Research Journal in Advanced Humanities

RJAH

https://doi.org/10.58256/q5m9z769

Open Access

Check for updates

REVIEW ARTICLE

Section: *Digital Humanities*

The criminal protection of digital evidence in criminal and civil matters: A comparative study

Abdullah Ehjelah[1], Maamoun Abu Zaitoun[1], Yusuf Obeidat[1], Hamzeh Abu Issa[2], & Majd Waleed Almanasra[3]

[1]Yarmouk University, Jordan

[2]Applied Science Private University, Jordan

[3]United Arab Emirates University, United Arab Emirates

*Correspondence: a.ehjelah@yahoo.com

ABSTRACT

This study addresses the topic of the criminal protection of digital evidence in matters of criminal and civil law. It does so by explaining the criminal procedures that must be observed to protect this evidence and detailing the legal provisions that criminalize and penalize acts of assault on digital evidence in comparative laws. The importance of this study lies in the fact that countries worldwide are currently moving toward the use of information technology in various fields. Information technology is now widely employed in contract execution, communication, and digital transactions, all of which are inevitably accompanied by digital evidence. Crimes involving this technology may arise, which are difficult to prove without the existence of digital evidence, thus necessitating special criminal protection for such evidence. The problem addressed by this study stems from a legislative shortfall in some comparative laws, which is represented by the narrow scope of criminal protection for digital evidence. This shortfall includes the requirement of specific characteristics in the perpetrator for the crime of assault on this evidence, as well as restricting substantive protection to digital evidence related only to crimes specified in electronic laws. Additionally, the problem includes the absence of protection for digital evidence related to civil matters. This study relied on the analytical and comparative approaches and reached several conclusions, most notably: There is suitable procedural criminal protection for digital evidence in comparative laws. There is also appropriate substantive criminal protection for digital evidence in Jordanian and Palestinian law, but the scope of substantive protection for digital evidence is limited under Emirati law. The study offers several recommendations, the most prominent of which is the addition of provisions to some electronic crime laws that expand the scope of substantive protection for digital evidence.

KEYWORDS: digital evidence, cyber crimes, criminal law, comparative law

Research Journal in Advanced Humanities

Volume 7, Issue 1, 2026

ISSN: 2708-5945 (Print)

ISSN: 2708-5953 (Online)

ARTICLE HISTORY

Submitted: 04 **December 2025**

Accepted: 28 **January 2026**

Published: 12 **March 2026**

HOW TO CITE

Ehjelah, A., Zaitoun, M. A., Obeidat, Y., Issa, H. A., & Almanasra, M. W. (2026). The criminal protection of digital evidence in criminal and civil matters: A comparative study. *Research Journal in Advanced Humanities*, *7*(1). https://doi.org/10.58256/q5m9z769

Published in Nairobi, Kenya by Royallite Global, an imprint of Royallite Publishers Limited

Introduction

It is natural that the technological revolution is accompanied by digital crimes, characterized by their rapid execution and the ease with which their traces can be erased by destroying or tampering with their digital evidence (Abu Issa et al., 2025). Given the importance of this evidence in uncovering the truth and the reliance of the judiciary on it in resolving criminal and civil cases before it, some comparative laws have established specific provisions criminalizing and penalizing acts of assault on digital evidence. These provisions aim to hide the facts relating to criminal and civil matters.

In light of these specific criminalizing and punitive provisions, and in line with the information technology revolution, the concept of criminal protection for digital evidence in criminal and civil matters emerged (Abu Issa & Khater, 2023). This is especially important since traditional provisions in criminal laws may not fully address the criminalization of assaults on digital evidence.

The significance of the study lies in its modernity and the fact that it has not been thoroughly researched. This is especially true as countries are currently moving toward using information technology in various fields on a wide scale (Al-Billeh & Abu Issa, 2025). For instance, this technology may be used in contract execution, communication, and digital transactions, which will undoubtedly be accompanied by digital evidence proving their authenticity (Obeidat, 2004; Obeidat, 2016; Khashashneh et al., 2023). In the public sector, the digital processing and storage of disciplinary offences committed by local government employees has even led to the recognition of a distinct right to digital expungement in comparative Jordanian–Qatari scholarship, illustrating how digital evidence and digital records continue to produce legal effects long after the underlying conduct has occurred (Aljazi, 2024).

Additionally, this widespread use may result in digital crimes that pose significant threats to states and individuals, which are difficult to prove without the existence of digital evidence. Recent research on the role of anti-corruption commissions in controlling administrative decisions in Jordan shows how central documentary and record-based evidence has become in administrative oversight mechanisms (Aljazi et al., 2024), much of which is nowadays generated and stored in digital form. Therefore, special criminal protection for such evidence must be provided (Juwaihan, Abu Issa, & Khater, 2025).

The problem addressed by this study can be summarized as follows: In light of the increasing risk of assaults on digital evidence required to prove contracts, communications, transactions, and digital crimes due to the rising use of information technology across various fields, appropriate criminal protection for this evidence must be provided.

This study's problem is further compounded by the legislative shortfall in some comparative laws on this matter. This shortfall can be clarified as follows:

1. The Emirati Cybercrime Law requires specific characteristics in the perpetrator for the crime of assault on digital evidence to be established.
2. This law limits the scope of criminal protection to digital evidence related to crimes explicitly mentioned therein, excluding digital evidence related to civil matters.

Although the Palestinian law extends criminal protection to digital evidence in judicial matters related to both criminal and civil issues, it does not clarify the meaning of judicial digital evidence.

Additionally, Lebanese law lacks specific criminal protection for digital evidence. Reference to the Lebanese Penal Code reveals that the scope of criminal protection for evidence, in general, is narrow, as the law requires its presentation before the judiciary for it to be protected.

The study raises a central question: What are the legislative shortcomings in comparative laws regarding the criminal protection of digital evidence?

The primary objective of the study is to identify legislative shortcomings in comparative laws regarding the criminal protection of digital evidence and to provide necessary recommendations to address this gap.

The study adopts the analytical method by analyzing the provisions of comparative laws related to the topic to highlight the shortcomings of these laws. It also employs the comparative method to examine similarities and differences between Jordanian, Emirati, Palestinian, and Lebanese laws regarding the criminal protection of digital evidence.

As for the study's structure, it is divided into an introduction, two sections, and a conclusion. The first

section addresses procedural protection for digital evidence, and the second discusses substantive protection for such evidence. Unlike conventional criminal law research structures, which usually begin with the substantive aspect and then move to the procedural aspect, this study begins with the procedural aspect before transitioning to the substantive aspect.

This exception is due to the unique nature of this study, which necessitates clarification of the subject of criminal protection - digital evidence as a fundamental element of the crime. It is challenging to identify and distinguish digital evidence from other data and information stored in systems and networks without first understanding the procedural steps involved in collecting and obtaining evidence, such as inspection, search, seizure, preservation, and storage of this evidence.

Procedural Protection in the Jordanian Cybercrime Law

Article (32) of the Jordanian Cybercrime Law No. (17) of 2023 provides procedural protection for digital evidence by granting judicial officers the authority to inspect and examine devices, programs, and information networks, and to seize devices, tools, programs, operating systems, and information networks, as well as to preserve information and data related to the crime.

In this context, the Zarqa First Instance Court, in its capacity as a criminal appellate court, stated in its decision No. (368/2020) the necessity of seizing all items necessary for uncovering the truth, organizing an official record for this purpose, and storing these items in containers appropriate to their nature, sealed with an official stamp.

On the other hand, Article (33) of the same law emphasizes procedural protection by granting the Public Prosecutor and the competent court the authority to take modern and unconventional measures to seize digital evidence. These measures include issuing many orders to those managing information systems and websites, such as removing, blocking, suspending, disabling, recording, or intercepting the flow of data or any publication or content, as well as prohibiting access to such data. They also include providing the Public Prosecutor and the court with all necessary data or information for uncovering the truth, urgently preserving the required data and information, and storing this data and information while ensuring their integrity.

The storage of data and information does not prevent copying it onto an electronic storage medium that can be seized and stored in a sealed container in accordance with the rules stipulated in the Jordanian Code of Criminal Procedure.

Procedural Protection in the Emirati Cybercrime Law

Article (60) of the Emirati Code of Criminal Procedure No. (38) of 2022 provides procedural protection for digital evidence by granting judicial officers the authority to take available precautionary measures regarding items that may contain traces useful for uncovering the truth. These officers are also authorized to seize items that may have been used in committing the crime, describe these items, present them to the accused for their observations, and secure the seized items in containers sealed with appropriate means to prevent tampering.

This was affirmed by the Federal Supreme Court of the UAE when discussing the necessity of securing items needed to uncover the truth in its ruling on appeal No. (133/17 - Criminal Law, hearing dated 27/1/1996). Articles (73) and (74) of the same law further emphasize procedural protection for digital evidence by granting the Public Prosecutor several powers, the most important of which are seizing all correspondence and letters held at postal offices, inspecting devices, systems, and electronic networks when required by the investigation, and monitoring and recording wired and wireless communications.

It is widely acknowledged that procedures such as inspection, search, seizure, and securing seized items are among the most important methods for collecting and preserving evidence (Al-Billeh et al., 2024; Altaani et al., 2024).

These procedures may be followed by obtaining witness statements and confessions from the accused remotely, in accordance with Article (1) of Emirati Federal Law No. (5) of 2017, regarding the use of remote communication technology in criminal procedures. Recent scholarship has analysed the impact of such remotely taken confessions on the criminal judge's conscientious conviction, highlighting the evidentiary and procedural sensitivities associated with this form of digital evidence (Ehjelah & Bani Amer, 2023).

Procedural Protection in the Palestinian Cybercrime Law

Articles (32), (33), (34), (35), and (36) of the Palestinian Cybercrime Law No. (10) of 2018 provide procedural protection for digital evidence by granting judicial authorities (the Public Prosecutor and the court) the power to issue several decisions and procedures, which are carried out by judicial officers.

The most important of these decisions and procedures include inspecting information technology tools and seizing devices related to the crime. It also involves obtaining devices, tools, methods, data, and electronic information connected to the crime (Al-Khawajah et al., 2023). Additionally, securing information technology tools that may uncover the truth is essential. Copying data and information relevant to the crime is also a key procedure. Appropriate means must be used to prevent access to stored data. The integrity of seized electronic evidence must be preserved. Lastly, monitoring and recording electronic communications and conversations is necessary to search for evidence related to the crime (Khater, 2024).

These decisions and procedures include the immediate interception of communication content and its recording. This means covert monitoring of communications within the framework of crime investigation, gathering forensic evidence, and preserving it according to procedural rules (Stoykova, 2023a).

In most cases, these decisions and procedures are carried out after accessing the electronic crime scene and examining its traces, including sent and received messages and all communications conducted via computers and information networks (Angel et al., 2024).

Procedural Protection in the Lebanese Cybercrime Law

Articles (121) to (124) of the Lebanese Electronic Transactions and Personal Data Law No. (81) of 2018 provide procedural protection for digital evidence by requiring judicial officers to adhere to specific measures when seizing and preserving digital evidence based on authorization from the Public Prosecutor or the competent court.

These measures include organizing a record of all actions taken during the seizure, preservation, analysis, or transfer of digital evidence, specifying the procedures taken, and documenting all entities that possessed the evidence and how it was transferred (Ehjelah, 2023). These measures particularly emphasize ensuring the integrity of the evidence from the moment of its seizure.

In all cases, an identical copy of the data and information must be preserved in the same form as it was at the time of seizure. The evidence must be secured on electronic media sealed with appropriate means. The Lebanese Code of Criminal Procedure's provisions on searches and seizures are applied to the handling of digital evidence (Khater, Abu Issa, & Alwerikat, 2023).

If the data or digital evidence is downloaded or transferred from an electronic location or computer system, its source must be clearly stated. Any digital evidence stored in an information system located within Lebanese territory can be seized if it is accessible from the system subject to inspection (Sokol et al., 2020).

This means that the law permits remote searches of information systems as long as they are located within Lebanese territory. However, this matter becomes increasingly complex when these systems extend to other parts of the world (Wilson-Kovacs et al., 2023).

Substantive Protection in the Jordanian Cybercrime Law

In general, Article (222) of the Jordanian Penal Code No. (16) of 1960 criminalized the destruction, concealment, or distortion of documents, records, or any item, regardless of its type, if it pertains to judicial proceedings. It imposed penalties classified as misdemeanors.

Specifically, Article (36/d) of the Jordanian Cybercrime Law criminalized and penalized acts involving tampering with or destroying digital evidence presented, derived, or extracted from devices, networks, and information systems. The article stipulates:

> "Anyone who conceals, tampers with, or destroys the evidence referred to in this article or its traces or obstructs the competent authorities from accessing such evidence shall be punished by imprisonment for a period of not less than three months."

We will clarify this protection under Jordanian law by addressing the elements and penalties of the crime of

tampering with digital evidence, followed by commentary on this approach:

First: Elements and Penalty of the Crime of Tampering with Digital Evidence

1. **The Object Element (Presumed Element):** This element represents the interest the legislator seeks to protect, namely, **digital evidence**.

The first question posed is: Is the protection here limited to digital evidence associated with crimes specified in the Jordanian Cybercrime Law No. (17) of 2023?

In our estimation, the protection extends beyond evidence tied to crimes exclusively governed by this law. Instead, it includes all digital evidence related to any crime, whether falling under this law or any other, as the provision's wording is general and unrestricted (Moussa, 2021).

The second question is: What is meant by the terms "digital evidence presented," "digital evidence derived," and "digital evidence extracted" from devices, equipment, media, or information networks?

In our view:

- **"Presented digital evidence"** refers to evidence submitted by individuals to judicial authorities, either voluntarily or at the authorities' request, after investigative or preliminary procedures related to a crime.
- **"Extracted digital evidence"** refers to evidence retrieved after investigative or preliminary procedures, maintaining its original form (whether in electronic or paper format, as a copy, transfer, or printout) from information systems.
- **"Derived digital evidence"** refers to evidence obtained through the collection and analysis of electronic data using specialized devices, software, or technological applications. It differs from "extracted evidence," as derived evidence involves analytical processing that generates new insights, whereas extracted evidence retains its existing format (Miller, 2023).

The third question posed is: Does criminal protection for digital evidence extend to include evidence related to electronic transactions unconnected to any crime?

In our assessment, this protection does extend to such evidence. This conclusion is based on the general and unrestricted language of Article (36), which encompasses all evidence related to criminal and civil matters (Stoykova, 2023a).

2. ***Actus Reus*:** This element involves **tampering with digital evidence**, meaning altering such evidence wholly or partially.
   - **Destroying evidence** refers to erasing it so that it becomes unusable.
   - **Concealing digital evidence** entails hiding or suppressing evidence to prevent its discovery.
   - The general and specific criminal intent may also involve obstructing the competent authorities from accessing this evidence by any means (Lewulis, 2022).

The Irbid First Instance Court, in its capacity as a criminal appellate court, clarified this aspect in its decision No. (7217/2023), stating that the general and specific criminal intent of the crime of destroying evidence, as stipulated in Article (222) of the Penal Code, involves actions that impede the integrity or availability of the evidence.

3. ***Mens Rea* (General and specific criminal intent):** *Mens rea* involves **general intent**, which consists of knowledge and intent. This includes:
   - Awareness of all circumstances and elements necessary for the existence of the crime.
   - Knowledge of tampering with or destroying digital evidence presented, derived, or extracted from information systems.
   - Awareness of obstructing the competent authorities from accessing such evidence (Dodge, 2018).

Additionally, the perpetrator must have the intent to tamper with or destroy the evidence.

The North Amman Magistrate Court, in its decision No. (3401/2022), confirmed that general intent (knowledge and intent) is required to establish the crime of destroying evidence, as stipulated in Article (222) of the Penal

Code.

4. **Penalty Prescribed for This Crime under Jordanian Law:** Article (36/d) of the Jordanian Cybercrime Law penalizes this crime with imprisonment for no less than three months. General legal principles stipulate that the maximum term of imprisonment is three years, as per Article (21) of the Jordanian Penal Code No. (16) of 1960.

Second: Commentary on the Jordanian Legislative Approach to the Crime of Tampering with Digital Evidence

In our view, the Jordanian legislative approach is commendable for the following reasons:

1. It does not require a specific qualification for the offender to establish the crime, such as being an administrator of a website or an account on an information network.
2. The protection extends to digital evidence related to both criminal and civil matters.
3. The law does not require a specific intent (e.g., intent to obstruct the authorities) to establish the crime (Stoykova & Franke, 2023).

Substantive Protection in the Emirati Cybercrime Law

"Any person responsible for managing a website, an account on an information network, an email, or an information system, who conceals or tampers with digital evidence of any crime stipulated under this decree-law, with the intent to obstruct the work of investigative, prosecutorial, or other competent authorities, shall be punished with imprisonment. The imprisonment period shall be no less than six months. Additionally, the person may face a fine of no less than 200,000 dirhams, or either of these penalties."

This protection under Emirati law will be clarified by addressing the conditions, elements, and penalties associated with the crime of tampering with digital evidence, followed by commentary on this legislative approach:

First: Conditions, Elements, and Penalty for the Crime of Tampering with Digital Evidence

1. **The Presumed Condition Regarding the Perpetrator's Status:** This law stipulates that a specific qualification must exist for the perpetrator to establish the crime: the individual must be "responsible for managing a website, account on an information network, email, or information system." (Birze, Regehr, & Regehr, 2023).

The perpetrator, in this case, must engage in acts of concealing or tampering with digital evidence of any crime stipulated under the Cybercrime Law.

2. **The Object Element (Presumed Element):** This element represents the interest the legislator seeks to protect, namely, **digital evidence related to crimes specified in the Emirati Cybercrime Law.**

Article (1) of the law defines **digital evidence** as follows:

> "Electronic information that has probative value or evidentiary strength, stored, transmitted, extracted, or obtained from computers, information networks, or their equivalents. Such information can be collected and analyzed using specialized technological devices, software, or applications."

Two key factors are associated with the digital evidence collected from electronic devices:

> - **The probative value of the information** stored, transmitted, extracted, or obtained from information networks before the competent authorities. The definition implies the ability of such information to establish the commission of a crime before judicial bodies.
> - **The ability to collect and analyze the information** using specialized devices, programs, or technological applications (Stoykova et al., 2022).

We believe that programs used for collecting, obtaining, or extracting information should possess technical features that ensure no changes, updates, deletions, or alterations occur to the data or information (Giri Santosa & Ibnu Kamali, 2022).

The process of collecting digital forensic evidence typically involves several stages, including:

1. Evidence collection.
2. Extraction.
3. Preservation.
4. Securing and sealing.
5. Documentation and description.
6. Preparation of seizure reports regarding the evidence (Belshaw & Nodeland, 2022).

3. **Actus Reus:** The general and specific criminal intent involves **tampering with digital evidence** to obstruct the competent authorities from accessing it.
   - **Tampering** refers to altering or erasing the evidence entirely or partially.
   - **Concealing digital evidence** entails hiding or suppressing it to prevent its discovery.

It is essential to note that the existence of a **primary underlying crime** is a prerequisite. The perpetrator must aim to obstruct the discovery of the original crime and the identification of the perpetrator (De Arcos Tejerizo, 2023).

In cases where the perpetrator engages in both tampering and concealing the evidence, these actions are considered part of a single offense known as a "continuing crime."

4. **Mens Rea (General and Specific Criminal Intent):** The mental element in this crime includes both **general intent** and **specific intent**:
   - **General intent** involves knowledge of all circumstances and elements of the crime, including knowledge of tampering with or concealing digital evidence related to crimes specified in the law, and the intention to commit these acts.
   - **Specific intent** involves the perpetrator's intent to obstruct the work of investigative, prosecutorial, or other competent authorities from accessing the digital evidence and identifying the perpetrator (Nikkel, 2020).

The existence of specific intent is crucial to establishing this crime.

5. **Penalty Prescribed for This Crime under Emirati Law:** Article (18) of the Emirati Cybercrime Law prescribes the following penalties:
   - Imprisonment for no less than six months.
   - A fine of no less than 200,000 dirhams.
   - Either or both penalties may be applied.

According to general principles, the maximum term of imprisonment is three years, as stipulated in Article (70) of the Emirati Penal Code No. (31) of 2021.

Second: Commentary on the Emirati Legislative Approach to the Crime of Tampering with Digital Evidence

1. The law restricts the scope of criminal protection for digital evidence to crimes specified within the Cybercrime Law, excluding other types of crimes.
2. It does not extend protection to digital evidence related to civil matters.
3. Requiring a specific qualification for the offender (i.e., being responsible for managing a website or account) is a restrictive approach that narrows the scope of the crime.
4. This specific qualification also violates the principle of equality in criminalization and punishment, as only individuals meeting this condition are penalized, while others who tamper with digital evidence are not (Klenka, 2022).

Substantive Protection in the Palestinian Cybercrime Law

Article (47) of the Palestinian Cybercrime Law No. (10) of 2018 states: "Anyone who tampers with, destroys, conceals, modifies, or erases judicial digital evidence shall be punished by

imprisonment for a period of no less than one year, and a fine of no less than one thousand Jordanian dinars, and no more than three thousand Jordanian dinars."

This protection under Palestinian law will be clarified by examining the elements and penalties associated with the crime of tampering with judicial digital evidence, followed by a discussion of the legislative approach in this regard (Stoykova, 2023b).

First: Elements and Penalty of the Crime of Tampering with Digital Evidence

1. **The Object Element (Presumed Element):** This element pertains to the interest the legislator seeks to protect, which is **judicial digital evidence**.

The question arises: What is meant by "judicial digital evidence" as mentioned in Article (47)?
We believe that the term refers to digital evidence presented by individuals to judicial authorities, such as judicial officers, the Public Prosecutor, or the court. This evidence is presented either voluntarily or upon request from the authorities after investigative or preliminary procedures have been conducted concerning a particular crime. This also includes evidence presented to **civil courts** in civil lawsuits.

2. ***Actus Reus*:** This element involves **tampering with judicial digital evidence**, which includes altering, destroying, concealing, modifying, or erasing such evidence.
3. ***Mens Rea* (Mental Element):** The mental element in this crime consists of **general intent** with its two components: knowledge and intent. The perpetrator must:
   - Be aware of all circumstances and elements necessary for the crime to occur.
   - Be aware that they are tampering with or destroying judicial digital evidence.
   - Intend to tamper with or destroy the digital evidence.

4. **Penalty Prescribed for This Crime under Palestinian Law:** Article (47) of the Palestinian Cybercrime Law stipulates the following penalties:
   - Imprisonment for no less than one year.
   - A fine no less than one thousand Jordanian dinars and no more than three thousand Jordanian dinars.
   - The maximum imprisonment term is three years, in accordance with general principles outlined in Article (21) of the Palestinian Penal Code No. (16) of 1960.

Second: Commentary on the Palestinian Legislative Approach to the Crime of Tampering with Digital Evidence
The Palestinian approach to the criminal protection of digital evidence has several noteworthy aspects:

1. **No Specific Qualification for the Perpetrator:** The law does not require a specific qualification or role for the perpetrator. This makes the protection more inclusive and applicable to any individual who tampers with judicial digital evidence.
2. **Protection Extends to Both Criminal and Civil Matters:** Unlike some comparative laws, Palestinian law extends protection to judicial digital evidence related to both criminal and civil matters. This ensures that all types of digital evidence, whether pertaining to criminal or civil cases, are safeguarded under the law.
3. **No Requirement for Specific Criminal Intent:** The law does not require the presence of specific intent (such as intent to obstruct justice or authorities). It is sufficient that the perpetrator has general intent to tamper with or destroy the evidence. This broad approach allows for better protection of digital evidence.

Substantive Protection in the Lebanese Cybercrime Law
Despite the distinctive procedural protections provided for digital evidence under the Lebanese Electronic Transactions and Personal Data Law No. (81) of 2018 (Articles 121 to 124), this law does not criminalize actions involving the tampering or destruction of digital evidence. Therefore, the Lebanese Penal Code No. (340) of 1943 is referred to in such cases.

Article (416) of the Lebanese Penal Code states:

"Anyone who alters, conceals, destroys, or damages any document or item that was previously presented to the judiciary shall be punished with a fine ranging from 50,000 to 600,000 Lebanese pounds."

This provision implies that digital evidence, like other forms of evidence, can be subject to criminal sanctions if tampered with, destroyed, or altered. However, this protection is limited to the instances where the evidence has been formally presented to the judiciary.

First: Legislative Gaps in Lebanese Law Regarding Criminal Protection of Digital Evidence

1. **Lack of Specific Provisions for Tampering with Digital Evidence:** Lebanese law lacks a specific provision criminalizing acts of assault on digital evidence, unlike the Jordanian, Emirati, and Palestinian laws. The reliance on general provisions in the Lebanese Penal Code limits the scope of protection for digital evidence.
2. **Narrow Scope of Protection:** The Lebanese law only extends criminal protection to digital evidence that has been presented to the judiciary. This restriction limits the scope of protection, as evidence that has not yet been submitted to the court is not covered by the law.
3. **Inadequate Penalties for Digital Evidence Tampering:** The penalties prescribed under Lebanese law for tampering with or destroying evidence (a fine between 50,000 and 600,000 Lebanese pounds) are insufficient and lack deterrent effects.

Conclusion

This has researched the legal implications of digital evidence in criminal and civil matters through a comparison of Jordanian, Emirati, Palestinian, and Lebanese legislation. The conclusion of the analysis is that comparative laws indeed provide at the procedural level adequate mechanisms for the investigation, collection, seizure, and preservation of digital evidence. Further, judicial authorities and law enforcement bodies are equipped with powers that enable them to access information systems, secure data, and maintain the integrity of electronic traces in a manner that supports the discovery of the truth and the administration of justice.

Legislation in Jordan and Palestine provides adequate protection for digital evidence at the substantive level. Both systems criminalize the tampering and destruction of such evidence and further provide protections for civil matters alongside criminal. This goes to show that the role of digital recorded evidence in contractual, civil, and other non-criminal issues is well recognized; the reliability and availability thereof are equally crucial in the context of non-criminal evidence as it is in prosecution cases.

In contrast, under Emirati law, substantive protection for digital evidence appears limited. By this, it means that protection is and can only be exercised with respect to specific crimes listed in the Cybercrime Law, while other requirements tied to the status of the perpetrator, in addition to having specific intent, restrict such protection. This limitation greatly impairs the ability of the law to respond in all-encompassing terms to all forms of attacks on digital evidence. Lebanon has some procedural safeguards for the handling of digital evidence; however, the punishments for the destruction of any evidence are still quite low and do not serve as much of a deterrent to crime. More so, the criminalization of the destruction of digital evidence and the protection of the digital evidence under general provisions of the Penal Code creates regulatory uncertainty-further restricting this already fragmented legal framework.

Given these discoveries, it appears from the ensuing deliberations that the necessity and urgency for legislative reform are evident. The provisions in comparative criminal procedure laws that deal with the investigation and seizure of evidence should be amended to clarify that the phrases "item" or "items" shall include all types and forms of digital evidence. Such clarification would eliminate interpretive ambiguities and would ensure that there is equal procedural protection for digital evidence as for physical evidence. The legislative assemblies in the jurisdictions named deserve encouragement for the enactment of enactments that would provide clear definitions for assaults on digital evidence that are required for proper adjudication in both criminal and civil matters and would punish such assaults with imprisonment for a term of two to three years. Further, it should eliminate any unacceptable limitations, such as confining the protection to just certain types of offenses or to particular statuses of offenders, which may unduly restrict the scope of criminalization. This will assist the lawmakers in bringing their legal systems in line with the realities of the digital age, thereby augmenting the protection of the integrity, availability, and evidentiary value of digital evidence.

References

Abu Issa, H., & Khater, M. (2023). Distance indecent assault crime in Jordanian law perspective. *Pakistan Journal of Criminology, 15* (1), 125–138.

Abu Issa, H., Al Wreikat, N., Al-Billeh, T., & Alhasan, T. (2025). From streets to screens: Legal implications of internet begging. *Humanities and Social Sciences Communications, 12*, 916. https://doi.org/10.1057/s41599-025-05189-w

Al-Billeh, T., & Abu Issa, H. (2025). The legislative and judicial framework for the administrative control authorities in Jordan: What are the risks of social networks on elements of public order? *Gosudarstvo i Pravo, (2)*, 144–153. https://journals.eco-vector.com/1026-9452/article/view/682850/kk_KZ

Al-Billeh, T., Al-Hammouri, A., Khashashneh, T., Al Makhmari, M., & Al Kalbani, H. (2024). Digital evidence in human rights violations and international criminal justice. *Journal of Human Rights Culture and Legal System, 4* (3), 842–871. https://doi.org/10.53955/jhcls.v4i3.446

Aljazi, J. D. (2024). The right of local government employees to expungement of disciplinary offences processed digitally in Jordanian and Qatari legislation. *Legality: Jurnal Ilmiah Hukum, 33* (1), 20–43. https://doi.org/10.22219/ljih.v33i1.36212

Aljazi, J. D., Alzubidi, K. L., & Al-Shibli, F. S. (2024). The role of the anti-corruption commissions in controlling the administrative decisions. *Journal of Governance & Regulation, 13* (1, Special Issue), 405–415. https://doi.org/10.22495/jgrv13i1siart14

Al-Khawajah, N., Al-Billeh, T., & Manasra, M. (2023). Digital forensic challenges in Jordanian cybercrime law. *Pakistan Journal of Criminology, 15* (3), 29–44.

Altaani, D., Ehjelah, A., Bani Amer, S., & Abu Issa, H. (2024). Virtual justice: Navigating the challenges of remote testimony at the International Criminal Court. *International Journal of Criminal Justice Sciences, 19*(2), 15–26.

Angel, O. E. M., et al. (2024). Digital evidence as a means of proof in criminal proceedings. *Revista de Gestao Social e Ambiental, 18* (4). https://doi.org/10.24857/rgsa.v18n4-028

Belshaw, S., & Nodeland, B. (2022). Digital evidence experts in the law enforcement community: Understanding the use of forensics examiners by police agencies. *Security Journal, 35* (1), 248–262. https://doi.org/10.1057/s41284-020-00276-w

Birze, A., Regehr, K., & Regehr, C. (2023). Workplace trauma in a digital age: The impact of video evidence of violent crime on criminal justice professionals. *Journal of Interpersonal Violence, 38* (1–2), NP1654–NP1689. https://doi.org/10.1177/08862605221090571

De Arcos Tejerizo, M. (2023). Digital evidence and fair trial rights at the International Criminal Court. *Leiden Journal of International Law, 36*(3), 749–769. https://doi.org/10.1017/S0922156523000031

Dodge, A. (2018). The digital witness: The role of digital evidence in criminal justice responses to sexual violence. *Feminist Theory, 19*(3), 303–321. https://doi.org/10.1177/1464700117743049

Ehjelah, A. (2023). Criminal modus operandi in Bahraini tax law No. 40 of 2017. *Pakistan Journal of Criminology, 15*(4), 389–400.

Ehjelah, A., & Bani Amer, S. (2023). Impact of confessions taken remotely via modern technology on the conscientious conviction of the criminal judge. *Pakistan Journal of Criminology, 15*(3), 211–223. https://www.pjcriminology.com/publications/impact-of-confessions-taken-remotely-via-modern-technology-on-the-conscientious-conviction-of-the-criminal-judge/

Giri Santosa, D. G., & Ibnu Kamali, K. M. (2022). Acquisition and presentation of digital evidence in criminal trial in Indonesia. *Jurnal Hukum dan Peradilan, 11*(2), 195–218. https://doi.org/10.25216/jhp.11.2.2022.195-218

Juwaihan, M., Abu Issa, H., & Khater, M. N. (2025). The crime of counterfeiting or imitating a trademark under Jordanian trademarks law. *The Journal of World Intellectual Property, 28*(2), 589–611. https://doi.org/10.1111/jwip.12346

Khashashneh, T., Al-Billeh, T., Al-Hammouri, A., & Belghit, R. (2023). The importance of digital technology in extracting electronic evidence: How can digital technology be used at crime scenes? *Pakistan Journal of Criminology, 15*(4), 69–85.

Khater, M. N. (2024). Criminalization of forgery of electronic payment cards in Jordanian legislation. *Pakistan*

Journal of Criminology, 16(1), 441–455. https://doi.org/10.62271/pjc.16.1.441.455
Khater, M., Abu Issa, H., & Alwerikat, N. (2023). The mother killing of her newborn to avoid disgrace under Jordanian law. *Pakistan Journal of Criminology, 15*(4), 21–27.
Klenka, M. (2022). Digital evidence in the international criminal law. *Pravnik, 161*(9), 866–880.
Lewulis, P. (2022). Collecting digital evidence from online sources: Deficiencies in current Polish criminal law. *Criminal Law Forum, 33*(1), 39–62. https://doi.org/10.1007/s10609-021-09430-4
Miller, C. M. (2023). A survey of prosecutors and investigators using digital evidence: A starting point. *Forensic Science International: Synergy, 6*, 1–22. https://doi.org/10.1016/j.fsisyn.2022.100296
Moussa, A. F. (2021). Electronic evidence and its authenticity in forensic evidence. *Egyptian Journal of Forensic Sciences, 11*(1). https://doi.org/10.1186/s41935-021-00234-6
Nikkel, B. (2020). Fintech forensics: Criminal investigation and digital evidence in financial technologies. *Forensic Science International: Digital Investigation, 33*, 200908. https://doi.org/10.1016/j.fsidi.2020.200908
Obeidat, Y. M. G. (2004). *The 'penalty' clause in English law: A critical analysis and comparison with Jordanian law* (Doctoral dissertation, University of Leeds).
Obeidat, Y. M. G. (2016). The efficient breach theory under Jordanian civil law. *Arab Law Quarterly, 30*(4), 336–356. https://doi.org/10.1163/15730255-12341328
Sokol, P., Rózenfeldová, L., Lučivjanská, K., & Harašta, J. (2020). IP addresses in the context of digital evidence in the criminal and civil case law of the Slovak Republic. *Forensic Science International: Digital Investigation, 32*, 300972. https://doi.org/10.1016/j.fsidi.2019.300972
Stoykova, R. (2023a). The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations. *Computer Law and Security Review, 49*, 105801. https://doi.org/10.1016/j.clsr.2023.105801
Stoykova, R. (2023b). Encrochat: The hacker with a warrant and fair trials? *Forensic Science International: Digital Investigation, 46*, 301602. https://doi.org/10.1016/j.fsidi.2023.301602
Stoykova, R., & Franke, K. (2023). Reliability validation enabling framework (RVEF) for digital forensics in criminal investigations. *Forensic Science International: Digital Investigation, 45*, 301554. https://doi.org/10.1016/j.fsidi.2023.301554
Stoykova, R., Andersen, S., Franke, K., & Axelsson, S. (2022). Reliability assessment of digital forensic investigations in the Norwegian police. *Forensic Science International: Digital Investigation, 40*, 301299. https://doi.org/10.1016/j.fsidi.2021.301299
Wilson-Kovacs, D., Helm, R., Growns, B., & Redfern, L. (2023). Digital evidence in defence practice: Prevalence, challenges and expertise. *International Journal of Evidence and Proof, 27*(3), 235–253. https://doi.org/10.1177/13657127231171620