LEGAL SAFEGUARDS AND CHALLENGES IN THE COLLECTION OF DIGITAL EVIDENCE IN THE UAE

[1]WALEED ALRAEESI, [2]SALEH ALRAEESI, [3]EISA ALBLOSHI, [4]MAHER ALJABER

[1]Master of Cybersecurity Law, Fujairah University.
[2,3,4]Associate Professor of Cybersecurity Law, Faculty Of Law. Fujairah University.
E-mail: [1]202510332@fu.ac.ae., [2]202510316@fu.ac.ae., [3]202510441@fu.ac.ae, [4]maheraljaber@bau.edu.jo

Abstract – In recent years, the United Arab Emirates has witnessed substantial structural changes across its economic, legal, and technical frameworks, as part of its transition toward a fully integrated model grounded in the digital economy, smart governance, and advanced information infrastructure. Cyber evidence has emerged as a fundamental element in the criminal evidentiary system; in many instances, it has become the sole evidence capable of uncovering the truth, given that cybercrimes generatedigital footprints rather than physical traces. The problematic nature of this study lies in examining the legal safeguards and challenges associated with the collection of digital evidence in the UAE. For the purpose of achieving the study's objectives, the study adopts a descriptive-analytical approach, based on a review of relevant legal studies on this subject, along with an analysis of the applicable legal provisions. The study reached several findings, most notably that the UAE legal system demonstrates flexibility regarding the admissibility of digital evidence; however, it still relies on general rules that require elaboration beyond what currently exists. Therefore, the study proposes several recommendations, the most important of which is the need to enact legislation that regulates cyber evidence with greater procedural detail.

Keywords - Digital Evidence, Legal Safeguards, Legal Evidence, UAE Legislation

I. INTRODUCTION

In recent years, the United Arab Emirates has witnessed profound structural transformations in its economic, legal, and technological frameworks, marked by a transition to an integrated model based on the digital economy, smart government, and advanced information infrastructure. This transformation was not merely a development in terms of means; rather, it represented a comprehensive reshaping of the very nature of legal relations. Consequently, transactions, obligations, and legal dispositions are now conducted within a digital environment characterized by speed, complexity, and the interchangeability of systems.

This new reality has led to the emergence of cyberspace as a legal domain parallel to the traditional one, where both legal and illegal acts are conducted alike. This has led to the emergence of modern patterns of crime that differ in their nature and mechanisms of commission from traditional crimes. Crime is no longer bound by time or place; rather, it has become capable of crossing borders, being carried out in virtual environments, and utilizing advanced technological tools that enable perpetrators to conceal their identities and cover their tracks. (Kerr, 2018).

In the midst of this transformation, cyber evidence has emerged as a fundamental element within the criminal evidentiary system. In many cases, it has become, the sole evidence capable of uncovering the truth, given that cybercrimes leave digital footprints rather than physical traces. However, such evidence raises substantive challenges concerning its nature, admissibility, reliability, and the handling mechanisms employed by the competent authorities.

Cyber evidence differs from traditional evidence by its intangible nature, rendering it imperceptible to direct human senses. Moreover, it can also be altered or destroyed without leaving a visible trace, and it can be easily copied or transferred, raising questions about the extent to which it can be relied upon as conclusive proof. Furthermore, this evidence may be distributed across multiple systems or countries, which complicates the process of gathering it and raises issues related to jurisdiction and international cooperation (Casey, 2011).

Recognizing these challenges, the UAE legislator sought to establish a sophisticated legal framework that keeps pace with the nature of cybercrimes while ensuring the protection of fundamental rights and freedoms. Consequently, modern legislation—most notably laws related to combating cybercrime and electronic transactions—has emerged to affirm the admissibility of digital evidence and establish a general framework for handling it. However, despite their importance, these provisions still require careful interpretation and application that takes into account rapid technological developments.

1.1. Problem of the Study

The problematic nature of this study lies in its investigating the legal safeguards and challenges inherent in the collection of digital evidence within the UAE. It aims to provide a comprehensive overview of the procedures that cyber evidence undergoes, commencing from the discovery phase, through seizure, preservation, and analysis, and concluding with its submission to the judiciary. Particular emphasis is placed on the legal guarantees underpinning these procedures, the challenges encountered, and the potential solutions to mitigate them (Casey, 2011).

1.2 Methodology

This paper relies on several integrated scientific approaches to ensure that its subject matter is addressed with precision and depth, specifically the descriptive-analytical approach. This approach was utilized to present and clarify concepts relevant to digital evidence, alongsidethe analytical approach which aimed at interpreting legal rules and examining their applications in light of technological developments. (Kerr, 2018).

1.3 Importance of the Study

Hence, the significance of this study arises from its objective to conduct an in-depth analysis of cyber evidence collection procedures within the UAE judicial system taking into account both legal and technical aspects, aiming at assess the adequacy of the existing regulatory framework while envisioning future developmental pathways in order to achieve a balance between the efficacy of criminal justice and the protection of fundamental rights and freedoms.

The significance of this study is not limited to the theoretical aspect; it extends to the practical aspect, as it can help support the work of judgesand members of the Public Prosecution, and improve the performanceof the competent authorities tasked with evidence collection. Furthermore, it serves as a pivotal reference for researchers in the field of Digital Criminal Law, which is currently one of the most rapidly evolving fields.

II. THE NATURE OF CYBER EVIDENCE

The concept of cyber evidence serves asthe cornerstone for constructing the theory of proof within the digital environmentas it is inconceivable to establish effective legal regulations governing the collection or evaluation of evidence without a precise definition of its nature, scope, and function. Arguably, the most salient characteristic of this concept is that it emanated from a radical shift in the very nature of legal relations. These relations have transitioned from the traditional physical framework to a virtual digital paradigm, where legal acts are carried out through technical means that leave no tangible traces in the traditional sense.

In this context, evidence is no longer understood as a physical object that can be directly seized or examined but rather consists of digital data generated within information systems, processed through algorithms, and stored on electronic media that may be local, cloud-based, or distributed across global networks. Consequently, cyber evidence is not an independent entity in and of itself, but rather the result of an interaction between the user and the technical system, which gives it a complex nature that combines legal and technical dimensions (Alenzi, 2022).

Accordingly, cyber evidence may be conceptualized as any digital representation of conduct, an incident, or an interaction, capable of extraction through legitimate technical methodologies, and admissible for the substantiation or refutation of a legal fact before the judiciary. This digital representation includes a vast array of forms, such as electronic communications, system access logs (log-in/log-out), geolocation data, network traffic records, stored or recovered files, and even behavioral patterns that can be inferred from data analysis.

Cybersecurity evidence, on the other hand, is dynamic in nature; it does not remain static but may change, be deleted, or be moved at any moment, which makes “preserving evidence” a real challenge. Digital evidence is not merely something to be discovered; it is something that must be “secured” quickly before it disappears or changes, which requires immediate intervention by the relevant authorities.

Cyber evidence may also be fragmented by nature, as the complete evidence is not found in a single location but is distributed across multiple sources, such as the user’s device, the service server, and the network, which necessitates a complex process of collection and analysis to link these parts together. This distribution raises the issue of the unity of the evidence and the extent to which it can be considered a single piece of evidence or a set of integrated evidence. (Brenner, 2010).

Given this, it becomes clear that digital evidence is more than just digital data; it constitutes a complex system of technical indicators that requires a deep understanding of its nature. This justifies the need to develop specific legal rules to address it, rather than subjecting it to traditional rules that are ill-suited to its nature.(Behl et al., 2007).

Digital evidence is characterized by several distinct attributes. Primarily, cyber evidence lacks a physical form that can be possessed or tangible transported; instead, it consists of digital data stored within electronic media. This attribute necessitates a fundamental shift in the concept of seizure; evidence is not physically moved but rather duplicated, a process that raises critical legal inquiries regarding the concepts of 'original' and 'copy' within the digital environment. Additionally, evidence can be lost or altered as a result of a simple intervention, whether caused by the user, the system, or even external factors.This fragility makes it necessary to take immediate and precise measures to preserve the evidence from the moment it is discovered. Finally, digital evidence is characterized by its cross-border nature, as it may be distributed across multiple countries, raising legal issues regarding jurisdiction and accessibility (Giolli et al., 2009)

Accordingly, the UAE legal system has adopted a sophisticated approach in recognizing the probative force of cyber evidence. This type of evidence is no longer perceived as an exception; rather, it has become an integral part of the evidentiary system,

governed by the same general principles while accounting for its unique nature.This has necessitated the establishment of legal and technical safeguards to ensure the integrity of the evidence. This involves the need to establish legal and technical controls that ensure the integrity of the evidence and make it technically verifiable, which requires strengthening the role of technical expertise in this context.Finally, it is worth noting the importance of distinguishing between traditional evidence and digital evidence, as traditional evidence relies on physical presence, which facilitates its transfer from its scene to the investigating authority; this is due to the ease of its preservation and, consequently, the facilitation of its transfer. (Brenner, 2010).

III. THE LEGAL SAFEGUARDS AND CHALLENGES IN THE COLLECTION OF DIGITAL EVIDENCE

The safeguards afforded to the accused constitute a cornerstone of the criminal justice system, and their significance is particularly heightened in the context of cyber evidence, given the technical complexity inherent in such evidence, which may impair the accused's ability to fully comprehend or effectively challenge it. Accordingly, the proper administration of justice in this domain necessitates the establishment of robust safeguards capable of maintaining an equitable balance between prosecutorial authority and the rights of the defense.

Foremost among these safeguards is the principle of procedural legality, whereby cyber evidence may only be collected in accordance with specific legal frameworks, with authorization from the competent authority, and within the limits prescribed by law. This principle is the cornerstone of protecting the accused from abuse of power.

The right to defense and confrontation is also a fundamental safeguard; the accused must be allowed to review the digital evidence presented against them, discuss technical reports, and challenge them through expert witnesses. This right takes on particular importance given the technical nature of cyber evidence. (Behl et al., 2017).

Additional safeguards include the presumption of innocence, whereby digital evidence shall not be deemed an irrebuttable presumption; rather, it must be assessed within the context of the totality of the evidence. Moreover, the principle of proportionality must also be observed, ensuring that evidence-gathering procedures do not exceed what is necessary to achieve their purpose. The importance of judicial oversight of search and seizure procedures is also highlighted, as such oversight serves as a fundamental safeguard against violations. (Alenzi, 2022).

Nevertheless, significant legal challenges arise during the collection of digital evidence, which can be encapsulated in the requirements to uphold individuals' right to privacy. Since digital evidence collection may necessitate accessing personal devices or electronic accounts containing sensitive data, it becomes imperative to establish precise controls to prevent any unlawful expansion in this domain. In this context, obtaining prior judicial authorization (a search warrant) is regarded as one of the most pivotal safeguards for privacy; it defines the scope and limits of the search, thereby preventing the arbitrary expansion of data collection. Furthermore, such authorization must be specific in terms of time, location, and subject matter. Hence, the principle of proportionality assumes prominence, requiring that the measures taken remain necessary and commensurate with the gravity of the crime, ensuring that data irrelevant to the investigation is not collected. This must be coupled with a strict adherence to data confidentiality, restricting the use of collected information solely to the confines of the case (Brenner, 2010).

Technical challenges also arise in the form of encryption, which requires special keys to decrypt the evidence that has been obtained. Furthermore, suspects often use specific methods to conceal their true identities, making it extremely difficult to track them down.(Taylor et al., 2011).

Furthermore, Legal challenges arise concerning judicial jurisdiction, where conflicts of jurisdiction emerge due to the cross-border nature of digital evidence. This complicates access to evidence when it is located outside a country's borders, a situation that requires international coordination and cooperation.

Finally, there are practical challenges stemming from a shortage of personnel capable of handling such evidence, which necessitates training these personnel through courses and workshops, taking into account the current rapid technological evolution of criminal methods, which makes it difficult for systems to adapt to these methods, particularly technological ones (Wall, 2007).

This study concludes that the UAE legislature is working diligently to keep pace with ongoing technological developments, leading it to adopt a modern approach based on integrating digital evidence into the evidentiary system without completely separating it from traditional evidence—an approach that reflects legislative flexibility aimed at accommodating technological advancements. Nevertheless, statutory provisions are often characterized by broad phrasing, leaving wide latitude for interpretation, which may result in disparities in practical application. The lack of specificity in certain procedural matters—such as forensic imaging mechanisms or data integrity verification standards—may create a gap between the statutory text and its implementation. Furthermore, the current regulatory framework relies heavily on general principles, such as procedural

legality and the integrity of evidence, without establishing specific technical standards. This makes reliance on technical experts inevitable, but at the same time may lead to varying outcomes. (Casey, 2011).

Consequently, this study emphasizes the imperative of refining procedures for handling digital evidence by establishing granular regulations for electronic search and seizure. These regulations should define data access mechanisms, protocols for managing cloud-based systems, and standards for documenting technical procedures. Moreover, clear 'Chain of Custody' rules must be developed to ensure the precise traceability of evidence from the point of collection. This requires enhancing the use of modern technical means in evidence collection through the use of artificial intelligence technologies, while establishing legal controls for their use to ensure that lawful limits are not exceeded. (Kerr, 2011).

IV. FINDINGS AND RECOMMENDATIONS

The current study has reached the following findings:

1. In light of the preceding analysis, it is clear that cyber evidence has become an essential element of criminal proof, rather than merely an auxiliary tool.
2. This study found that the integrity of procedures for seizing, preserving, and subsequently analysing digital evidence is the decisive factor in the admissibility of the evidence.
3. This study also found that numerous legal, technical, and practical challenges arise when collecting digital evidence.
4. Finally, this study concluded that the UAE legal system is flexible regarding the admissibility of digital evidence, but it relies on general rules that require further elaboration.

In light of the findings, and amid the accelerated pace of digital transformation, the study proposes the following recommendations:

1. The need to enact specialized procedural legislation that regulates cyber evidence in detail, establishing uniform technical standards for handling and analyzing digital evidence, by regulating the use of artificial intelligence in handling digital evidence and its analysis mechanisms, and by developing oversight mechanisms for technical expertise to ensure its impartiality.
2. strengthen international coordination and cooperation in the field of cybercrime by facilitating access to digital evidence across borders.
3. Advancing the capacity-building and qualification of judges and members of the Public Prosecution in the field of digital evidence. This is essential to keep pace with the tremendous technical advancements in the field of cybercrime and the methods used to commit such crimes.

REFERENCES

[1] Behl, A., & Behl, K. 2017. Cybersecurity and cyberwar: What everyone needs to know. Oxford Academic Journal. 12(2), 55–70.

[2] Bernner, S. 2010. Cybercrime: Criminal Threats from Cyberspace. Praeger Security International

[3] Casey, E. 2011. Digital Evidence and Computer Crime (3rd ed.). Academic Press. United States.

[4] Kerr, O. 2018. Computer Crime Law (4th ed.). West Academic Publishing. United States.

[5] Taylor, M., Haggerty, J., Gresty, D., & Lamb, D. 2011. Forensic investigation of cloud computing systems. Network Security. 2011(3), 4–10.

[6] Wall, D. 2007. Cybercrime: The Transformation of Crime in the Information Age. Polity Press. United Kingdom.

★★★