

Preliminary Procedures for Digital Crimes and the Rights of the Accused: A Comparative Study of UAE and Egyptian Legislation

Faisal Suhail Hamdan Hassan Alzaabi*^{1,a} Dr. Dina Binti Imam Supaat^{2,b}

i Faculty of Syariah and Law, Universiti Sains Islam Malaysia, Nilai, Negeri Sembilan, Malaysia

ii Faculty of Syariah and Law, Universiti Sains Islam Malaysia, Nilai, Negeri Sembilan, Malaysia
dina@usim.edu.my

*(Corresponding author) e-mail: faisalal970@gmail.com

HOW TO CITE: ABSTRACT

Faisal Suhail Hamdan Hassan
Alzaabi, Dina Binti Imam Supaat,
(2026).
Preliminary Procedures for Digital
Crimes and the Rights of the
Accused: A Comparative Study of
UAE and Egyptian Legislation.
International Journal of Special
Education, 41(23s), 1193 - 1203

This study examines the legal protection of an accused person's rights during the preliminary stages of investigating digital crimes, comparing Emirati and Egyptian legislation. It addresses the challenges posed by digital evidence—specifically the speed required for its collection, its susceptibility to alteration or destruction, and the need to balance investigative effectiveness with the safeguarding of the accused's procedural rights. The study aims to assess the extent to which the respective legal frameworks provide procedural safeguards suited to the unique nature of digital investigations and to identify similarities, differences, and legislative gaps between them. Employing descriptive-analytical and comparative legal methodologies, the study analyzes relevant legislation and procedural rules governing arrest, search, the preservation of digital data and evidence, interrogation, and the right to counsel, while comparing the level of protection afforded to the accused in both systems. The findings reveal a convergence between Emirati and Egyptian legislation in recognizing the importance of digital evidence and the necessity of subjecting its collection to legal and judicial oversight; however, the comparison also highlights differences regarding the level of detail in regulating procedures and safeguards related to digital searches, data preservation, evidence integrity and the chain of custody, and the scope of judicial oversight. The study also revealed common gaps regarding the need for more specific rules to address the technical and evolving nature of digital evidence and to ensure the defense's ability to effectively examine and challenge it. The study's primary contribution lies in providing a comparative analysis that links the efficiency of digital investigations with fair trial guarantees, identifying the strengths and shortcomings of both systems, thereby establishing a foundation for developing a clearer and

COPYRIGHT STATEMENT:

Copyright: © 2026 Authors.
Open access publication under the
terms and conditions

of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>). more balanced procedural framework to protect the rights of the accused in digital crime cases.

Keywords: Digital crimes; rights of the accused; electronic search; technical defense; UAE;

Introduction

Investigations into digital crimes have raised legal challenges that extend beyond the mere criminalization of online conduct to the adequacy of procedural safeguards afforded to the accused during the preliminary stages of criminal proceedings. This issue is particularly pronounced during arrest, interrogation, search, the seizure of devices and digital data, and the preservation and analysis of electronic evidence. Digital investigations often require rapid intervention to preserve evidence, yet these actions remain constrained by fundamental rights—most notably the right to privacy, the right to legal counsel, the privilege against self-incrimination, the presumption of innocence, and the right to challenge the admissibility of evidence presented against the accused. Consequently, the central legal issue addressed in this study is the extent to which Emirati and Egyptian legislation strike a balance between the requirements for effective digital crime investigations and the protection of the accused's procedural rights.

Despite the extensive legal literature concerning cybercrimes and digital evidence, much of it focuses on criminalization, penalties, jurisdiction, and the evidentiary weight of electronic evidence. Comparative analysis regarding the safeguards afforded to the accused during the preliminary procedural stage remains less explored—particularly concerning the implications of the technical nature of digital evidence for search, seizure, interrogation, the right to a defense, and the chain of custody. Systematic comparative studies of the Emirati and Egyptian experiences in this field remain limited; this study seeks to address that gap. Accordingly, it poses a central question: To what extent do Emirati and Egyptian laws provide effective procedural safeguards to protect the rights of the accused

during the preliminary investigation stages of digital crimes? This gives rise to two subsidiary questions: What are the similarities, differences, and legislative gaps between the two systems regarding the regulation of arrest, interrogation, search, digital seizure, the right to legal counsel, and the handling of digital evidence? And how can these safeguards be enhanced to strike a balance between investigative efficiency and the protection of the accused's rights? The comparison between the United Arab Emirates and Egypt is grounded in the significance of both legal systems within the Arab world; while they share common foundations in criminal procedure, they differ in their regulation of offenses, investigative techniques, and the handling of digital evidence. Thus, this comparison makes it possible to determine whether legislative differences result in varying levels of procedural protection and to identify practices that could contribute to legislative development in both countries. In terms of scope, the study focuses specifically on the rights of the accused during the preliminary investigation stage of digital crimes, particularly safeguards related to arrest, detention, interrogation, legal representation, search, electronic seizure, the preservation of digital evidence, and the challenging of such evidence. The study does not delve into the substantive provisions defining digital offenses, the prescribed penalties, or the full trial and appellate processes, except insofar as is necessary to explain the impact of preliminary procedures on the rights of the accused. The study's originality lies in its shift from a descriptive comparison of legal texts to a functional and critical analysis of procedural safeguards. It achieves this by identifying points of convergence and divergence, legislative gaps, and the extent to which traditional procedural rules are suited to the unique nature of digital evidence. In doing so,

the study aims to provide a comparative framework that can inform the development of clearer rules regarding the legality of digital searches and seizures, the integrity of the chain of custody, the right to a technical defense, and judicial oversight—thereby striking a more effective balance between law enforcement requirements and fair trial guarantees.

Methodology?

The study employs a comparative, analytical legal methodology to examine the procedural safeguards afforded to the accused in digital crimes within the United Arab Emirates and Egypt. These two countries were selected due to the similarities in the general foundations of their criminal procedure laws, contrasted with differences in the regulation of digital crimes and digital evidence; this allows for the identification of commonalities, distinctions, and legislative gaps. The sources analyzed include constitutions, criminal procedure codes, legislation regarding cybercrime and digital evidence, relevant judicial rulings and principles, and international human rights instruments. Legal texts and judicial precedents are analyzed using a functional approach that focuses on the practical protection of rights, rather than merely comparing the wording of statutes. The comparative criteria encompass the legality of arrest and detention; safeguards regarding interrogation and access to counsel; judicial oversight; digital search and seizure; the integrity and chain of custody of digital evidence; and the ability to challenge such evidence. The International Covenant on Civil and Political Rights (ICCPR) serves as the normative framework for evaluation—specifically Article 9 (liberty, security, and freedom from arbitrary arrest), Article 14 (fair trial and defense guarantees), and Article 17 (protection against arbitrary or unlawful interference with privacy). These standards are applied with due regard for the specific legal status of each country: Egypt is a State Party to the Covenant, whereas for the UAE, the study utilizes the Covenant's standards as an international comparative benchmark for

assessment, rather than as a direct treaty obligation.

Preliminary Procedures in UAE Law and Legislation

Pre-trial procedures hold particular significance in the context of digital crimes, as they represent the stage where the State's authority to gather evidence intersects with the accused's rights to liberty, privacy, defense, and a fair trial. The UAE's legal framework is primarily grounded in the UAE Constitution and Federal Decree-Law No. (38) of 2022 Promulgating the Criminal Procedural Law, alongside Federal Decree-Law No. (34) of 2021 Concerning Combating Rumors and Cybercrimes. The legal issue lies not merely in the existence of investigative authority, but in the limits of that authority, the accompanying safeguards, and the suitability of rules—originally designed for traditional search and seizure—for the digital environment.

Arrest

The Constitution establishes the supreme foundation for procedural protection; Article (26) guarantees personal liberty, stipulating that no person may be arrested, searched, or detained except in accordance with the law, while also prohibiting torture and degrading treatment. The Criminal Procedural Law reinforces this protection by specifying the circumstances under which the accused's liberty may be restricted and identifying the authority competent to issue such an order. During the Public Prosecution's investigation phase, Article (100) regulates arrest warrants, authorizing the Prosecution to issue them in specific instances. These include the accused's failure to appear after being summoned without a valid excuse, the likelihood of flight, the absence of a known place of residence, or the accused being caught **in flagrante delicto** (red-handed). Thus, arrest is not treated as an absolute power, but rather as a measure requiring a specific legal basis. The law establishes a significant temporal safeguard: Article (102) mandates the immediate interrogation of the arrested person. If immediate interrogation is not feasible, the individual may not be held in custody

for more than twenty-four hours before being referred to the Public Prosecution, which must then either interrogate the individual or order their release. Consequently, exceeding legal limits on arrest or continuing to restrict liberty without the requisite legal basis and oversight raises questions regarding the lawfulness of the procedure and the implications for any evidence derived from it.

Pre-trial Detention

Pre-trial detention differs from arrest in terms of its nature, duration, and impact on personal liberty. Under Article (103) of the Criminal Procedure Law, the Public Prosecution may—following the interrogation of the accused—order pre-trial detention if sufficient evidence exists regarding a felony or a misdemeanor punishable by a penalty other than a fine. Thus, the legislator conditions detention on two fundamental requirements: the prior interrogation of the accused and the existence of sufficient evidence justifying the continued restriction of their liberty.

The importance of these safeguards is particularly evident in the context of digital crimes. While the risk of data deletion or alteration may justify rapid measures to preserve evidence, this should not automatically serve as grounds for continued detention if the evidence can be protected through less restrictive means—such as the technical securing of devices or the creation of a certified forensic copy of the data. Therefore, the necessity and proportionality of detention must be assessed independently of the mere digital nature of the crime. Third: Interrogation and Defense Rights

Interrogation is a central element of procedural protection, as it brings together the authority to conduct an investigation and the accused's right to self-defense. Provisions of the Criminal Procedure Law in this regard must be read in conjunction with Article 28 of the UAE Constitution, which establishes the presumption of innocence and the accused's right to legal representation.

In digital crimes, the right to defense cannot be viewed merely as the presence of a lawyer; evidence may include metadata, access logs, IP addresses, forensic copies of devices, and information extracted from remote platforms or servers. Therefore, an effective defense requires that the accused and their counsel be able to understand the technical basis of the evidence and challenge the integrity of its extraction and its attribution to the accused. This highlights a potential gap between the legal recognition of the right to defense and the actual technical capacity to exercise it in digital cases.

Search and Seizure in the Digital Environment

Digital searches represent the issue that most clearly demonstrates the need to re-evaluate traditional procedural rules. General search rules are premised on the necessity of a legal basis, the specification of the search location and purpose, and adherence to the scope of the authorization. However, applying these principles to a smartphone or computer differs fundamentally from searching a physical location; a single device may contain correspondence, photos, financial, health, and professional data, location logs, and information spanning years. Complexity is further compounded in the case of cloud storage. Possessing a physical phone does not necessarily mean that the authority to search it automatically extends to all remotely stored accounts and data accessible via the device. Cloud-based data may reside on servers outside the country and involve third parties, raising issues regarding the scope of judicial authorization, territorial jurisdiction, privacy, and proportionality. This highlights a significant gap in the current procedural framework: while general rules establish the legitimacy of search and seizure, they do not always address the qualitative and quantitative limits of digital searches with the same level of detail. Therefore, a distinction must be made between the seizure of the physical device and the search of its contents; between locally stored data and cloud-based data; and between the urgent preservation of data and its substantive examination and use as evidence.

The Legal Framework in the Context of Digital Crimes

Rapid advancements in technology and digital communication have fundamentally transformed the nature of crime and the methods by which it is committed; digital crimes have emerged as a new category of offenses relying on electronic media networks and information systems. This shift has posed profound challenges to traditional legal systems originally designed to address conventional physical crimes, necessitating a re-examination of numerous procedural concepts particularly regarding preliminary measures such as arrest, detention, interrogation and the seizure of digital evidence (Al-Hajjar 2021). In this context a need has arisen to develop a legal framework capable of balancing the requirements of combating digital crimes with the protection of the accused's rights in accordance with international laws foremost among them the International Covenant on Civil and Political Rights. This requirement directly contributes to addressing the study's questions regarding the effectiveness of UAE legislation in protecting the rights of the accused during preliminary proceedings for digital crimes and the extent of its alignment with international safeguards. The United Arab Emirates has sought to keep pace with this evolution by enacting Federal Decree-Law No. (34) of 2021 Concerning Combating Rumors and Cybercrimes which serves as the primary legislative framework governing crimes involving information technology alongside Federal Decree-Law No. (38) of 2022 Concerning Criminal Procedures which regulates arrest and investigation powers and their associated procedures. While this approach demonstrates a clear legislative recognition of the unique nature of digital crimes critical analysis reveals that the framework's effectiveness cannot be assessed solely through its statutory provisions; rather it must be evaluated based on its capacity to address the practical challenges inherent in the nature of these crimes (Kilani 2024).

The first of these challenges arises during the arrest phase. Digital crimes differ from traditional

offenses in that evidence may be ephemeral encrypted or subject to immediate deletion necessitating rapid intervention by investigative authorities to preserve it. Although UAE legislation grants investigative authorities relatively broad powers in this regard a potential issue arises: in practice this flexibility could lead to an overbroad interpretation of concepts such as "necessity" or *in flagrante delicto* (commission of the crime in plain view) particularly in cases of ongoing or cross-border cybercrimes. Consequently the research question regarding the effectiveness of safeguards finds its practical application at this specific juncture; the mere existence of legal provisions governing arrest is insufficient if they are susceptible to broad interpretations that might undermine prior judicial oversight of restrictions on liberty (Dutra 2024).

From the perspective of the International Covenant on Civil and Political Rights Article 9 stipulates that any restriction on liberty must be based on clear legal grounds be proportionate and not be arbitrary. When applying this criterion to evaluate UAE legislation it becomes evident that the law aligns in principle with these tenets; however it lacks sufficiently detailed standards defining the concept of limits of expanding the scope of *in flagrante delicto* (caught-in-the-act) scenarios in the electronic realm a gap that paves the way for inconsistencies in practical application (Aazourn 2022).

The legislative and regulatory framework for digital crimes serves as the cornerstone for criminal justice policies addressing this category of offenses. This is due to the distinct technical nature of such crimes which differs fundamentally from traditional offenses regarding the means of commission the nature of evidence their cross-border scope and the speed with which digital traces can be erased or altered. Technological advancement has not only given rise to new criminal patterns but has also reshaped the relationship between investigative authorities and individual rights particularly during preliminary procedures involving arrest digital searches and the collection of electronic

evidence. Consequently the importance of the legislative framework extends beyond merely defining criminal acts to encompass the regulation of procedural powers and their limits within the digital environment (Kilani 2024).

In this context both the UAE and Egyptian legislatures have enacted specialized laws to combat digital crimes; the UAE issued Federal Decree-Law No. (34) of 2021 concerning Combating Rumors and Cybercrimes while Egypt enacted Law No. (175) of 2018 on Combating Information Technology Crimes. These laws reflect a clear effort to develop legal tools capable of addressing technology-related crimes whether by expanding the scope of criminalization or by granting investigative authorities the technical means to access and seize digital evidence. However comparative analysis reveals that the differences between the two systems lie not only in legislative drafting but also in the underlying legal philosophy governing the regulation of the digital sphere itself (Shaimaa Alwan 2024).

In the UAE the legislative framework is characterized by a high degree of flexibility and continuous updating granting the system a greater capacity to keep pace with rapid technological evolution. However in practice this flexibility may result in an expansion of the discretionary powers of investigative authorities particularly regarding digital searches and access to electronic data. In the Egyptian system regulation relies more heavily on established constitutional and judicial precedents; yet the relative reliance on traditional criminal procedural rules raises questions about the framework's ability to effectively accommodate the technical nuances of digital crimes (Abdul Salam Al-Enezi 2014).

From an analytical perspective a comparison between the two systems should not be limited to outlining legislative differences; rather it should address the study's core question regarding the effectiveness of these legal frameworks in protecting the rights of the accused during the preliminary stages of digital crime investigations. While expanding the scope of criminalization or investigative powers may enhance security

efficiency in practice it risks curtailing certain procedural safeguards unless constrained by precise and clear controls. In this context Articles 9 14 and 17 of the International Covenant on Civil and Political Rights provide a crucial evaluative framework for analyzing the Emirati and Egyptian legislation as they address the protection of personal liberty the guarantee of a fair trial and the protection of privacy against arbitrary interference. Evaluating both systems against these standards reveals that while both aim to strike a balance between digital security requirements and procedural safeguards the real challenge lies in the practical effectiveness of this balance particularly given the complex technical nature of digital evidence and the broad scope of electronic investigative powers. Accordingly this study aims to provide a comparative analysis of the legislative and regulatory frameworks governing digital crimes in the UAE and Egypt. It examines the definitions of digital crimes the sources of the governing legal rules policies regarding criminalization and penalties and the extent to which legislation keeps pace with technological advancements. The objective is not merely to identify similarities and differences but to evaluate each legal system's capacity to address digital challenges without compromising the fundamental safeguards afforded to the accused during the preliminary stages of criminal proceedings.

In the United Arab Emirates Federal Decree-Law No. (34) of 2021 concerning Combating Rumors and Cybercrimes did not establish an exhaustive all-encompassing definition of digital crimes; instead it adopted a descriptive approach to criminalization by enumerating specific acts such as unauthorized access to information systems data interception and the dissemination of rumors or misleading information via electronic means that constitute offenses. This indicates that the UAE legislator relies on the functional scope of digital crimes specifically its connection to the use of information technology as either the instrument or the subject matter of the crime thereby granting the legal provisions the flexibility to be applied effectively and to keep pace with technological advancements

(Mohamed Morsi Abdo & Mohamed Siddiq 2019). In Egypt Law No. 175 of 2018 on Combating Information Technology Crimes adopted a similar approach; rather than providing a comprehensive general definition of digital crimes it focused on specifying criminalized acts such as compromising network integrity unauthorized access system disruption or the dissemination of illicit online content. Nevertheless the Egyptian law did provide definitions for certain terms associated with digital crime such as "information system" and "data" thereby helping to clarify the scope of application (Shaimaa Alwan 2024). Regarding scope both legal systems adopt a broad concept of digital crimes that encompasses offenses committed using electronic means as well as those targeting information systems themselves. However UAE legislation is distinguished by a wider scope of criminalization that includes acts related to digital contents such as the dissemination of rumors or misinformation reflecting a commitment to protecting public order and societal security within the digital environment. In contrast Egyptian legislation focuses more heavily on protecting information infrastructure and technical systems alongside criminalizing specific content-related acts (Kilani 2024).

A difference between the two systems is also evident in the clarity of legal terminology; Egyptian law incorporates operational definitions for certain technical concepts which helps minimize ambiguity during implementation. Conversely the UAE's reliance on general wording offers greater flexibility but may raise questions regarding the precision of interpretation in certain instances. Furthermore comparative studies indicate that the absence of a unified definition for digital crimes in both systems reflects the nature of these offenses which evolve more rapidly than legislation can keep pace with thereby prompting lawmakers to adopt specific criminalization strategies. ...flexible approach rather than an all-encompassing definition (Al-Shammari & Al-Mahlawi 2025). In Egypt the Court of Cassation plays a pivotal role in solidifying safeguards for the rights of the accused particularly regarding arrest and search

procedures. The Court has ruled that the invalidity of an arrest and search renders all evidence derived from them invalid precluding its use as a basis for conviction.

Comparative analysis reveals that neither Emirati nor Egyptian legislation establishes, as a general rule, a distinct, exceptional regime for arrest or detention solely because a crime is digital in nature; consequently, the lawfulness of restricting liberty remains subject to general criminal procedural rules, including the conditions governing arrest, *in flagrante delicto* situations, judicial oversight, and detention periods. In contrast, the Egyptian legislator has prescribed specific rules for certain digital investigation procedures; Article 6 of the Anti-Cybercrime Law (Law No. 175 of 2018) authorizes the issuance of reasoned orders for data collection, data preservation, and system searches, while Article 7 expressly regulates urgent blocking measures in cases involving an imminent threat or impending harm. Therefore, the urgency of preserving digital evidence should not, in itself, be interpreted as an independent basis for expanding arrest or detention powers beyond established general procedural safeguards.

Discussion

A comparison of the UAE and Egyptian legal systems regarding digital crimes reveals that legislators have sought to develop legislative and procedural tools enabling law enforcement authorities to combat crimes committed using information and communication technologies. However evaluating the effectiveness of this system should not be limited to its capacity to detect digital crimes and apprehend perpetrators; it must also extend to the extent to which it respects the rights and safeguards afforded to the accused during preliminary proceedings. While the technical nature of digital crime may necessitate rapid measures such as arrest search seizure and data preservation these actions must be carried out within the framework of the principles of procedural legality and the presumption of innocence while upholding personal liberty privacy the right to a defense and the right to a fair trial. In the UAE Federal

Decree-Law No. (34) of 2021 Concerning Combating Rumors and Cybercrimes establishes a specialized legislative framework to address a wide range of crimes committed using information technologies. Its provisions cannot be interpreted in isolation from Federal Decree-Law No. (38) of 2022 Promulgating the Criminal Procedural Law which governs safeguards related to preliminary inquiries investigations arrests searches interrogations pre-trial detention and other measures affecting the liberty and rights of the accused. This interplay underscores the importance of subjecting measures taken in digital crime cases to the general safeguards governing criminal procedure even when the

object of the search or seizure is digital rather than physical in the traditional sense. Conversely the Egyptian legislator has regulated information technology crimes through Law No. 175 of 2018 on Combating Information Technology Crimes alongside relevant criminal procedural rules. Consequently assessing the rights of the accused in digital crime cases within the Egyptian legal system cannot rely solely on the anti-cybercrime law; rather it requires a comprehensive reading that integrates this specialized legislation with the procedural rules governing the powers of judicial police officers and investigative authorities as well as the safeguards afforded to individuals subject to criminal proceedings

Comparative Theme	UAE	Egypt	Common Safeguards	Significant Difference	Digital-Investigation Gap	Consequence for Accused
Arrest	Governed principally by Federal Decree-Law No. 38/2022; arrest requires a lawful statutory basis	Governed by the Code of Criminal Procedure; arrest depends on legally prescribed circumstances	Legality, protection of personal liberty, procedural supervision	Differences in statutory formulation and procedural mechanisms	No autonomous arrest regime merely because evidence is digital	Digital urgency should not independently justify deprivation of liberty
Initial/pre-trial detention	Subject to statutory time limits and prosecutorial/judicial supervision	Subject to statutory limits and judicial/prosecutorial controls	Detention is legally regulated and reviewable	Different procedures and periods of detention/review	Risk that fear of deletion or alteration of digital evidence becomes a broad justification for detention	Potential disproportionate restriction of liberty
Interrogation	Right of defence and prohibition of unlawful coercion	Defence guarantees and restrictions on coercive interrogation	Defence, voluntariness and procedural legality	Differences in detailed procedural regulation	Traditional legal assistance may be insufficient where evidence is technically complex	Accused may be unable effectively to challenge forensic conclusions

Digital search	General search-and-seizure rules supplemented by cybercrime legislation	General procedure supplemented by Law No. 175/2018, including specific digital-investigation powers	Lawful authority and protection against arbitrary interference	Egypt provides more express provisions concerning access to digital systems/data in some contexts	Uncertainty over whether authority to seize a device necessarily permits comprehensive examination of its contents	Risk of overbroad access to private and unrelated information
Cloud/remote data	General procedural and cybercrime rules apply, but questions remain over scope and territorial reach	Digital-evidence provisions provide greater specificity, although cross-border issues remain	Requirement of lawful investigative authority			

One of the most significant comparative issues arises when transitioning from traditional criminal procedures to search and seizure operations within the digital environment. While traditional searches are typically linked to a specific physical location or object searching a smartphone or computer can grant access to a vast array of personal and professional data including images correspondence logs files and accounts much of which may be unrelated to the crime under investigation. Therefore the mere lawfulness of seizing a device does not necessarily authorize unrestricted access to all its contents. This highlights the necessity of defining the scope of a digital search specifying the target data the purpose of access the relevant timeframe and the connection to the crime under investigation to ensure proportionality between the investigative interest and the accused's right to digital privacy Furthermore arrest detention and interrogation in digital crime cases present unique challenges regarding the accused's ability to comprehend the nature of the technical evidence cited against them. Charges may be based on electronic logs metadata IP addresses account access records or technical expert reports the significance of which is difficult for a non-

specialist to evaluate. Consequently guaranteeing the right of defense in such cases is not achieved merely by allowing the accused to retain counsel; rather it requires enabling the defense within the limits prescribed by law to access digital evidence understand the methods of its acquisition and examination challenge its technical and legal integrity and utilize specialized technical expertise when necessary.

The lawfulness of digital evidence is a matter closely linked to the rights of the accused. The probative value of evidence cannot be divorced from the manner in which it was obtained preserved and examined. While the UAE legislator has strengthened the legal framework for electronic evidence through Federal Decree-Law No. (35) of 2022 concerning Evidence in Civil and Commercial Transactions evidence used in criminal proceedings remains fundamentally governed by criminal procedural rules and the legality of the procedures used to collect and seize it. Thus relying on an electronic message file or record against the accused raises questions regarding the evidence's source integrity attribution to the accused the methods of its seizure and extraction and the potential for alteration or tampering emerges as a crucial

technical safeguard for the integrity of the evidence. Documenting the stages of acquisition transfer copying analysis and storage of the device or data and identifying the individuals who handled them helps ensure the evidence remains intact and unaltered from the moment of seizure until its presentation in court. This is significant not only for bolstering the prosecution's case but also for safeguarding the rights of the accused enabling them to challenge the integrity and reliability of the evidence should material irregularities affect the procedures of its collection preservation or analysis. The comparison also highlights the importance as an extension of the right to a defense in digital cases. Disparities in technical knowledge between investigating authorities and the accused can in practice undermine the latter's ability to challenge the evidence presented against them. Consequently, enabling the accused to engage an independent technical expert subject to the fulfillment of relevant legal conditions serves as a crucial safeguard for examining digital evidence verifying the integrity of its extraction and analysis and contesting technical reports submitted by the prosecution. Thus the right to a defense in the digital realm should be understood in broader terms that account for the technical nature of evidence that may form the primary basis of the charges.

Conclusion

The study concludes that both Emirati and Egyptian legislation provide a fundamental set of procedural safeguards to protect the accused

during the initial stages of criminal investigation—particularly regarding the legality of arrest and detention, judicial oversight, defense rights, and the regulation of searches and seizures. However, the comparative analysis reveals that the primary challenge lies not in the absence of these safeguards, but in the adequacy of traditional procedural rules when applied to digital investigations. Key gaps include the lack of sufficient definition regarding the scope of digital device searches; the distinction between seizing a device and examining its contents; access to cloud-stored data; ensuring the integrity of the digital evidence chain of custody; and enabling the defense to effectively examine and challenge technical evidence. These gaps risk expanding the scope of privacy intrusion, undermining the ability to challenge the legality and reliability of evidence, and creating an imbalance between the technical capabilities of investigative authorities and the accused's ability to exercise their right to defense. Consequently, the study recommends developing more specific procedural rules for digital investigations that define the scope of search authorizations, regulate access to remote and cloud-based data, establish clear requirements for documenting the integrity of digital evidence, and ensure the defense has a genuine technical capacity to examine such evidence, while also clearly defining the legal consequences of violating these safeguards. Such measures would enhance the balance between the effectiveness of criminal investigations and the protection of liberty, privacy, and defense rights within both legal systems.

Reference

- Abu Al-Maali Issa Abu Al-Maali & Najla Khairi Al-Fitouri. (2025). Preservation of digital evidence in light of the International Criminal Court system and its supplementary regulations. *Al-Asala Journal* 6(11).
- Ahmed Bahr & Hala. (2023). The penal order and the termination of criminal proceedings under UAE legislation. *Journal of Jurisprudential and Legal Research* 35(43) 183-225.
- Israa Younis Hadi. (2025). Contemporary use of artificial intelligence in criminal investigation. *Ashur Journal of Legal and Political Sciences* (published by the Iraqi Association for Legal Sciences) 2(4) 333-367.
- Bushra Mohamed Al-Amin. (2010). Police justice systems in Arab countries: A comparative study (Volume 493). Naif Arab University for Security Sciences (NAUSS).
- Belmiliani Ezzeddine & Khannouch. (2023). The International Covenant on Civil and Political Rights: A comparative study between Islamic Sharia and Algerian law. *Journal of Law and Humanities* 16(2) 809-827.

- Izourn Amal & Haddad Mubarak Islam. (2022). Mechanisms of the Human Rights Committee in implementing the 1966 International Covenant on Civil and Political Rights (Doctoral dissertation Mouloud Mammeri University).
- Yousef Najeh Bani Jaber. (2024). Obligations under the International Covenant on Civil and Political Rights and their susceptibility to suspension during states of emergency.
- Khaled Mohammed Hamad Al-Juma. (2010). The Human Rights Committee's Interpretation of the International Covenant on Civil and Political Rights: An Applied Study of the Committee's Views on Individual Complaints Regarding Violations by States Parties. *Journal of Law* 34(4).
- Khaled Mohammed Al-Juma. (2008). The Principle of Judicial Independence in the International Covenant on Civil and Political Rights and the Kuwaiti Constitution: A Critical Comparative Study. *Journal of Law* 32(1).
- Allah-Jabu Abdul-Wahid Osama Mubarak. (2020). A Study Discussing the 2019 Sudanese Constitutional Document and the 2019 Sudanese Power Ostracism (Isolation) Law and Comparing Them with the Provisions of the International Covenant on Civil and Political Rights. *Journal of Legal and Social Sciences* 5(3) 760-773.
- Al-Enezi Abdul-Majid Khalaf Mansour. (2013). Safeguards Limiting Pre-trial Detention in Kuwaiti Law and Their Compatibility with Article 9 of the International Covenant on Civil and Political Rights. *Journal of Law / Journal of Rights* 37(3).
- Shaimaa Alwan Hassan. (2024). Legal Challenges in Combating Cybercrimes. *Journal of Humanities and Natural Sciences* 5(10) 363-381.
- Abdulsalam Ahmed Abdullah Al-Ashqari. (2025). The Role of the Civil Judge in Evaluating and Managing Documentary Evidence. *Journal of Humanities and Natural Sciences* 6(12) 453-467.
- Abdulsalam Hussein Al-Enezi. (2014). Legal Guarantees for Defendants Accused of Terrorism-Related Crimes under International Conventions and Egyptian and Kuwaiti Legislation. *Journal of Law* 38(1).
- Adhraa Ahmed Issa Insaf. (2025). Legal Protection Afforded in Electronic Sales Contracts. *Journal of Humanities and Natural Sciences* 6(7) 599-620.
- Imad Ahmed. (2021). The Rights of the Accused During the Preliminary Investigation Stage. *Journal of Humanities and Natural Sciences* 3(8) 172-198.
- Fathi Rizkallah. (2024). Procedural Provisions for Electronic Judicial Notification: A Comparative Study of Egyptian Law No. 146 of 2019 (Amending Certain Provisions of the Economic Courts Law) Omani Law No. 125 of 2020 (Regarding the Simplification of Litigation Procedures) and the New UAE Civil and Commercial Procedures Law No. 42 of 2022. *Journal of Jurisprudential and Legal Research* 46(46) 1003-1103.
- Hussein Belhirsch. (2013). Restrictions Imposed on the Freedom to Manifest Religion or Belief: A Comparison between the International Covenant on Civil and Political Rights and Algerian Legislation. *Journal of Legal and Political Research and Studies* 3(1) 142-163.
- Bin Suwailem bin Mohammed Al-Alouni and Ziyad. (2024). The Validity of Electronic Documents Electronic Signatures and Electronic Correspondence as Evidence in Light of Islamic Jurisprudence and Saudi Judiciary: A Comparative Study of Saudi Egyptian Jordanian and Emirati Legal Systems. *Journal of the Faculty of Islamic and Arabic Studies for Girls in Damanhour* 9(2) 1069-1134.
- Law No. (175) of 2018 on Combating Information Technology Crimes – Arab Republic of Egypt.
- United Arab Emirates. (2022). Federal Decree-Law No. (38) of 2022 Concerning Criminal Procedures. Abu Dhabi: Official Gazette.
- United Arab Emirates. (2021). Federal Decree-Law No. (34) of 2021 Concerning Combating Rumors and Cybercrimes. Abu Dhabi: Official Gazette.
- United Arab Emirates. (1987). Federal Law No. (3) of 1987 Promulgating the Penal Code (and its amendments). Abu Dhabi: Official Gazette.