Law and Political Science Journal | *Volume*:11/ N°: 02. (2025), p759-768

*Accepted*19/12/2025 *Received* 20/12/2024

Crimes Against Electronic Signatures and Their International Confrontation

Derbale Mohammed

University Center Of Naama (Algeria)

darbel@cuniv-naama.dz

Abstract:

Crimes against electronic signatures have become crimes of the modern age. Tackling such crimes is impossible without international cooperation and the establishment of treaties and agreements at all levels of law enforcement. No single country can eliminate these crimes independently. The Algerian legislator has introduced legal protections for the confidentiality of signature data through the Electronic Signature and Certification Law of 2015, addressing both the material and moral elements of these offenses. Algeria has also ratified numerous agreements in this field, including the Arab Convention on Combating Cybercrimes. These efforts aim to enhance protection mechanisms via the internet, grant electronic signatures direct legal recognition, and improve internet service quality to achieve effective results.

Keywords: *Crime, Certification, Electronic, International Cooperation.*

ملخص:

إن جرائم الإعتداء على التوقيع على الإلكتروني صـــارت من جرائم العصـــر لذلك بغير التعاون الدولي وعقد العديد من الاتفاقيات الدولية والمعاهدات على الصـعيد الشـرطي في جميع مراحل وقوع الجريمة لأن من المسـتحيل على أي دولة بمفردها القضـاء على جرائم الاعتداء على هذا التوقيع وقد اوجد المشـرع الجزائري حماية جزائية من أجل سرية بيانات التوقيع في قانون التوقيع والتصديق الالكتروني لسنة 2015 وذلك حماية لهذا التوقيع بقيام الركنين المادي والمعنوي لهذه الجريمة ولقد صـدقت الجزائر على الكثير من الاتفاقيات في هذا المجال منها الاتفاقية العربية لمكافحة جرائم الانترنت وذلك بتفعيل أسـاليب الحماية التي تستعمل من خلال شبكة الانترنت واصباغ الصفة القانونية بشكل مباشر على التوقيع الالكتروني والعمل على تحسين جودة خدمات الانترنت لأجل الوصول إلى نتائج مرضية.

الكلمات المفتاحية:الجريمة، التصديق، الالكتروني، التعاون الدولي.

1. INTRODUCTION

The modern world is increasingly saturated with highly advanced and precise communication networks, enabling the rapid transfer of data and information between both nearby and distant regions. These networks, along with the data transmitted and stored in high-speed devices, have caused significant damage to some countries, companies, and individuals due to the technological advancements of recent decades. These developments have influenced the evolution and dynamics of crime, making international cooperation a critical necessity to prevent cybercrimes and implement effective measures to address them. Given the global and transnational nature of crimes against electronic signatures, their combat requires the concerted efforts of the international community. To address this issue, the descriptive-analytical method is employed, focusing on two main points: first, understanding the concept of cybercrime and identifying the cybercriminal, and second, examining crimes against electronic signatures within this framework and their international confrontation.

Modern information and communication technologies have brought about profound changes in public life, as governments strive to keep pace with rapid and ongoing global advancements using all available methods, data, and tools. These technological developments have reshaped public expectations, whether in terms of individuals' desire to obtain electronic signatures or the efforts of institutions and entities responsible for providing such services.

Significance of the Study: The significance of this study lies in its presentation of a unique model for understanding the concept of the electronic signature and its legal implications.

Objectives of the Study: This study aims to assess the capabilities and preparedness for the implementation of an electronic signature system.

Methodology: The study relies on a comparative, analytical, and descriptive methodology.

2. The Nature of Cybercrime

Cybercrime is a newly emerging criminal phenomenon, linked to computer technology and modern innovations, which have become essential due to the digital transformation across institutions. The international community has advocated for the incorporation of such technologies into legal frameworks to facilitate transactions between institutions and individuals, saving time. Consequently, this phenomenon has become shrouded in ambiguity, as computer technology is constantly evolving, making it difficult to define the forms and types of computer crimes. Additionally, cybercrimes are transnational, crossing the borders of all nations. Therefore, international and security cooperation between authorities is necessary to curb these crimes in the country where they originate[1]. No country can single-handedly eradicate cybercrimes, and international collaboration is essential, especially given the rapid advancements in communications and information technology.

2.1The Concept of Cybercrime

The introduction of computer technology into both individual and organizational life has directly contributed to altering traditional behavioral patterns. This development has opened the door to new behaviors that involve negative actions, such as crimes committed using computers or information-related crimes. As a result, it has become necessary to ensure broader criminal protection for information stored in computers, particularly to prevent

hacking, surpassing the protection given to information contained in paper files. This is due to the vulnerability of the former and its significance[2].

The concept of cybercrime remains relatively new due to its association with modern technology, especially the internet. It is considered a unique crime, committed through the use of computers[3].The term has been described in various ways, such as computer and internet crimes, digital crimes, and cybercrimes. It is also referred to as "clean crimes" because they are often committed with little physical evidence. These crimes have been approached from two perspectives.

2.1.1The Narrow Definition of Cybercrime

Proponents of this perspective define cybercrime as: any unlawful act where knowledge of computer technology is crucial for its commission, as well as for its investigation and prosecution[4]. This definition emphasizes the necessity of comprehensive knowledge of computer systems and technologies, not only for committing the crime but also for investigating and prosecuting it. This narrow definition restricts cybercrime to cases where criminals possess a significant understanding of technology, as well as investigators, such as police officers, judges, and others involved in prosecution and investigation.

The legal scholar “Klaus Tideman” defines cybercrime as all forms of unlawful behavior committed using computers[5].According to this perspective, a crime is considered a cybercrime as long as the computer or any other technological means is used in its commission, and the perpetrator must possess knowledge and expertise in this field.

2.1.2The Broad Definition of Cybercrime

The scholars of the broad approach criticized the narrow definition of cybercrime, prompted some legal scholars to propose a more inclusive, and expanded definition. Legal scholars (Creado and Michel) defined computer crime as the use of a computer as a tool to commit crimes, in addition to cases involving unauthorized access to the victim’s computer or data. Furthermore, computer crimes extend to physical attacks, such as credit card fraud, and violations involving machines, including breaches of automated payment systems, such as electronic funds transfer checks.

2.1.3The Position of the French Legislator on Cybercrime

The French legislator has not defined cybercrime explicitly. Instead, it criminalized certain acts contributing to its occurrence under specific legal provisions. These provisions are found in Chapter Three of the French Penal Code, titled "Offenses Against Data Processing Systems," which outlines cybercrime offenses[6].

2.1.4The Position of the Algerian Legislator

In response to the growing number of crimes in the field of information technology, the Algerian legislator included provisions related to cybercrimes in Law No. 09/04, which

outlines specific rules for preventing and combating crimes related to information and communication technology. The Algerian legislator defined cybercrime in Article 2 as offenses against automated data processing systems, as specified in the Penal Code, and any crime that is facilitated by the use of information technology systems and computers[7].

2.2 The Cybercriminal

The term "cybercriminal" refers to the main perpetrator in an electronic crime. This individual possesses exceptional intelligence and a high level of knowledge in information technology as a basic requirement. The cybercriminal uses specific tools and devices to commit these crimes, and they can be either a natural person or a legal entity, such as an organization aiming to harm a competitor. The act may be committed either in good faith or bad faith, with the cybercriminal using a device to engage in unlawful behavior, such as attacking websites or damaging data and information on another's device[8].

2.2.1 Definition of the Cybercriminal

In the field of electronic information, the cybercriminal is often referred to as a "hacker." A hacker is an individual who engages in destructive and illegal activities on the internet. The hacker is sometimes also called a "digital criminal," and there is no direct translation for the term "hacker" in Arabic. Hackers have the ability to store information in numerical form and use it when needed to commit a crime[9].There are both small-scale and large-scale cybercriminals in the field of electronic crime, and they are treated equally. Unlike traditional criminal groups, their activities may become more dangerous if they adapt socially and possess a criminal personality[10].

Cybercrime began in the 1990s when the first creative criminals emerged with the advent of technology. Over time, cybercriminals, particularly hackers, became more specialized in areas such as data destruction, extortion, and sabotage. Cybercriminals do not hesitate to commit their crimes under any circumstances. Cybercriminals can be categorized into two groups: one group may belong to an organized criminal network focused on obtaining sensitive and dangerous information[11].These individuals are skilled in computer technology and often represent the core of organized crime. The cybercriminal’s profile differs significantly from that of other criminals in terms of intelligence, educational qualifications, and proficiency in information technology. Cybercriminals acquire extensive knowledge and expertise through repeated practice with computers. What starts as a hobby can evolve into criminal activity. Cybercriminals can be classified into several categories based on the severity of their crimes[12].

1. Pranksters: A group that harms others merely for fun.
2. Hackers: Individuals who break into security systems of computers to prove their expertise in hacking. This group represents one of the most dangerous categories of cybercriminals, as they have carried out high-level intrusions against governments and countries[13],earning them the title of cybercriminals.

2.2.2 Characteristics of the Cybercriminal

The cybercriminal differs from other criminals in several important ways:

1. Professional Criminal: The cybercriminal is highly skilled and efficient in using computers and technology.

2. Intelligent Criminal: Intelligence is the primary characteristic of the cybercriminal. This individual is well-versed in computer technologies and can manipulate them to their advantage. The criminal activity requires significant intelligence, skill, and experience[14].

3. Non-Violent Criminal: The crimes committed by cybercriminals are based on trickery rather than physical violence. They do not use force to commit their crimes but rely on their exceptional intelligence. Since cybercriminals typically do not deal directly with individuals, there is no need for physical violence[15].

4. Socially Adapted Criminal: The cybercriminal is socially adapted due to their sharp intelligence. The more they adapt socially, the greater the criminal risk they pose.

5. Tendency to Commit Crimes: The cybercriminal exhibits a criminal inclination associated with their personal interests, especially their deep fascination with computer knowledge and access.

3.Crimes Against Electronic Signatures

Crimes targeting electronic signatures, along with the associated security and legal assistance, have gained significant importance in fostering trust in transactions and paper-based documents. Given the frequent use of electronic signatures, it became necessary to legally regulate them, especially for contracts concluded remotely. Security and legal assistance in crimes against electronic signatures can take several forms, including data preservation. Investigating authorities in the requested state are responsible for preserving electronic document data[16]because perpetrators of electronic signature crimes can only be pursued through international cooperation. This allows for identifying the criminal and collecting vital evidence. It may also become clear to the requested state that the transmitted data, within its territory, shows that the data originated from a service provider in a third country. There are many international treaties and regional agreements under international law to facilitate this cooperation[17].

3.1 Security and Legal Assistance Between States

The electronic signature plays a crucial role in financial transactions between individuals and legal entities across all international legal systems. The Algerian legislator aligned with international laws by issuing a legal text in 2015, identified as Law No. 15/04, dated February 2015, which establishes the general rules related to electronic signatures and certification[18].

However, attacks on electronic signatures are among the fastest-growing forms of criminal activity. One of the important measures in managing judicial assistance in crimes involving attacks on electronic signatures is for investigative teams to access data located outside their

territory or received through computers within their jurisdiction. Additionally, there are various types of security measures associated with information, which are fundamental to information systems, ensuring the protection of data and its storage in technical and legal terms.

3.1.1 Mutual Assistance in Intercepting Electronic Content Data

The process of intercepting electronic document data, which involves breaching confidentiality and privacy, is particularly sensitive when intercepting communications through wired or wireless means. Legal protections exist to safeguard the private lives of individuals, requiring judicial authorization before intercepting communications. Law enforcement officers conducting such operations are obliged to maintain professional secrecy under penalty of law, as stipulated in the penal code, where violating professional confidentiality is punishable[19]. Judicial and legal assistance in crimes against electronic signatures may take various forms, such as preserving data and facilitating easy access by hackers. Article 30 of the "Budapest Convention" specifies the circumstances under which data may be withheld, stating that authorities in the requested state are not required to disclose the transmitted data for the same reasons as withholding data about stored information[20].

3.1.2 Preservation of Stored Data in Computer Systems

The urgent preservation of data stored within computer systems is a critical task. Any state can request the preservation of data stored on computer systems located within another country. Due to the potential for breaching confidentiality when intercepting data, strict regulations govern the preservation of such data. Every state must establish a continuously accessible public contact point to facilitate immediate assistance for investigations and lawsuits[21]. All such processes are conducted via secure protocols, converting information into clear signals using specialized software. States must ensure the confidentiality of encrypted data and protect the privacy of communications exchanged between contracting parties. Consequently, every effort must be made to ensure the confidentiality of data used to create electronic signatures by all available means[22].

3.1.3 The General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a European Union law that governs the collection and use of personal data. It is a modern legislative framework for data protection that officially entered into force in May 2018. Although the GDPR is a regulation issued by the European Union, its impact extends beyond EU borders, as many non-European entities that rely on digital advertising services and electronic signatures are also subject to its provisions.

The GDPR is built upon widely recognized principles of privacy and data protection. It reinforces existing requirements for confidentiality and security, enhances technical safeguards, and regulates the mechanisms for cross-border data flows. One of its key functions is the protection of electronic signatures from unauthorized access and cyber breaches.

This regulatory approach is also in line with the principles outlined in the UNCITRAL Model Law on Electronic Signatures, as referenced in the 2006 revision of the UNCITRAL Model Law on International Commercial Arbitration.

3.1.4Electronic Certification

As the risks of electronic piracy and misuse of technology continue to grow, it has become essential to implement means to verify the identities of contracting parties and confirm their intentions, involving a neutral and trusted third party. This third party plays a mediating role in authenticating electronic transactions by issuing an electronic certificate[23]. The Algerian legislator introduced this term as related to documentation services, based on the UNISTAR law on electronic signatures. It defines an electronic certification service provider as a natural or legal person who issues electronic certificates and provides other services in the field of electronic certification. Electronic signatures are protected from potential risks because these transactions occur through electronic mediums and virtual contracting bodies[24].

3.2 Judicial Authorities Competent to Prosecute Electronic Signature Crimes

The determination of the competent authority to prosecute crimes related to electronic signatures depends on whether the crime is transnational, involving individuals who are either Algerian or from other nationalities. Crimes committed by Algerians within the national territory do not raise issues concerning territorial and jurisdictional competence. However, due to the global nature of these crimes, there may be overlap between Algerian and foreign judicial jurisdictions. Legal assistance may involve the interception of data related to electronic content, the exchange of expertise, technical assistance, and the rapid disclosure of transmitted and stored data within devices. Since the search concludes with the identification of the location and place of the targeted data, processing the data to make it visible and extracting it from the device as printed documents does not constitute a search for criminal evidence but rather access to this evidence in order to secure it from electronic devices[25].

3.2.1 Mechanism for Creating Electronic Signatures

To create an electronic signature, a secure mechanism is required to protect data, which necessitates the use of a secret key and other elements or codes used in the creation process, in addition to the signer. Article 10 of Law No. 15/04 of 2015 requires that the mechanism for creating an electronic signature be secure. Article 11 of the same law stipulates that a secure mechanism for creating an electronic signature must meet certain requirements[26], the most important of which is ensuring the confidentiality of the data used to create the signature. The legitimate signer must protect this data in a trustworthy manner, and it should not be altered after the signature has been applied. The Algerian legislator has emphasized the confidentiality of the data to protect it from breaches and the risk of forgery.

3.2.2 Cyber Police in Electronic Signature Crimes

The cyber police rely on a massive central database that records all incidents and criminal activities, especially those related to attacks on electronic signatures. France and other Western countries were pioneers in establishing such specialized agencies, which focus on tracking down criminals and countering these types of crimes.

In this context, Algeria established a Central Office for Combating Technology-Related Crime, created by Ministerial Decree No. 2000-405 under the central police judicial administration of the Ministry of the Interior. Its primary mission is to pursue criminals involved in cybercrime, including examining, seizing, and searching devices, with support from various agencies[27]. On the international level, the most important body responsible for this role is INTERPOL, which identifies crimes related to electronic signature attacks. INTERPOL can coordinate field resources in ongoing investigations related to information technology. To facilitate international cooperation, INTERPOL organizes an international conference every two years on cybercrime, including crimes involving attacks on electronic signatures. This conference collects, stores, analyzes, and shares information on such crimes with all member countries[28].

3.2.3 Criminal Protection of Electronic Signatures

The evidentiary value of outputs obtained from computers is crucial, as it provides a basis for linking a particular act to a specific individual. The significance of computer-generated outputs, whether digital or printed, varies in comparative legislation in terms of their admissibility as evidence in criminal cases. The criminal judge has the discretion to form their conviction based on a particular piece of evidence. With the rise of scientific evidence alongside technological advancements, the judge's discretion to assess the weight of evidence in their judgment—whether to convict or acquit—is unrestricted. There is no dispute regarding the validity of computer outputs as evidence, as judges have full discretion to evaluate evidence and render their judgments[29].

Conclusion :

Crimes related to the assault on electronic signatures, along with the developments in modern technology and the global shift towards the use of advanced technologies, have had significant impacts on individuals' lives. The electronic signature has played a major role in bridging distances, particularly in international trade, especially in e-commerce, which has eliminated many of the barriers that characterized traditional commerce.

At the same time, negative consequences have emerged, notably cybercrime, which has spread widely through individuals who are highly skilled and possess vast experience and capabilities in information technology, making them a direct threat to others' finances and even intruding into individuals' private lives. The legislator has attempted to address this issue with measures adopted by most countries worldwide to detect such crimes. The strength of legal provisions in combating these crimes varies from one country to another. Most international and national legislations have recognized electronic signatures, granting them legal validity for proof. The goal is to broaden the use of electronic signatures, making them accessible to society through state-backed initiatives, as it will eliminate much of the bureaucratic red tape. Additionally, it has the same evidentiary weight as a traditional signature, along with activating protection methods used through the web and granting them legal status.

The Arab world is likewise undergoing a digital revolution that has significantly impacted all aspects of life. As a result, the electronic signature has become a vital instrument for both public and private entities providing services through computer-based platforms. It is

therefore imperative to study and draw upon the experiences of technologically advanced countries in the implementation of electronic signature systems, which continue to require further legal, technical, and practical examination.

Key Findings

1. The subject of electronic signatures remains a relatively recent area of legal development.
2. The implementation of electronic signature systems is a fundamental project that can help solidify core democratic principles.

Recommendations

It has become imperative to keep pace with technological advancements. As developments in computing and digital networks accelerate at an unprecedented rate, and in light of the global interconnectedness of information systems, enhancing legal and technical protective measures in the field of electronic signatures is now more crucial than ever.

References:

1 -Adel Abdel-Aali Ibrahim Farashi, Challenges of International Cooperation in Combating Cybercrimes and Ways to Overcome Them, New University Publishing House, Alexandria, 2015, p. 8.

2- Hisham Mohamed Farid Rostom, Cybercrimes: Foundations of Technical Criminal Investigation, Security and Arts Journal, Dubai Police Academy, Issue 3, 1999, p. 110.

3- Naghamouche Mohamed Meloudia Ahmed, Cybercrime: The Necessity of Developing International Cooperation Mechanisms in Combating It, Journal of Legal and Political Studies, Vol. 4, Issue 2, 2018, p. 268.

4- Farid Nashef, Mechanisms of International Cooperation in Combating Cybercrimes, Journal of Research in Law and Political Science, Vol. 8, Issue 1, 2022, p. 433.

5- Herdo Center for Digital Change Support, Cybercrime and the Digital Evidence Validity in Criminal Proof, Cairo, 2014, p. 87.

6 - Herdo Center for Digital Expression Support, Previous Reference, p. 10.

7- Law No. 09/04 dated August 5, 2009, On the Specific Rules for the Prevention and Combating of Crimes Related to Information and Communication Technology, No. 47, dated August 16, 2009.

8 - Kamal Al-Karki, Technical Aspects of Misuse of Computers, A paper presented at the Symposium on Crimes Arising from Technologic

Aucune source spécifiée dans le document actif.al Development, Cairo, 1998, p. 21.

9 - Ghazi Abdulrahman Hayan Al-Rasheed, Legal Protection Against Internet Crimes, Doctoral Dissertation, Islamic University of Lebanon, Faculty of Law, 2004, p. 140.

10 - Ahmed Abdullah Fikry, Crimes of Information Systems, University Freedom Publishing House, Egypt, 2007, p. 74.

11 - Mahmoud Ahmed Abbabsa, Computer Crimes and Their International Dimensions, Culture Publishing and Distribution House, 2009, p. 42.

12 - Mahmoud Saad Abdel-Majid, The Cybercriminal, University Publications Press, Alexandria, 2022, p. 41.

13 - Fathallah Mahmoud Rajab, Explanation of Cyber Extortion Crimes: A Comparative Applied Study, New University Publishing House, Alexandria, Egypt, p. 79.

14 - Tariq Ibrahim Desouki Attia, Information Security: The Legal System for Information Protection, New University Publishing House, Alexandria, 2009, p. 322.

15 - Tariq Ibrahim Desouki Attia, Previous Reference, p. 323.

16 -Yasser Mohamed Elkomy Abu Hatab, Criminal and Security Protection of Electronic Signatures: A Comparative Study, Al-Maaref Establishment, Alexandria, 2014, p. 358.

17 - Faris Khattabi, Criminal Protection of Electronic Signatures, Doctoral Dissertation, Faculty of Law, University of Ben El-haj Lakhdar, Batna, 2020/2021, p. 27.

18 - Law No. 15/04 dated February 1, 2015, Setting the General Rules for Electronic Signatures and Certifications, Article *6*.

19 - Naseer Mohamed Mohamed, Electronic Evidence and Its Validity Before Courts, Scientific Books Publishing House, Lebanon, 2013, p. 77.

20 - Yasser Mohamed Elkomy Abu Hatab, Previous Reference, p. 359.

21 - Major General Siraj, Former Vice President of INTERPOL, INTERPOL Reference.

22 -Sameer Hamid Abdulaziz Al-Hammal, Contracting via Modern Communication Technologies, Dar Al-Nahda Al-Arabiya, Egypt, 2006, p. 220.

23 - Ghazali Naziha, Legal Mechanisms for Protecting Electronic Payment Methods in Algerian Legislation, Journal of Political and Administrative Research, 2017, p. 292.

24 - Mohamed Atouli, Technical and Legal Mechanisms for Protecting Electronic Signatures, Al-Fikr Journal, Issue 18, 2019, p. 305.

25 - Khattabi Faris, Criminal Protection of Electronic Signatures, Doctoral Dissertation.

26 - Ibrahim Sayed Ahmed, Electronic Commerce Law, Electronic Signature, and Intellectual Property Law, New University Publishing House, Alexandria, Egypt, 2005, p. 323.

27- Ayman Ramadan Mohamed Ahmed, Criminal Protection of Electronic Signatures: A Comparative Study, Dar Al-Nahda Al-Arabiya, Cairo, Egypt, 2011, p. 417.

28- Jamil Abdulbaqi Saghir, Evidence of Criminal Proof and Modern Technology: A Comparative Study, Dar Al-Nahda Al-Arabiya, 2005, p. 77.

29 - Yasser Mohamed Elkomy Abu Hatab, Previous Reference, p. 308.