REVIEW ARTICLE

AJEE
ACCESS TO JUSTICE IN EASTERN EUROPE
Peer-reviewed Journal

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print)
ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

Review Article

DIGITAL EVIDENCE AS A MEANS OF PROOF IN CRIMINAL PROCEEDINGS IN THE UAE

Ayman Nawwaf Alhawawsheh*, Qusay Salman Alfalahi, Khaled Ramadan Soltan, Abdulghani Qasem Taher and Luma Ali Al Dhaheri

ABSTRACT

Background: *This paper addresses key issues related to the admissibility of digital evidence—a pivotal concern in modern legal proceedings. The use of such evidence is fraught with challenges, particularly due to the rapid technological changes and heightened concerns surrounding electronic data privacy. In the criminal justice system, these challenges can impact the admissibility of evidence, its presentation in trial, and the charging and resolution of cases.*

This study examines the difficulties of admitting digital proof before the UAE judiciary. Considering the trend towards the digital world as an alternative to the tangible world, interest is increasing in the extent of the authenticity and strength of the means of technical storage of information in proof, the importance of the authenticity of computer extracts, and the extent to which the legal system of proof can accommodate these new types of means of proving. The study concludes that, despite the difficulty in obtaining digital evidence and the necessity of providing certain conditions required for its acceptance, it often enjoys a higher degree of credibility than traditional forms of evidence due to its accuracy and scientific and technical nature. This article seeks to address these challenges and explore potential solutions.

Methods*: This paper adopts a legal-analytical methodology focused on the UAE's legal framework. It employs a descriptive-analytical approach, utilising content analysis to analyse legal texts. Specifically, it reviews the position of the UAE legislator on the use of electronic evidence and analyses the perspectives of legal scholars and judicial rulings related to the validity of electronic evidence in criminal proceedings.*

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

Results and Conclusions: *The analysis and comparison of relevant legal frameworks yielded several findings. Foremost, among these is the need for the judiciary to adapt to digital and electronic evidence, recognising its standalone evidentiary value—provided that the conditions of certainty, legitimacy, and integrity are met. Such evidence must also be subject to oral examination and accessible to all parties.*

Particular attention is paid to the Federal Decree Law No. (34) of 2021 on Combating Rumours and Cybercrimes, which affirms the validity of digital evidence in criminal proof by explicitly defining and recognising its probative value under Article 65. The study concludes that digital evidence has characteristics that distinguish it from physical evidence, and current procedural rules do not adequately regulate its proper treatment; it is currently considered a form of documentary evidence.

1 INTRODUCTION

Criminal evidence remains one of the greatest challenges facing authorities responsible for combating crime at all levels. This difficulty arises from the deliberate efforts of criminals to conceal their crimes and their identities to evade justice. However, technological progress has greatly contributed to uncovering many previously unsolved crimes, which in the past were shrouded in mystery and routinely recorded as committed by an unknown person.[1]

The objective of this study is to examine the concept of digital evidence and assess whether a legislative framework exists regarding its definition and the strength of proof. It also aims to evaluate the extent of the validity and strength of digital evidence before criminal courts in jurisprudence, legislation, and judicial practice, and to identify legislative trends across different legal systems. This is particularly important given the significance of digital evidence, which distinguishes it from traditional evidence. Its digital nature makes it especially significant in proving crimes involving computers or communication networks, as such evidence often requires decoding and translating magnetic or electrical signals into data and information related to the crime.[2]

As it is widely understood, evidence is an item or information that tends to establish the existence of a fact or make it probable. By one estimate, digital evidence is a factor in approximately 90% of criminal cases.[3] Evidence can take various forms, including witness testimony, documents, photographs, videos, voice recordings, DNA testing, or other

1 Farouk Al-Kilani, *Lectures on the Principles of Criminal Trials* (Dar Al Farabi 1985).

2 Jessica Smith, 'Criminal Evidence: Relevancy' in James M Markham, Jessica Smith and Shea Riggsbee Denning, *North Carolina Superior Court Judges' Benchbook* (UNC School of Government 2015).

3 Christa M Miller, 'A Survey of Prosecutors and Investigators Using Digital Evidence: A Starting Point' (2022) 6 Forensic Science International: Synergy 100296, doi:10.1016/j.fsisyn.2022.100296.

tangible objects. Nevertheless, not all evidence is automatically admissible in court. It must comply with the specific jurisdiction's rules of evidence.[4]

2 RESEARCH METHODOLOGY

The descriptive and analytical approach will be employed to examine the subject of the validity of proof in digital evidence. This will involve tracing relevant references from a variety of sources, including legislative texts, judicial rulings, academic books, and scientific dissertations. The study primarily focuses on the legal framework in the UAE and a Directive of the European Union Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings. A mixed-methods design is employed, combining both analytical and comparative approaches to assess amendments to the UAE Penal Code regarding indicators from a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence.

This process involves assigning thematic units to the respective articles on the UAE and the European Union, as well as comparative legal research. These methods are effective in revealing and interpreting legislative and jurisprudential changes. Data for the study are drawn from legal documents, including the UAE Penal Code and the ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings.

2.1. Objectives and Research Problem

Criminal proof through digital evidence is considered one of the most prominent aspects of modern legal systems, particularly in light of the increasing threat posed by cybercrime. Such crimes can result in extensive economic, financial, and security-related harm. The legislative position varies: while some recognise it as a legitimate and reliable proof of evidence, like other traditional evidence, others question its legal value. This study explores the growing importance of digital evidence in the context of proof in criminal proceedings. It aims to address the following key questions: What is the legal legitimacy of digital evidence? How is digital evidence treated under UAE legislation and judicial practice in criminal cases?

4 Vanshika Shukla, 'The Admissibility of Digital Evidence: Challenges and Future Implications' (2023) 9 Commonwealth Law Review Journal 464.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

3 THE CONCEPT OF DIGITAL EVIDENCE

3.1. The Concept of Digital Evidence in the European Union

Electronic evidence, as defined in paragraph 1(b) of the ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings,[5], refers to any evidence that exists in electronic form or is transmitted in electronic form at the time it is obtained. It is irrelevant whether the evidence was already stored electronically before the time of acquisition or became electronically stored as a result of the act of acquisition. For instance, image recordings taken by a criminal investigation department in criminal proceedings are thus considered electronic evidence, as they are stored in electronic form upon acquisition.

3.2. The Concept of Digital Evidence in the UAE

The UAE legislator explicitly addressed digital evidence in Federal Decree Law No. (34) of 2021 On Countering Rumours and Cybercrimes,[6] specifically in Article 1, where digital evidence is defined as any electronic information that possesses probative force or value and is stored, transmitted, extracted, or derived from computer sets, information networks, and similar sources.[7] Such evidence may be gathered and analysed using special technological devices or applications.[8]

By comparing the previous texts, it is evident that the UAE legislator[9] has settled the controversy over the validity of electronic evidence in criminal proceedings,[10] explicitly recognising it as a form of material evidence. The definition provided in the UAE legislation closely aligns with the European Union's conceptualisation. According to the Proposal for a Directive, evidence means any object, data, or information to be used to prove a fact in criminal proceedings (para. 1(a)).[11] The term "evidence" is thus very broadly defined.

5 ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings' (*European Law Institute (ELI)*, September 2020–May 2023) <https://www.europeanlawinstitute.eu/projects-publications/publications/eli-proposal-for-a-directive-of-the-european-parliament-and-the-council-on-mutual-admissibility-of-evidence-and-electronic-evidence-in-criminal-proceedings/> accessed 10 February 2025.

6 Federal Decree Law No (34) of 2021 'On Countering Rumors and Cybercrimes' [2021] Official Gazette of UAE 712.

7 Musa Masoud Arhouma, 'Procedural Problems Raised by Transnational Crime' (The First Maghreb Conference on Informatics and Law: Academy of Graduate Studies, Tripoli, 28-29 October 2009) 3.

8 John Ashcroft (ed), *Electronic Crime Scene Investigation: A Guide for First Responders* (US Department of Justice, Office of Justice Programs, National Institute of Justice 2001).

9 Federal Decree Law No (34) of 2021 (n 6) art 1.

10 Mhd Samer Al Kattan, 'Digital Justice "Model of the United Arab Emirates"' (2023) 18(1) Revista de Gestão Social e Ambiental 4-5, doi:10.24857/rgsa.v18n1-091.

11 ELI Proposal (n 5).

4 LEGAL FRAMEWORK FOR THE DIGITAL EVIDENCE IN THE EUROPEAN UNION AND UAE

4.1. The Legality Characteristic of Digital Evidence

Digital and informational evidence—considered a fundamental means of proving cybercrimes— raises many problems regarding its legitimacy and reliability, whether at the level of initial reports conducted by criminal investigation personnel or at the level of discussions that take place publicly and in the presence of the court. These challenges persist throughout all stages of the criminal process.[12]

4.2. The Judge's Freedom to Evaluate the Evidence

First, it is necessary to define the field or scope of this crime, as this is central to understanding the evidentiary framework. The scope of information crime is considered somewhat narrower than what has been approved by some jurisprudence. It primarily encompasses crimes where the subject matter involves information, data, or documents stored in computers, information systems, application programs, or related software. Whether the data is publicly available or confidential, certain conditions must be met. These include whether the perpetrator is qualified for this legitimate access—such as through authorised passwords—or gained entry through illegal methods such as hacking.

Cybercrimes often involve the alteration of data, disrupting its flow, rendering it temporarily or permanently unstable, or destroying it permanently, all with the aim of achieving certain goals.[13]

Notably, some criminal legislation has not assigned particular procedural distinctions to cybercrimes in terms of proof. Consequently, these crimes remain subject to the general principle of proof established in the penal article. Under this principle, the Public Prosecution may rely on any recognised legal means of proof to pursue the accused and defend them before the investigating judge and the court. Likewise, the accused may refute these charges by all means of proof.

The principle of freedom of proof also governs the discretion of the criminal judge, who is entrusted with the evaluation and assessment in each case.[14] The presumption of innocence guarantees that the burden of proof is borne by those who claim contrary to this principle. It would be contrary to this principle to require the defendant to prove their innocence, as they are presumed innocent until proven guilty.

12 Aman Vedwal, 'Admissibility of Digital Evidence for Cyber Crime Investigation' (School of Law, University of Petroleum & Energy Studies (UPES) 2023) 16, doi:10.2139/ssrn.4443356.

13 System Security Study Committee and others, *Computers at Risk: Safe Computing in the Information Age* (National Academy Press 1991).

14 Smith (n 2).

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

It follows from this that in the event of an inability to prove what was alleged with conclusive evidence, the criminal judge must acquit the accused, whose innocence is presumed. Moreover, even if evidence is presented in a case that the judge could not establish. His complete conviction in the crime attributed to the accused was due to the doubt that remained in his belief regarding it, because doubt is always interpreted in the interest of the accused.[15]

From the above, it can be said that if proving a crime means not only verifying its occurrence, but also attributing it to a specific person, then attribution requires that there be evidence proving that attribution or connection, and the evidence is within the scope of proving the crime and attributing it to a specific person in general, either it may be physical evidence, or it may be moral or verbal evidence, such as testimony and confession.[16]

To establish the principle of freedom of proof, crimes can be proven by any means of proof, except in cases where the law requires otherwise. The judge rules according to his deep conviction, and the decision must include what justifies the judge's conviction by stating all the factual and legal reasons on which it is based, even in the case of innocence. Therefore, nothing is preventing the criminal judge from relying, in convicting or acquitting the accused, on the various means of proof approved in the penal code, including digital evidence, about proving the commission of information crimes and attributing them to the persons being investigated for that purpose, if there is nothing explicitly preventing or indirectly resort to it.[17]

However, the multiplicity of forms, manifestations, and descriptions of information crime, which can take the form of an infringement on databases and data, the form of forgery and destruction of electronic documents, or the form of information fraud and deception makes it difficult to prove in most cases because there is no reliable material evidence or witnesses who can rely on it. Benefiting from their testimonies in this context, and from the high efficiency and skill that the perpetrators often possess in this field to hide their identities, mislead the monitoring authorities, and delete everything that might identify them or the method they used to penetrate an information system.

This requires members of the criminal investigation team charged with researching and investigating this type of crime to have enough skills and competencies in the areas of information systems and the Internet to obtain means of proof that guarantee the attribution of these crimes to their perpetrators. It also imposes on all judicial bodies involved in the dispute, from the Public Prosecution to the Judiciary. Investigation and

15 Osama Ahmed Al-Manaasah and Jalal Mohammed Al-Zoubi, *Information Technology Crimes: A Comparative Study* (Dar Althkafa 2022).

16 Ayman Nawwaf Alhawawsheh, 'Cybercrimes in the Kingdom of Saudi Arabia' (11th Cybercrime Conference, Jordan, Faculty of Law, Jerash University, 5-6 May 2015) 15.

17 ibid.

governance bodies must possess sufficient knowledge in this field so that they can follow up on perpetrators, hold them accountable, and impose the penalties stipulated by law.[18]

4.3. The Legal Framework for Digital Evidence in the European Union

To date, no uniform standard has been introduced by the EU legislator for harmonising domestic judicial procedures or establishing coherence within the EU's internal judicial order. Notably, the admissibility of e-evidence data in court is completely alien to the GDPR. Although the issue directly influences trial procedure, judicial impartiality, and potentially undermines the right to a fair trial, the GDPR provides no guidance.

Despite the absence of a harmonised admissibility framework at the EU level, national courts, in abiding by their domestic legal system, retain the discretion to determine whether the evidence obtained through illegal processes should be excluded.[19] In instances where a public body or law enforcement agency legally gathers sensitive data as evidence of an imminent threat to public interest or security, a clear-cut rule of law governs the matter.

However, legal complexity emerges in cases when such evidence is obtained illegally and both parties appear before a national court, each attempting to substantiate their claims through competing evidentiary submissions. In such scenarios, the judge should first decide the validity and authenticity of the data and then examine the substantive issues of the case. The position advanced in this research is that judicial determinations regarding the admissibility of e-evidence directly influence the EU's fundamental right to a fair trial.[20]

While EU legislation tends not to oversee the admissibility of e-evidence, the current stance of the European Court of Human Rights system reveals a much more practical approach. However, it is important to distinguish between the admissibility of evidence in domestic legal proceedings. The former is enshrined in Article 35 of the ECHR, which sets out the procedural criteria for a claim to be considered admissible by the Court.

To evaluate procedural irregularities, the ECtHR has established a test known as the "overall fairness" test. According to this test, the court must consider ten factors to determine the admissibility of evidence. The ten-factor test ensures that obtaining and presenting evidence at trial and procedural actions of domestic law enforcement do not jeopardise the accused's fundamental rights, notably the right to a fair trial (Article 6 ECHR).[21] Of these ten principles, the reasoning of judicial decisions, the principle of immediacy, legal certainty,

18 Al-Manaasah and Al-Zoubi (n 15).

19 Giulia Lasagni, 'Admissibility of Digital Evidence' in Vanessa Franssen and Stanisław Tosza (eds), *The Cambridge Handbook of Digital Evidence in Criminal Investigations* (CUP 2025) 126.

20 Oleksii V Kostenko and Vahid Akefi Ghaziani, 'Admissibility of Illegally Obtained e-Evidence: A Critical Study of EU law and the precedents of the European Court of Human Rights' (2024) 2 European Journal of Privacy Law and Technologies 205, doi:10.57230/EJPLT242OVKVAG.

21 Ibid 213.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

prejudicial publicity, and (requirements related to) plea bargaining face only minor challenges rooted in the digital nature of e-evidence and may, therefore, be set aside.[22]

The ECtHR does not evaluate the validity of each piece of evidence; such evaluations fall within the competence of national courts. Rather, the ECtHR exercises its judicial capacity only after the exhaustion of all domestic remedies.

By contrast, the position in the UAE presents a distinct legal approach. Article 210 of the UAE Code of Criminal Procedure, titled "Satisfaction of the Judge," provides that a judge shall adjudicate on the case based on their own satisfaction.[23] The basis of proof in criminal cases is the court's conviction and confidence in the evidence presented to it. The law does not restrict the criminal judge to specific evidence, but rather gives him absolute authority to form his belief from any evidence or indication presented to him.[24]

The ECtHR's jurisprudence in *Bykov v. Russia*[25] illustrates the complexities surrounding covert evidence-gathering operations. In that case, the Federal Security Service of the Russian Federation (FSB) orchestrated a covert operation involving a third party (V.) who was instructed to carry on a hidden radio-transmitting device to engage in a conversation with the applicant in a guesthouse where he was residing. During the encounter, V. initiated a discussion about an assassination plot with the applicant and falsely claimed to have already carried it out. In an effort to convince the applicant, V. showed him evidence linked to the victim, including a watch. Ending their chat, V. received a cash reward from the applicant, consistent with their prior arrangement. Upon exhausting domestic remedies, the applicant submitted a complaint to the ECtHR, which recognised that conducting covert listening constitutes a breach under Article 8 of the Convention.[26] However, the Court held that such a violation did not render the obtained evidence illegal. Provided the use of the evidence complied with the requirements of Article 6 (1), it could be deemed admissible. Finally, the court, concerning non-pecuniary damages, awards the applicant €1000—€118,089.25 lower than his request.[27]

In *Schenk v. Switzerland*,[28] the Court made a judgment concerning illegally intercepted calls in France, which had been forwarded to Swiss law enforcement authorities. Although the

22 Radina Stoykova, 'The Right to a Fair Trial as a Conceptual Framework for Digital Evidence Rules in Criminal Investigations' (2023) 49 Computer Law and Security Review 105801, doi:10.1016/j.clsr.2023.105801.

23 Federal Decree Law No (38) of 2022 'Promulgating the Criminal Procedures Law' [2022] Official Gazette of UAE 737.

24 Apps Nos 1006 and 1114 of 2023 (Abu Dhabi Court of Cassation (Crim), 26 December 2023).

25 *Bykov v Russia* App no 4378/02 (ECtHR, 10 March 2009) <https://hudoc.echr.coe.int/fre?i=001-91704> accessed 10 February 2025.

26 Kostenko and Ghaziani (n 20) 216.

27 Applicant claimed 4,059,061.80 Russian Roubles (119,089.25 euros) for both pecuniary and nonpecuniary damages. See, *Bykov v Russia* (n 25) para 108.

28 *Schenk v Switzerland* App no 10862/84 (ECtHR, 12 July 1988) <https://hudoc.echr.coe.int/eng?i=001-57572> accessed 10 February 2025.

ECtHR acknowledged that the interception lacked a legal basis, it concluded there was no evidence of a violation of Article 6 ECHR. Given the existence of other evidence, the use of illegal interception did not compromise the presumption of innocence or render the proceedings unfair.[29]

4.4. The Legal Framework for Digital Evidence in the UAE

Based on the principles of a fair trial, a court may not base its decision to convict an individual on any arguments or evidence that has not been presented and discussed orally during a public hearing. As such, the court must present and discuss all the evidence presented to it,[30] whether by the judicial police, the public prosecution service, or the civil claimant. In application of this, the Court of Cassation of the Emirates ruled:

"Given the text of Article (50) of the Law of Evidence in Commercial and Transactions and the text of Article 269 of the Code of Criminal Procedure - and on what the judiciary of this court has established - that the final criminal ruling issued acquitting the accused is based on the non-occurrence of the act. That which is attributed to the accused, or if the court doubts that it happened on his part, or that there is insufficient evidence against him - is the only one that has authority that the civil courts are bound by in cases that have not been decided by a final ruling and that are related to the subject of that criminal case, and the acquittal ruling based on the fact that the act attributed to the accused is not punished, or the absence of the elements of the crime does not have this authority before the civil courts, and this does not prevent them from examining the availability of evidence of the mistake and its attribution to the person who committed it, since the contested ruling concluded, about the subsidiary case, that it is not permissible to examine liability. The fifth respondent has erred in applying the law, and the appeal 1 on the ruling is unfounded."[31]

Notably, since the entry into force of Federal Decree Law No. (34) of 2021 on Combating Rumours and Cybercrimes, Emirati courts have demonstrated a cautious approach in relying solely on digital evidence derived. Although courts have discretionary authority to convict based on digital evidence—such as data extracted from the victim's computer, the accused's computer, information systems, or other digital evidence recorded in a judicial police report—they typically reinforce such evidence with one or several other "traditional" forms of evidence. These may include the accused's confessions, witness testimonies (for either the prosecution or the defence), or expert findings. Courts may also request that expert reports be supplemented—particularly when access to information from digital devices is obstructed. In the absence of adequate evidence or means of proof, the court must acquit the accused.

29 Stoykova (n 22) 8.

30 Smith (n 2).

31 App No 711 of 2011 (Abu Dhabi Court of Cassation (Crim), 18 October 2011).

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

Effectively combating this type of crime, therefore, requires preserving the rights and interests of those who pursue it. In all cases, legislative and judicial solutions must be sought to achieve a balance between the interests of the state in combating these extremely serious crimes and the interests of those accused of committing them, whose innocence must be presumed unless and until a judicial decision is issued against them with the force of res judicata.

The UAE legislator, under Article 65 of the Federal Decree Law and under the title of Validity of Evidence, stipulates that evidence derived or extracted from devices, equipment, media, electronic supports, information systems, computer programs, or any means of information technology constitutes authentic material forensic evidence in criminal proceedings.

It is observed that the legislator has, as an initial step, limited the provision to affirming the evidentiary authority of digital evidence. The law equates digital evidence with physical forensic evidence in terms of its evidentiary value for criminal proof. However, it is hoped that the Emirati legislator will further specify the conditions and controls related to the mechanism for obtaining such evidence, the techniques used, and the relevance of the evidence to the electronic crime in question. This includes the requirement that digital evidence be collected and stored by a competent judicial officer or by experts or specialists assigned by the investigative or trial authorities, the procedures for examining copies of the digital evidence and, where necessary, reviewing the original, and the documentation of digital evidence in official records prior to the examination by specialists. The record should include the location of seizure, the place of its storage, handling procedures, and the technical specifications of the evidence. This approach mirrors the one adopted by the Egyptian legislator.[32]

A question arises regarding the authenticity of evidence obtained by the prosecution to prove the accused's guilt, versus evidence obtained by the accused to prove their innocence.

Digital evidence extracted by the Public Prosecution has authority against the accused, provided it is obtained lawfully. However, the accused may, in some circumstances, rely on evidence even if it is not legitimate. The judge retains the discretionary rule to issue an acquittal if he is convinced of the accused's innocence despite the illegitimacy of the evidence. For example, if a judicial police officer (outside the cases of flagrant) inspects the accused's phone without obtaining permission from the Public Prosecution and compels the accused to reveal the password, any incriminating evidence found therein would be inadmissible due to the unlawful method of acquisition.

Conversely, if the accused relies on unlawfully obtained evidence—such as photographing someone without obtaining permission—to prove their innocence, the

32 Law No 175 of 2018 'Anti-Cyber and Information Technology Crimes Law' [2018] Official Journal of Egypt 32(C), art 11.

judge may consider the evidence, and if convinced, may rule in favour of acquittal despite the evidence's illegitimacy.[33]

In application of the aforementioned priciples, the UAE Court of Cassation ruled that when the court reviewed the case documents and the accused's plea to invalidate the evidence derived from recordings and photos taken from the accused's phone—allegedly obtained by the complainant—the accused's goal was to cast doubt on the legitimacy of the digital evidence derived from the recordings and photos.[34] The court held that this was an attempt to undermine consistent case evidence. The court unanimously found the appellant had committed the crime of promoting immoral consent as alleged in the case files. It concluded that the defence's objection amounted to nothing more than an objective controversy in the assessment of the evidence, which falls within the exclusive discretion of the court. The court was satisfied with the facts of the incident, the credibility of the incident, and the evidence presented therein, rendering the defence's objections meritless.[35]

In another case, the court reaffirmed that establishing criminal liability depends on the trial judge's conviction, which must be based on the evidence presented. The judge has the right to weigh the evidence and consider only those testimonies, confessions, and evidence that he is comfortable with, provided that the law does not restrict him to a specific piece of evidence.[36]

Moreover, it is established that if an arrest and search are conducted unlawfully, any conviction based on the resulting evidence is invalid. The ruling emphasised that no conviction can be based on evidence derived from such an unlawful search, including the testimony of the person who conducted it.

Finally, in another case, the court found that the conviction of the second accused—the appellant in the appeal at hand—was based on the testimony of law enforcement officers and the confession of the first accused. However, the court determined that the confession had been extracted through an illegal process. The first accused had admitted that the second accused had delivered drugs to him for sale and promotion. This confession prompted the police officers to request permission from the Public Prosecution to arrest and search the second accused. Since the arrest and search were based on unlawfully obtained evidence, they were deemed invalid—a matter concerning public order due to its connection with the legitimacy of the conviction. Consequently, all evidence derived from this unlawful procedure, including the testimony of the one who conducted it.

Given that the first accused's admission was the basis for the search and arrest, and that the ruling against the first accused had already been overturned due to the illegality of the evidence, the same reasoning applied to the second accused. The Court of Cassation held

33 App No 903 of 2022 (Abu Dhabi Court of Cassation (Crim), 7 November 2022).

34 App No 1030 of 2021 (Abu Dhabi Court of Cassation (Crim), 27 January 2022).

35 ibid.

36 App No 270 of 2008 (Abu Dhabi Court of Cassation (Crim), 27 January 2009).

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

that the judgment should be overturned for both parties, due to the shared basis of appeal, the unity of the incident, and the interest of justice. Accordingly, the appealed ruling was overturned and referred back, without the need to examine the grounds of appeal.[37]

4.5. Legitimacy Of Obtaining Electronic Evidence

The UAE legislator has stipulated the legitimacy of obtaining evidence in Article 73, titled Searching the Communications and Technical Means and Recording of Conversations. The provision stipulates:

> "1. The Prosecutor may seize, at the post offices, all correspondence, letters, papers, printed materials, and parcels, and, at the telegram offices, all cables. Furthermore, he may search the devices, networks, equipment, media, electronic supports, information systems, computer programs, or any technical means whenever the investigation so requires, or he may assign experts or specialists he deems appropriate to perform the same.
>
> 2. Subject to prior approval of the Attorney General, the Prosecutor may monitor and record the conversations, including wired and wireless communications. "[38]

A textual analysis of this article reveals that the method of obtaining the evidence must be legitimate. If it is not, any resulting ruling may be rendered invalid.

The UAE Court of Cassation has reinforced this principle, confirming that the trial court has the authority to understand the facts of the case, assess the evidence and accept expert reports as long as it is convinced of their credibility.[39]

In another case, it was ruled: "In this appeal, it becomes invalid, and it is a matter related to public order due to its connection to the legitimacy of the evidence of conviction, and all evidence derived from this invalid procedure is invalid, including the testimony of the person who conducted it and the confession of the first accused against him."[40]

If the only evidence supporting the claimant's conviction is found to be illegitimate during the Court's assessment, the doctrines of allowance and suppression represent differing viewpoints on the fairness of a trial. Suppose the sole evidence is the product of illegal government surveillance. In such cases, suppression could, in certain scenarios, undermine the public interest, especially when the alleged conduct poses a serious threat to public safety. In some cases, some might argue that excluding the evidence solely due to a procedural misstep, such as a warrant defect, allows a potentially dangerous individual to avoid accountability.

37 App No 142 of 2013 (Abu Dhabi Court of Cassation (Crim), 19 June 2013).
38 Federal Decree Law No (38) of 2022 (n 23).
39 App No142 of 2023 (n 37).
40 Apps Nos 1006 and 1114 (n 24).

It is also conceivable that the infringement of privacy may not be of particular interest to the accused, who nonetheless asserts his legal right to a fair trial in order to dismiss the case. However, if there is several evidence in a case and the first piece of evidence was obtained illegitimately, the second piece (correlated or irrelevant to the subject of the first) must be suppressed to protect the fundamental rights of the accused, provided there is no opposing public interest justifying its admission.

Moreover, courts should be careful to distinguish between the following orders in gathering supportive evidence. First, if legitimate-looking evidence stems from an illegitimate measurement or evidence which was itself a product of illegal action, all further evidence (no matter whether correlated to the first or not) must be disregarded by applying the exclusionary rule.

Nonetheless, some governments permit the admission of illegal evidence, even if it is obtained through an illegitimate route.[41]

5 DIGITAL EVIDENCE IN FOREIGN JURISDICTION (JOINT INVESTIGATION TEAMS)

Joint investigation team (JIT) represent one of the most advanced tools used in international cooperation in criminal matters. A JIT comprises a legal agreement between competent authorities of two or more States, enabling them to conduct criminal investigations. These teams typically include prosecutors, law enforcement authorities and judges, and are established for a fixed period—typically between 12 and 24 months—sufficient to carry out a specific investigation effectively.[42]

Under the auspices of Europol and Eurojust, several JITs have been set up to support cross-border investigations. These joint investigations allow for an efficient way of collecting and sharing electronic evidence pertinent to an investigation. However, experience has shown that further development of a common European framework is necessary to increase the legal certainty needed for such joint investigations to be carried out more smoothly and efficiently.[43]

In the UAE, the legislature stipulated provisions for International Judicial Cooperation in Criminal Matters.[44] However, this law has a legislative vacuum regarding the exchange of

41 Kostenko and Ghaziani (n 20) 210.

42 'A Joint Investigation Team (JIT)' (*European Union Agency for Criminal Justice Cooperation*, 2025) <https://www.eurojust.europa.eu/judicial-cooperation/instruments/joint-investigation-teams> accessed 10 February 2025.

43 Jeanne Pia Mifsud Bonnici, Melania Tudorica and Joseph A Cannataci, 'The European Legal Framework on Electronic Evidence: Complex and in Need of Reform' in Maria Angela Biasiotti and others (eds), *Handling and Exchanging Electronic Evidence Across Europe* (Law, Governance and Technology Series 39, Springer 2018) 222, doi:10.1007/978-3-319-74872-6_11.

44 Federal Law No (39) of 2006 'Concerning International Judicial Cooperation in Criminal Matters' [2006] Official Gazette of UAE 457.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

digital evidence, even among the Gulf Cooperation Council (GCC) countries. While instances of cooperation and joint investigations with other countries do occur, these are not codified.[45] Here, it is recommended that the UAE legislator consider adopting aspects of the Europol and Eurojust model, particularly regarding the exchange of digital evidence at the international level.[46]

6 CONCLUSION

The article concludes that the adoption of the EU e-evidence rules is an important step toward enhancing joint efforts in the fight against crime. Fundamentally relying on the principle of mutual trust among EU Member States and the presumption of their compliance with Union law, the rule of law, and fundamental rights and values, the application of the e-evidence package will nonetheless require constant scrutiny, monitoring, and cooperation among all involved actors.[47]

It is imperative that the UAE and the Gulf Cooperation Council (GCC) countries draw upon the European Parliament's experience, particularly the ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings.

This study offers several suggestions and recommendations, emphasising that comparative legislation should explicitly recognise digital evidence as valid in criminal proceedings and grant it conclusive probative value—as a justified exception to the criminal judge's discretion in evaluating evidence. Legislators are encouraged to follow the example of the Emirati legislator by including provisions that ensure the integrity of digital evidence as a prerequisite for its admissibility. It is also recommended to explicitly permit the search and seizure of content from virtual environments by amending the criminal procedure laws to reflect the appropriate tools of proof for such crimes. Furthermore, it is essential to define the conditions that digital evidence must meet—particularly the requirement of legality—for it to be accepted in proving or disproving cybercrime.

45 For instance , Abu Dhabi Police sent two teams to the United Kingdom, as per the higher leadership's directives, following the shocking assault on the Emirati nationals (Ohoud, Khuloud and Fatima). A first team from the Criminal Investigation Department (CID) was dispatched to follow up on the case and the criminal investigations, in cooperation with the British authorities. The second team, from the Social Support Centers Department, was in charge of providing psychological support to the victims of this tragic accident.

46 Bayazid Hossain, 'Digital Evidence in Foreign Jurisdiction and Quality of Justice' (2023) 1 ELCOP Journal on Human Rights 143, doi:10.59871//SFGB7594.

47 Adam Juszczak and Elisa Sason, 'The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice: An Introduction to the New EU Package on E-evidence' [2023] 2 EUCRIM: Electronic Evidence 182, doi:10.30709/eucrim-2023-014.

For evidence to be admissible in criminal proceedings, it must be relevant, material, and competent. This standard applies to court proceedings in civil cases as well. To be relevant, evidence must reasonably help prove or disprove some fact. The degree to which this evidence increases or decreases the likelihood of the fact influences the weight the judge gives it.

It is recommended that the UAE legislator adopt the experience of Europol and Eurojust regarding the exchange of digital evidence at the international level, and codify the treatment of digital evidence obtained in foreign jurisdictions to enhance the quality of justice.

REFERENCES

1. Al Kattan MS, 'Digital Justice "Model of the United Arab Emirates"' (2023) 18(1) Revista de Gestão Social e Ambiental e04945, doi:10.24857/rgsa.v18n1-091.
2. Alhawawsheh AN, 'Cybercrimes in the Kingdom of Saudi Arabia' (11th Cybercrime Conference, Jordan, Faculty of Law, Jerash University, 5-6 May 2015).
3. Al-Kilani F, *Lectures on the Principles of Criminal Trials* (Dar Al Farabi 1985).
4. Al-Manaasah OA and Al-Zoubi JM, *Information Technology Crimes: A Comparative Study* (Dar Althkafa 2022).
5. Arhouma MM, 'Procedural Problems Raised by Transnational Crime' (The First Maghreb Conference on Informatics and Law: Academy of Graduate Studies, Tripoli, 28-29 October 2009).
6. Ashcroft J (ed), *Electronic Crime Scene Investigation: A Guide for First Responders* (US Department of Justice, Office of Justice Programs, National Institute of Justice 2001).
7. Hossain B, 'Digital Evidence in Foreign Jurisdiction and Quality of Justice' (2023) 1 ELCOP Journal on Human Rights 143, doi:10.59871//SFGB7594.
8. Juszczak A and Sason E, 'The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice: An Introduction to the New EU Package on E-evidence' [2023] 2 EUCRIM: Electronic Evidence 182, doi:10.30709/eucrim-2023-014.
9. Kostenko OV and Ghaziani VA, 'Admissibility of Illegally Obtained e-Evidence: A Critical Study of EU law and the precedents of the European Court of Human Rights' (2024) 2 European Journal of Privacy Law and Technologies 205, doi:10.57230/EJPLT242OVKVAG.
10. Lasagni G, 'Admissibility of Digital Evidence' in Franssen V and Tosza S (eds), *The Cambridge Handbook of Digital Evidence in Criminal Investigations* (CUP 2025) 126.
11. Mifsud Bonnici JP, Tudorica M and Cannataci JA, 'The European Legal Framework on Electronic Evidence: Complex and in Need of Reform' in Biasiotti MA and others (eds), *Handling and Exchanging Electronic Evidence Across Europe* (Law, Governance and Technology Series 39, Springer 2018) 189, doi:10.1007/978-3-319-74872-6_11.

12. Miller CM, 'A Survey of Prosecutors and Investigators Using Digital Evidence: A Starting Point' (2022) 6 Forensic Science International: Synergy 100296, doi:10.1016/j.fsisyn.2022.100296.
13. Shukla V, 'The Admissibility of Digital Evidence: Challenges and Future Implications' (2023) 9 Commonwealth Law Review Journal 464.
14. Smith J, 'Criminal Evidence: Relevancy' in Markham JM, Smith J and Denning SR, *North Carolina Superior Court Judges' Benchbook* (UNC School of Government 2015).
15. Stoykova R, 'The Right to a Fair Trial as a Conceptual Framework for Digital Evidence Rules in Criminal Investigations' (2023) 49 Computer Law and Security Review 105801, doi:10.1016/j.clsr.2023.105801.
16. Vedwal A, 'Admissibility of Digital Evidence for Cyber Crime Investigation' (School of Law, University of Petroleum & Energy Studies (UPES) 2023) doi:10.2139/ssrn.4443356.

AUTHORS INFORMATION

Ayman Nawwaf Alhawawsheh*
PhD (Law), Professor in Criminal Law, Faculty of Law, American University in the Emirates, Dubai, United Arab Emirates
ayman.alhwawsheh@aue.ae
https://orcid.org/0000-0002-0356-1896
Corresponding author, responsible for research methodology, data curation, investigation, and writing- original draft.

Qusay Salman Alfalahi
PhD (Law), Professor, College of Law, American University in the Emirates, Dubai, United Arab Emirates
qusay.alfalahi@aue.ae
https://orcid.org/0000-0002-8609-3150
Co-author, responsible for conceptualization, formal analysis, validation, writing-original draft.

Khaled Ramadan Soltan
PhD (Law), Associate Professor in Criminal Law, College of Sharia and Law, Imam Malik College, Dubai, United Arab Emirates.
k.ramadan@imc.gov.ae
https://orcid.org/0000-0001-5995-1597
Co-author, responsible for research methodology, data curation, investigation, writing-original draft.

Abdulghani Qasem Taher
PhD (Law), Assistant Professor in Criminal Law, Faculty of Law, Umm Al Quwain University, Umm Al Quwain, United Arab Emirates.
drabdulghani.m@uaqu.ac.ae
https://orcid.org/0000-0003-3659-4640
Co-author, responsible for research methodology, data curation, investigation, writing-original draft.

Luma Ali Al Dhaheri
PhD (Law), Associate Professor, College of Law, American University in the Emirates, Dubai, United Arab Emirates
luma.aldahery@aue.ae
https://orcid.org/0000-0003-4826-5123
Co-author, responsible for research methodology, data curation, investigation, writing-original draft.

Competing interests: No competing interests were disclosed.

Disclaimer: The authors declare that their opinion and views expressed in this manuscript are free of any impact of any organizations.

RIGHTS AND PERMISSIONS

EDITORS

ABOUT THIS ARTICLE

Cite this article
Alhawawsheh A, Alfalahi Q, Soltan K, Taher A and Dhaheri L, 'Digital Evidence as a Means of Proof in Criminal Proceedings in the UAE' (2025) 8(3) Access to Justice in Eastern Europe 1-20 <https://doi.org/10.33327/AJEE-18-8.3-a000111> Published Online 18 Jul 2025

DOI: https://doi.org/10.33327/AJEE-18-8.3-a000111

Keywords: *digital evidence, admissibility, proof, legitimacy, cybercrime.*

DETAILS FOR PUBLICATION

Date of submission: 12 Feb 2025
Date of acceptance: 20 May 2025
Online First publication: 18 Jul 2025
Whether the manuscript was fast tracked? - No
Number of reviewer report submitted in first round: 2 reports
Number of revision rounds: 1 round with major revisions

Technical tools were used in the editorial process:
Plagiarism checks - Turnitin from iThenticate https://www.turnitin.com/products/ithenticate/
Scholastica for Peer Review https://scholasticahq.com/law-reviews

АНОТАЦІЯ УКРАЇНСЬКОЮ МОВОЮ

Оглядова стаття

ЦИФРОВІ ДОКАЗИ ЯК ЗАСІБ ДОКАЗУВАННЯ В КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ В ОАЕ

Айман Навваф Альгававше*, Кусай Салман Альфалагі, Халед Рамадан Солтан, Абдулгані Касем Тагер та Лума Алі Аль Дагері

АНОТАЦІЯ

Вступ. *У цій статті розглядаються ключові питання, пов'язані з допустимістю цифрових доказів, що становить основну проблему сучасного судочинства. Використання таких доказів супроводжується низкою труднощів, зокрема через стрімкий розвиток технологій та зростаючу стурбованість питаннями конфіденційності електронних даних. У системі кримінального правосуддя ці виклики можуть впливати на допустимість доказів, порядок їх подання в суді, висунення обвинувачень та вирішення справ.*

У цьому дослідженні розглядаються труднощі, пов'язані з прийняттям цифрових доказів у судовій системі ОАЕ. З огляду на тенденцію до переходу до цифрового світу як альтернативи матеріальному, зростає інтерес до ступеня автентичності та надійності засобів технічного зберігання інформації в процесі доказування, важливості автентичності комп'ютерних витягів і того, наскільки правова система доказування здатна пристосуватися до цих нових видів засобів доказування. У дослідженні зроблено висновок, що, незважаючи на труднощі в отриманні цифрових доказів та потребу в забезпеченні певних умов, необхідних для їх прийняття, цифрові докази часто користуються вищим ступенем довіри, ніж традиційні форми доказів, завдяки своїй точності та науково-технічному характеру. Метою цієї стаття є вирішення цих проблем та дослідження потенційних рішень.

Методи. *У цій роботі застосовується юридично-аналітична методологія, що зосереджена на правовій базі ОАЕ. Також у статті використовується описово-аналітичний підхід, здійснюється аналіз юридичних текстів за допомогою контент-аналізу. Зокрема, було розглянуто позицію законодавця ОАЕ щодо використання електронних доказів, проаналізовано погляди вчених-юристів та судові рішення, пов'язані з допустимістю електронних доказів у кримінальному процесі.*

Результати та висновки. *Аналіз і порівняння відповідних нормативних актів дали підстави для низки висновків. Серед них, перш за все, є необхідність адаптації судової системи до цифрових та електронних доказів, визнання їх самостійної доказової сили – за умови дотримання правової визначеності, законності та цілісності. Такі докази також повинні підлягати усному дослідженню та бути доступними для всіх сторін.*

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

Особлива увага приділяється Федеральному декрету-закону № (34) від 2021 року «Про боротьбу з чутками та кіберзлочинністю», який підтверджує достовірність цифрових доказів у кримінальному доказуванні, чітко визначаючи їхню доказову силу відповідно до статті 65. У дослідженні також було зроблено висновок, що цифрові докази мають характеристики, які відрізняють їх від матеріальних доказів, а чинні процесуальні норми не регулюють належного поводження з ними; наразі вони розглядаються як різновид документальних доказів.

Ключові слова: *цифрові докази, допустимість, доказування, легітимність, кіберзлочинність.*