidence to information technologies and relating to electronic signatures, it was also published later implementing decree no. 2016-1673 of 5-12-2016 relating to the reliability of copies

⁴⁸ Abdelkader Al-Qahwaji, *Previous Reference*, p. 54.

⁴⁹ *Law on Information Technology, Files, and Civil Liberties*.

⁵⁰ Huda Qashqoush, *Intentional Damage to Computer Programs and Data*, pp. 11--12.

2- Common Elements in Offences Affecting the Confidentiality of the Electronic Document:

Several common elements can be summarised as follows:

a. The Perpetrator:

The perpetrator in unauthorised access offenses is any person who connects to a protected computer without authorisation and does not have a reasonable expectation that their act would not infringe upon the right to privacy in the case of communication to or from a protected computer. The offense does not require any special status on the part of the perpetrator; it may be committed by any person, whether or not they have a professional relationship with electronic processing systems⁵¹. Excluded from this definition is anyone who has a contractual relationship with the owner or manager of a protected computer that authorises them to access that computer, whether wholly or partially⁵².

b. The Act of Unauthorised Access:

The act of access itself constitutes the offense. Comparative legislation does not specify what is meant by "access" or how access is gained; therefore, the offense may be committed by any means whatsoever. Access may occur by using special devices to break the code of the database or by using the correct code belonging to another authorised person. The offense presupposes that access to the data system is not open to the public but is restricted to a limited number of persons or entities⁵³.

⁵¹ Ali Abdelkader Al-Qahwaji, *Previous Reference*, p. 51.

⁵² See, in this regard, Article 2510 of the United States Federal Code: 'Computer trespasser'

A) means a person who accesses a protected computer without authorisation and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and

B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer." And here, the issue of Case C-162-16, the Court of Justice of the European Union also underlined the importance of the authenticity of electronic signatures in commercial transactions, specifying that authentication systems must be sufficiently robust to prevent forgery and Google case -Spain sl -Marche 6-Eur-lex 62012cj 0131-FR, V Spanish data protection agency regarding the processing of personal data.

⁵³ Medhat Abdel Halim Ramadan, *Criminal Protection of Electronic Commerce*, p. 50.

Unlawful presence may also occur after initially legitimate access, such as when a person exceeds the authorised time frame or the permitted purpose for accessing the information system⁵⁴.

One opinion in legal scholarship holds that the offense of unauthorised access is instantaneous, whereas unlawful presence in the system is continuous⁵⁵. In our view, this opinion is open to question, as the key factor in determining the nature of the offence is whether its material element is capable of continuation. There is no doubt that access to electronic data storage systems may persist for some time, during which the material element of the offense continues to be committed, and the offense does not cease until the perpetrator ends their unauthorised access. In our estimation, it should also be noted that the dual criminalisation under the aforementioned French provision, which penalises both access and presence, cannot be relied upon to distinguish the nature of the offence, as this duality is intended to address cases where a person who initially authorised access subsequently exceeds the permitted scope an issue unrelated to the intrinsic nature of the offense.

The offense is not established by mere unauthorised access; rather, such access must be fraudulent. This means that acts of inadvertence or error do not amount to fraudulent access. Conversely, access that is not accompanied by deceit is not regarded as unauthorised: if the system permits access without any deceit or fraud, the act loses its unlawful character, even if the permission is the result of an operational error, as no blame attaches to the individual in such circumstances.

Access may be lawful in itself, whereas continued presence in the system becomes unlawful, in which case the conduct is characterised by deceit. Access may also be open to the public but restricted to specific databases and not to system files, making it imperative to access these areas⁵⁶.

c. Resorting to Deceptive Methods:

Unauthorised access must be achieved by deceptive means, and the term “deceptive methods” is interpreted broadly. It does not require the perpetrator to use fraudulent devices to gain access; it is sufficient that access is obtained without authorisation, provided that the requisite criminal intent is present. The French judiciary has interpreted the expression “fraudulent access” as stipulated in Article 323-1 of the aforementioned Penal Code to include all unlawful means

⁵⁴ Jamil Abdelbaki Al-Saghir, *Criminal Law and Modern Technology, Book One: Crimes Arising from the Use of Computers*, (1992), p. 150.

⁵⁵ Medhat Abdel Halim Ramadan, *Criminal Protection of Electronic Commerce*, p. 51.

⁵⁶ Jamil Abdelbaki Al-Saghir, *Criminal Law and Modern Technology*, p. 151.

by which a perpetrator gains entry into an automated information processing system⁵⁷. This occurs when the right to access electronic data and records is limited to certain persons or entities, excluding the perpetrator. Sometimes, such access may be generally permitted to the public but is subject to specific conditions. In these cases, the right to access the data is not lawful unless these conditions are fulfilled. Examples of such conditions include the requirement to pay specific fees to access a particular website and download files from it⁵⁸.

Failure to satisfy these conditions renders electronic access unlawful. Deceit is present if the perpetrator manages to break the access code; it is also present if the perpetrator uses the legitimate password or code for access when not authorised to do so.

d. Criminal Intent:

Offences of accessing or remaining in a data processing system are intentional offences; the perpetrator must be aware that they are accessing a site they are not permitted to enter and must intend to do so. Thus, the offense does not exist if the access or presence was the result of an error. Accordingly, criminal intent is absent if it is shown that the perpetrator accessed the database by chance or due to a mistake, and their conduct does not indicate the existence of intent. Another example is when access to the system is based on a subscription and the person had previously accessed the system lawfully, but the subscription expired, and they were unaware of this fact. Evidence of intent includes the use of deceptive methods to gain access to or remain in the system, such as stealing an access card or breaking a code when entry requires a specific code or card⁵⁹.

Once criminal intent is established, the motives behind the perpetrator's act are irrelevant. It makes no difference whether the access was driven by curiosity, a desire to prove the ability to overcome system restrictions,⁶⁰ to benefit from the information and data contained in electronic records and databases, or to commit any other unlawful act.

⁵⁷ Paris, April 5, 1994, D. 1994. I.R., p. 130.

⁵⁸ "Hacker into United States Courts' Information System Pleads Guilty," 2002, www.cybercrime.gov.

⁵⁹ Jamil Abdelbaki Al-Saghir, *Criminal Law and Modern Technology*, p. 151.

⁶⁰ Ashraf Tawfiq Shams El-Din, *Criminal Protection of the Electronic Document: A Comparative Study*, p. 125.

Conclusion

The comparative legislation examined in this study has not fully succeeded in ensuring adequate criminal protection for electronic documents. Unlike the prevailing approach to the traditional concept of the written instrument, these legislations have not established clear parameters for the electronic document. Some have limited themselves to enacting laws on electronic signatures, others have included electronic records, and a number of these legislations have expanded the definition of such records in a way that excludes certain forms from the precise meaning of the document. Some comparative legislations have conflated the concept of the electronic document with that of electronic data and information, despite the important distinction between them; indeed, some have even confused the document with data processing systems and computer operations.

Accordingly, there is an urgent need to enact legislation that establishes the foundations of an integrated theory for the electronic document, addressing its composition, conditions for validity, evidentiary value, principal applications, and the general framework for technical rules to be used by those dealing with electronic documents. The legislature should take into account, in this law, the traditional meaning of the written instrument and the implications of adopting the concept of the electronic document for the application of existing legislation. The law should define the forms of interference with the electronic document, as established in this study, and criminalisation of acts affecting the electronic document should be preceded by the adoption of preventive policies designed to establish safeguards to protect against such interference before it occurs.