THE ELECTRONIC SIGNATURE AS EMERGIG CRIMES

[1]SARAH ABDULLA ALZEYOUDI, [2]MAHER ALJABER

[1]Master of Cybersecurity Law, Fujairah University
[2]Associate Professor, Faculty of Law, Fujairah University.
E-mail: [1]2025220039@fu.ac.ae,[1]m.aljaber@fu.ac.ae, [2]maeraljaber@bau.edu.jo.

Abstract - The world has witnessed tremendous advancements in digital technologies over the past few decades, opening up vast new possibilities in the fields of communication, education, and work. The significance of this study lies in identifying crimes related to the misuse of electronic signatures as one of the most serious problems facing society today. This problem stems from the widespread use of digital services and the threats they pose to individuals and institutions. This study addresses the issue of criminal liability for crimes committed using electronic signatures, taking into account the nature of digital crimes, the speed of their spread, and the complexity of digital evidence. Using a descriptive-analytical approach, this study describes the origins of electronic signature crimes and their legal, technical, and social dimensions. It then analyzes these dimensions to arrive at a comprehensive understanding of the factors influencing the emergence of these crimes. The study concludes that cybercrimes, particularly the misuse of electronic signatures, pose a real threat to our society today, as they directly affect individuals, institutions, and states financially, psychologically, and in terms of security. The study recommends updating national legislation to cover all types of cybercrimes, establishing clear and effective penalties for all types of cybercrimes, and ensuring that these penalties keep pace with rapid technological developments.

Keywords - Electronic Signature, Cyber Crimes, Legal Liability, UAE

I. INTRODUCTION

In recent decades, the world has witnessed a tremendous boom in digital technology, which has opened up vast opportunities for communication, education, and work. At the same time, however, this digital development has created a fertile environment for the emergence of cybercrime, defined as illegal acts committed using digital means (Al-Wadgiri, 2016). Digital services are an essential part of our daily lives, making individuals and organizations more vulnerable to digital risks, which include threats to privacy and data protection, financial security, or the misuse of personal data (Abdel Aal, 2025). Therefore, societies today face a major challenge in combating these crimes, not only because of their rapid spread and ability to cross geographical borders, but also due to the complexity of digital evidence and the difficulty in identifying perpetrators, in addition to differences in legislation between countries—a situation that requires legal authorities to develop their understanding of cybercrime.

Problem of Study

The focus of this study is to examine criminal liability for crimes committed through the use of electronic signatures, given the digital nature of such crimes, their rapid spread, the complexity of digital evidence, and the difficulty of proving criminal intent, in addition to differences in legislation among countries given that these crimes are cross-border in nature. The problem becomes clear through an understanding of how to determine the criminal liability of perpetrators in crimes committed through the misuse of electronic signatures. The study also highlights the legal and technical difficulties in collecting digital evidence and presenting it in court, as well as determining the extent to which national and international legislation keeps pace with these rapid developments in the methods of committing electronic signature crimes.

The Importance of Study

The significance of this study lies in its focus on crimes involving the misuse of electronic signatures, which are among the most serious challenges facing modern societies due to the widespread use of digital services and the resulting risks to individuals and institutions. The study also helps clarify the concept of electronic signatures, their types, and their essential elements, thereby enhancing the legal and technical understanding of these crimes and assisting judicial authorities in addressing them more effectively. Furthermore, the study provides an understanding of the criminal liability associated with crimes involving the misuse of electronic signatures and the relevant methods of proof, thereby supporting legal efforts to prosecute perpetrators and impose appropriate penalties. This study also aims to identify the legal and technical challenges in combating cybercrimes, including difficulties in proving the case, identifying the perpetrator, and international cooperation, thereby contributing to the development of practical solutions to improve legislation and legal mechanisms to combat them. Finally, this study seeks to raise public awareness of the importance of protecting personal data and sensitive information and to encourage the adoption of secure practices when using digital tools, thereby reducing the incidence of cybercrime.

Methodology

This study employs a descriptive-analytical approach, in which the phenomenon of electronic signature

crimes and their legal, technical, and social dimensions are described and then analyzed to arrive at a comprehensive understanding of the factors contributing to the emergence of these crimes, the criminal liability they entail, and the methods of proof associated with them. This is achieved through the collection of data and information from reliable sources such as legal texts, academic journals, previous studies, and national and international legislation related to cybercrimes. The study also relies on an analysis that examines the elements of cybercrimes, methods of proof, and legal challenges, while comparing different legislations in the Arab world and internationally.

II. THE NATURE OF ELECTRONIC SIGNATURE

UAE Federal Decree-Law No. (46) of 2021 on Electronic Transactions and Trust Services provides definitions for electronic signatures, qualified electronic signatures, and certified electronic signatures, The UAE law defines an electronic signature as a signature consisting of letters, numbers, symbols, a voice, a fingerprint, or a processing system in electronic form, which is attached to or logically associated with an electronic document, and which serves to verify the identity of the signatory and their acceptance of the content of the data associated with it. A trusted electronic signature, on the other hand, is an electronic signature that meets the conditions specified in Article (19) of this Decree-Law. An approved electronic signature is a qualified electronic signature created using an approved electronic signature tool and issued based on an approved electronic signature certificate (Al-Wadgiri, 2016).

The U.S. Federal Law also defines an electronic signature as a symbol, code, or electronic process attached to or incorporated into a contract or other record, executed or displayed by a person with the intent to sign the record. Egyptian Law No. 15 of 2004 on Electronic Signatures defines an electronic signature as a mark placed on an electronic document in the form of letters, numbers, symbols, or other signs, which has a unique character that allows the signer to be identified and distinguishes them from others (Al-Wadgheiri, 2016).

There are numerous jurisprudential and legal definitions of the concept of an electronic signature, and it is evident from all these definitions that there is a clear convergence in substance despite differences in wording. UAE law is among the modern legal systems that seek to strike a balance between legal tradition and technological advancement regarding types of crimes, as it classifies them into felonies, misdemeanors, and violations based on clear and specific legal provisions, thereby providing legislative stability. However, with the emergence of cybercrimes, the use of electronic signatures in electronic transactions has increased, leading to the emergence of various types of related cybercrimes, which vary in form and method. These crimes include electronic signature forgery, digital identity theft, and unauthorized system intrusion, as well as the use of signatures in fraudulent or illegal operations. These types of crimes stand out as one of the challenges facing digital development, requiring effective legal and technical measures to address them (Abdel Aal, 2025).

U.S. law, on the other hand, is characterized by a unique system that combines written legislation with a case law tradition, granting it considerable flexibility in addressing both traditional and modern crimes. It classifies crimes into felonies and misdemeanors, and the severity of a crime is determined based on its nature and the prescribed penalty, This allows the judge to play an important role in interpreting legal texts and applying the law to the facts of a case. However, with the rapid and widespread adoption of electronic signatures, a range of related crimes has emerged that undermine the credibility of electronic transactions. Among the most prominent of these are the forgery of digital signatures, electronic identity theft, and fraud involving the misuse of signatures, in addition to cyberattacks targeting authentication systems through unauthorized access to or disruption of signature systems, and the misuse of signatures, such as their use in fraudulent schemes and fictitious contracts, or even unauthorized disclosure through the leakage of signature keys or authentication data (Al-Wadgiri, 2016). These crimes reflect an evolution in criminal methods within the digital environment, which necessitates the development of ongoing mechanisms to combat them (Abdel Aal, 2025).

III. THE LEGAL VALIDITY OF ELECTRONIC COMMERCE

National legislation has moved toward recognizing electronic signatures and granting them legal validity as evidence, with the aim of keeping pace with rapid technological advancements and facilitating electronic and digital commercial transactions. For example, the UAE legislature has adopted a clear legal framework through the Electronic Transactions and Trust Services Law, which grants electronic signatures legal validity provided they meet technical and legal requirements that ensure the signer’s identity, their control over the signing device, and the ability to detect any alterations to the electronic document. It has also focused on enhancing trust in digital transactions by regulating trust services and electronic certification, thereby strengthening the evidentiary weight before the courts.

Accordingly, the UAE legislature and all national laws that have recognized electronic signatures have deemed any violation of electronic signatures to be a crime, and have defined the elements of cybercrime as similar to those specified in the general rules of criminal law. Crimes related to electronic signatures are based on legal, material, and moral elements, with a clear reliance on legal texts without significant expansion in judicial interpretation. It is noted that UAE law has prioritized the clarity of legal rules over their flexibility. In the field of electronic signatures, the UAE is considered to have an advanced regulatory framework, as electronic signatures are regulated under the laws governing electronic transactions, with precise conditions established to ensure security—such as identity verification and document integrity—and certification authorities are subject to government oversight, which enhances trust in digital transactions (Al-Darmaki, 2024).

As for criminal liability, the law is clear and strict, particularly regarding cybercrimes, to the extent that it imposes criminal liability on legal entities for the commission of any crimes related to electronic signatures, with the aim of strongly protecting the digital community (Emad al-Din, 2020).

One of the elements of crimes related to electronic signatures is a material element, which consists of any unauthorized use of an electronic signature or tampering with the digital information associated with it, including forging an electronic signature or entering false data into electronic transaction systems. In addition, there is a mental element consisting of criminal intent—that is, the intention to commit electronic fraud or to achieve personal gain or harm others.

As for the nature of criminal liability, UAE law imposes imprisonment and fines on those who commit forgery or tamper with electronic signatures, with penalties increased or reduced depending on the individual's role in the crime, It should be noted that the UAE legislature classifies these crimes as federal offenses. Furthermore, with regard to the nature of criminal liability for cybercrimes and electronic forgery, they are classified under UAE law as federal offenses, and perpetrators may be punished with imprisonment for several years and substantial fines (Al-Darmaki, 2024).

Egypt followed the same approach when its legislature established penalties for the commission of any crime related to electronic signatures, provided that the material element—such as forgery, the unlawful use of an electronic signature, hacking, or tampering with electronic systems related to the signature—is present. In addition, the mental element must be present, consisting of criminal intent aimed at achieving personal gain or even causing harm to others. The Egyptian legislature has established penalties for crimes of forgery and tampering with electronic signatures, punishing perpetrators with imprisonment and fines, with the possibility of harsher penalties when such crimes are committed against public funds or critical infrastructure (Al-Darmaki, 2024).

IV. CONCLUSION

This study reached a number of conclusions, namely:

1. Cybercrimes involving the misuse of electronic signatures pose a real threat to modern societies due to their direct impact on individuals, institutions, and nations—whether financially, psychologically, or in terms of security.
2. Cybercrimes involving the misuse of electronic signatures differ from traditional crimes due to their distinctive characteristics, such as rapid spread, the ability to cross geographical borders, the difficulty of identifying the perpetrator, and the complexity of digital evidence, which increases the difficulty of investigation and prosecution.
3. Criminal liability for cybercrimes involving the misuse of electronic signatures rests on three essential elements: the legal element, the material element, and the subjective element, with the necessity of proving criminal intent using reliable digital evidence.
4. Traditional methods of proof are insufficient to address cybercrimes involving the misuse of electronic signatures; rather, one must rely on digital evidence, technical data analysis, login records, and IP addresses, while consulting digital forensic experts to ensure the validity of the evidence.

Based on these findings, this study recommends:

1. The need to update national legislation to cover all types of cybercrimes, while establishing clear and effective penalties for each type of such crime and ensuring that they keep pace with rapid technological developments.
2. The need to strengthen international cooperation among countries to combat cybercrime through standardized agreements, information sharing, the extradition of criminals, and the facilitation of digital evidence collection.
3. The need to develop community awareness programs regarding cyber risks, targeting both individuals and institutions, to enhance the protection of personal and financial data and reduce the incidence of cybercrime.

REFERENCES

[1] Abdel-Aal, Ahmed. (2025). Electronic Forgery: Between Traditional Legislation and Modern Countermeasures. *The*

Academic Journal of Research and Scientific Publication, 70, 42–62.

[2] Al-Darmaki, Fatima. (2024). *Elements of the Crime of Electronic Forgery* (Unpublished doctoral dissertation). Mansoura University.

[3] Al-Wadgiri, Muhammad. (2016). Legal Protection of Electronic Signatures. *E Moroccan Journal of Legal Studies and Consultancy, 1*, 39–54.

[4] Emad al-Din, Barakat. (2020). The Evidential Value of Electronic Signatures in Proving Electronic Transactions. *Journal of the Research Professor of Legal and Political Studies, 4*(2), 1332–1345.

★★★