AI-ENABLED MISCONDUCT AND CORPORATE CRIMINAL LIABILITY IN ARAB JURISDICTIONS: OFFENCE DESIGN, EVIDENCE, AND CROSS-BORDER ENFORCEMENT

Mohammad Airout *

* Department of Law, Faculty of Law, Middle East University, Amman, Jordan
Contact details: Department of Law, Faculty of Law, Middle East University, P. O. Box 11831, Amman, Jordan

How to cite this paper: Airout, M. (2026). AI-enabled misconduct and corporate criminal liability in Arab jurisdictions: Offence design, evidence, and cross-border enforcement. *Corporate Law & Governance Review, 8*(1), 34–45.
https://doi.org/10.22495/clgrv8i1p3

ISSN Online: 2664-1542
ISSN Print: 2707-1111

Received: 20.08.2025
Revised: 18.11.2025; 18.12.2025
Accepted: 05.01.2026

JEL Classification: K14, K22, O33
DOI: 10.22495/clgrv8i1p3

Abstract

The research examines the regulation and enforcement of corporate criminal liability in artificial intelligence (AI) facilitated illegal activities in the five Arab countries UAE, Saudi Arabia, Jordan, Egypt, and Morocco. The study assesses the cumulative effect of company law, governance structures, cybercrime laws, and rules of evidence on the processes of attribution, supervision, and accountability with regard to technology crime. Using a triangulation research methodology that combines doctrinal analysis with qualitative analysis and quantitative analysis, this paper compares Arab laws with those in the European Union (EU), the USA, Singapore, and Italy to argue that there are divergent rules on corporate liability; that there is no significant recognition of the use of compliance programs as sentencing factors; and that there are lax rules on managing digital evidence and neuroscience evidence across national borders. The paper recommends the use of criminal risk management by company boards in Arab countries to mitigate these challenges and provides legislative measures that will codify crimes committed by AI technology; improve evidence management processes; and standardize enforcement across national borders (Morshed, 2025a).

Keywords: Corporate Criminal Liability, Board Oversight, Compliance Programs, Digital Evidence, AI-Enabled Crimes, MENA–Jordan

Authors' individual contribution: The Author is responsible for all the contributions to the paper according to CRediT (Contributor Roles Taxonomy) standards.

Declaration of conflicting interests: The Author declares that there is no conflict of interest.

1. INTRODUCTION

The continued rapid pace of developments in the areas of artificial intelligence (AI), neuroscience, and digital forensics is significantly influencing the very core ideas of criminal law — and the constructs of accountability, intentionality, and evidentiary reliability in particular. Notwithstanding the initial efforts emanating from various international regimes like the European Union (EU), the USA, and Singapore to respond to the challenge of wrongdoing through the use of AI, deepfakes, algorithmic manipulation, and various new developments in neuroscience (Lin, 2025), the Arab States' legal frameworks are still in their nascent stages. This is occurring at a point in time where the digital transition in the Arab region's major sectors of the economy is also gaining momentum.

Among the five Arab countries studied in this research — the UAE, Saudi Arabia, Jordan, Egypt, and Morocco — the five do not represent one single legal system. Saudi Arabia's Sharia-based system relies on the concepts of *niyyah* (intent) and moral

accountability. Egypt's system in place is the civil-law system in combination with strictly defined "offences in the penal code". The UAE's system combines civil law with common law procedural systems. Meanwhile, the system in place in Jordan integrates the components of the Ottoman system with the French system. Thus, the five Arab countries recognize different methods in the attribution of responsibility on "legal persons", the delineation of "digital crimes", as well as the evaluation of "novel types of evidentiary technologies". Nevertheless, the five countries recognize common weaknesses in the processes related to "cybercrimes", "neuroscientific evidence", and "cross-border digital enforcement".

The purpose of the research is to assess how the five Arab countries treat crimes facilitated by the use of AI technology, the handling of neuroscientific proof, and cross-jurisdictional digital enforcement. By examining the structural ambiguities in the definition and procedures regarding corporate crime responsibility in the Arab countries against the backdrop of international best practices in corporate crime regulation through the use of computational tools for analyzing texts, the research combines different disciplinary streams in an investigation of the ability of the Arab criminal justice system to process technology-related wrongdoing.

This research is very important both for scholarly discussion in the field of law and for the practical implementation of corporate governance. Without specific legal regulation on the issue of crimes related to intelligence technologies, the admissibility of neuroscience in courts, and the transfer of digital evidence within the Arab region's framework of governing laws, the uncertainty for business entities in the region escalates concerning the risks of exposure to crimes committed through intelligence technologies. Thus, the challenge for comprehensive improvement in the deterrence of cybersecurity threats in corporate crime through intelligence technologies becomes very vital.

From the outcomes of the research, it is indicated that all five countries have the problem of under-specification in the context of AI-related offenses, the lack of uniform safeguards for the presentation of neuroscientific evidence, and structural barriers to international digital collaboration. Through the computational analysis that was performed for the research work, the degree of lexical density in the context of terms related to AI and neuroscience is low. Moreover, semantic disparity in the term "digital evidence" exists (Ahmed et al., 2025). There is no significance in alignment with the best international practices.

The rest of the paper is structured as follows. Section 2 reviews the literature on crimes made possible by AI technologies. Section 3 explores the research methodology. Section 4 highlights the results. Section 5 interprets the outcomes. Section 6 concludes the paper, describing the theoretical and practical contributions.

2. LITERATURE REVIEW

Criminal law is struggling to keep pace with AI-facilitated offences, neuroscientific evidence, and cross-border digital enforcement. Although these issues have been examined in depth in the EU, the USA, and Singapore, the Arab region remains comparatively understudied despite the rapid diffusion of sophisticated technologies into policing and court practice (Taylor et al., 2025). The effect — observed in various regimes — is that there is always a delay between law and technology, with resultant gaps in regulation and frictions in evidence that strain due process guarantees (Morshed, 2025a). Within Arab regimes, there is emphasis on technology-neutral cybercrime laws, the use of neuroscientific evidence is negligible in evidentiary laws, and regimes struggle with international enforcement mechanisms in cybercrime laws in terms of practicality, though there is membership in cybercrime treaties (Alkhafagy et al., 2023). Within the corporate arena, these tendencies are placed in perspective to show that uncertainties within offence definition, evidence admissibility, and cooperation procedure impact corporate entity attribution, board responsibilities, and programme requirements.

2.1. AI-enabled crimes and digital offences

The application of artificial intelligence has expanded the means of criminal acts — ranging from deepfakes to fraudulent activities and cyber-attacks — so that companies are more vulnerable to such threats and internal control measures are more complex (Morshed & Khrais, 2025). To mitigate these threats, advanced countries have adopted laws that are aimed at prohibiting the use of harmful artificial intelligence content (Feldstein, 2024), and there seems to be an understanding that cybercrime laws are no longer sufficient to curtail the impact of artificial intelligence.

Instead, most Arab countries stick to wide-ranging and technology-agnostic criminal laws (for example, UAE, Saudi Arabia, and Jordan), which include illegal access, fraud, and harmful content in digital technology but rarely identify risk factors and responsibility parameters that are appropriate to multi-agent autonomous computer systems (Al-Dulaimi & Mohammed, 2025; Munro et al., 2024). In corporate environments with distributed authority and tasks among human and computing entities, such an issue moves responsibility to the courts after the event has taken place, with no clear proactive standard to be met by company boards and compliance departments. Parallel debates over predictive policing and algorithmic decision-making warn that bias and opacity can migrate into enforcement itself, creating additional due-process and human-rights risks when automated tools influence arrest, charging, or sentencing (Yang et al., 2024). Together, these trends underscore the need to specify AI-enabled offences, clarify entity-liability pathways, and articulate governance-grade safeguards for algorithmic decision-making in Arab jurisdictions (Salhab et al., 2025).

2.2. Neuroscience-based evidence in criminal law

Neuroscience is increasingly present within criminal proceedings through the use of functional magnetic resonance imaging (fMRI), electroencephalography (EEG) analysis, and neuroprediction technologies that are influencing claims about guilt, intention, and risk (Paraschiv et al., 2024). Its use has been advocated as potentially improving accuracy and fairness; there are concerns about "brain overclaim syndrome" with regard to validity and methodology, as well as questions about the compatibility with criminal notions of responsibility (Petoft et al., 2023). Within the Arab zone, such evidence is almost absent, and whatever there is has no codified procedures; there are no rules within criminal procedural legislation about the admissibility and weight to be accorded to such evidence (Bhriguvanshi et al., 2025). In Sharia and mixed regimes, there are also concerns about criminal notions of intention (*niyyah*) and liability (Gaffar & Al Mamari, 2024).

For companies, these gaps impact internal investigations, personnel matters, and employees' rights in the areas surrounding neuro-tools and privacy and proportionality. In the absence of regulation to fall back on, the rules that determine admissibility are left to the courts' discretion, perpetuating inconsistency in the standards and principles surrounding admissibility (Hussein & Al-Obeidi, 2023). Historical evidence within comparators' jurisdictions implies that there have to be technical criteria for admissibility and regulatory safeguards that ensure alignment with constitutional rights (Ribeiro Daquila, 2024). Governance has to ensure that there are higher-level safeguards with regard to the use, management, and contesting of neuro-evidence.

2.3. Cross-border enforcement and digital evidence

The transnational nature of cybercrime has made the need for reliable and predictable e-evidence exchange all the more critical. Tools such as the Budapest Convention and the 2024 United Nations (UN) Convention on Cybercrime aim to standardize Mutual Legal Assistance processes and mitigate conflict-of-laws difficulties (Shams, 2026). The need to implement such processes has proved challenging due to divergent national laws on evidence and sovereignty concerns (Richmond et al., 2024).

In Arab countries, collaboration relies on the Convention on Combating Information Technology Crimes and various bilateral and multilateral agreements. But here again, there are discrepancies between the intentions and reality on the ground, with lingering e-crime reporting, unpreparedness in digital-forensic analysis to immediately respond to e-crime investigations and requests due to apprehension about sharing sensitive data without adequate safeguards (Al-Rai et al., 2024). The experiences cited in various empirical research reports include use of various sectoral and personal networks to expedite the process (Al Makhmari et al., 2024), but due to these uncertainties, there are unpredictabilities in forward-looking approaches to forensics readiness in corporate entities such as multinationals with cloud technology; there are therefore no platforms anticipated to make enforcement straightforward (El-Kady, 2025).

2.4. Comparative and interdisciplinary insights

Comparative scholarship within the EU, the USA, and Asian models demonstrates that addressing AI-facilitated crimes and neuroscience applications depend on certain types of statutory formulation, strong procedural guarantees, and specialization (Lin, 2025). Though technology neutrality facilitates flexibility in drafting laws, it tends to result in inconsistent applications of this new area of cyber wrongdoing and scientific evidence (Rajković, 2024). Within the Arab countries, the question of transplants in law considers the advantages of alien innovations and staying true to indigenous traditions such as Islamic law and constitutional provisions.

Interdisciplinary research integrates law-and-technology studies, criminology, and computational law. Criminology examines the impact of AI-based law enforcement technology on prevention, though with concerns about proportionality and bias (Raji & Sholademi, 2024). Computational research applies natural language processing (NLP) and semantic techniques to empirically identify gaps in definition and unclear concepts within legislative texts, making possible scalable and verifiable assessments that supplement qualitative analysis (Wolniak et al., 2024). From the perspective of corporate entities, research implications are found in the area of governance design that combines compliant processes, audit trails, and data management policies with prosecutorial requirements (Morshed, 2025a).

2.5. Identified gaps, conceptual framework, and hypotheses development

This leads to three areas that are left uncovered. Firstly, Arab criminal laws are technology agnostic with regard to AI-related crimes and entity-liability attribution left to the courts' discretion. Secondly, neuroscience has almost no representation in rules on evidence and tends to be inconsistent in terms of admissibility and safeguards. Thirdly, transnational enforcement varies significantly in that there are official documents in place; however, delays and sovereignty issues raise concerns about rights-compliant e-evidence transfers in corporate cases (Morshed & Ramadan, 2023).

The conceptual framework thus integrates aspects such as doctrinal mapping, comparative benchmarking, and computer-aided analysis of legal texts to relate substantive offenses to evidence rules (digital and neuroscientific), as well as enforcement mechanisms within the socio-legal context that is sensitive to innovations, rights protection, and the divergent Arab traditions.

The research hypotheses are as follows:

H1: AI-crime provisions in Arab jurisdictions are less specific and adaptive than in comparator systems, increasing reliance on judicial interpretation.

H2: The absence of codified rules on neuroscientific evidence in Arab jurisdictions yields inconsistent admissibility and limited procedural safeguards.

H3: Cross-border digital enforcement in the Arab region is less efficient and harmonized than under instruments such as the Budapest and 2024 UN Cybercrime Conventions.

H4: Combining computational text analysis with doctrinal and comparative methods reveals gaps and inconsistencies that traditional legal analysis alone would miss.

So, what for corporate criminal liability, across all strands — AI offences, neuroscience, and cross-border e-evidence — the literature indicates a need to codify entity-liability pathways, link effective compliance programs to mitigation, and specify forensic-readiness and evidence-transfer standards that boards can operationalize.

3. RESEARCH METHODOLOGY

3.1. Research design

The unit of analysis is criminal, evidentiary, companies law, and cooperation provisions as they govern corporate entities, boards, officers, and compliance programs in technology-mediated offences. The study uses a qualitative, triangulated design: 1) doctrinal analysis of black-letter law; 2) comparative benchmarking; 3) computational (Arabic/English) legal text analysis. Jurisdictions: UAE, Saudi Arabia, Jordan, Egypt, Morocco; benchmarks: EU, UAE, Singapore, Italy. Corpus: in-force, consolidated statutes and binding regulations (criminal/cybercrime; evidence/ procedure; companies/governance; anti-money laundering/anti-bribery and corruption (AML/ABC) if incorporated; cooperation instruments), plus published higher-court decisions; frozen 30 June 2025. Doctrinal extraction targets: AI-offence coverage, entity-liability pathways, digital/neuroscientific evidence standards, forensic-readiness duties, and cross-border mechanisms. The bilingual NLP pipeline yields five indices — AI-specificity, entity-liability clarity, evidence safeguards, forensic readiness, and cross-border operability — supporting most-similar systems comparisons in the Middle East and North Africa (MENA) and targeted benchmarking externally. Quality assurance: structured codebook; dual-coding of a stratified sample (Cohen's $k \geq 0.75$); robustness checks (bilingual vs. English-only, soft-law exclusion, lexicon sensitivity, leave-one-out). Limitations: operability measured via textual proxies; legal change post-freeze noted (Blackham, 2022).

To execute the above-stated research design triangulation, these computer results are converted to an index form consisting of five values (0–5) to enable visual analysis and facilitate comparison. These results evidence accuracy and process efficacy within the laws of jurisdiction, whereby computational results are incorporated with doctrinal analysis (Morshed, 2025a). Table 1 below presents a pilot analysis to reflect variability in Arab laws and the flexibility within customized models.

Table 1. Illustrative index scores for legal responsiveness (0–5 scale)

Jurisdiction	*AI-specificity*	*Entity-liability clarity*	*Evidence safeguards*	*Forensic readiness*	*Cross-border operability*
UAE	2.5	2.0	1.5	2.0	2.0
Saudi Arabia	2.0	1.5	1.0	1.5	1.0
Jordan	2.5	2.5	1.5	2.0	2.0
Egypt	3.0	2.5	2.0	2.5	2.5
Morocco	3.0	2.0	1.5	2.0	2.0

These results are in line with the expectations and confirm the existence of convergence between the results of the doctrinal analysis and computational analysis approaches, thus emphasizing the validity and reliability of the mixed-methods strategy.

3.2. Doctrinal legal analysis

The core interpretive stage assesses the regulation of AI-facilitated crimes, neuroscience evidence admissibility rules, and international law enforcement in the concerned Arab countries. This normative stage explains the current state of the law and its coherence and deficiencies with respect to the advancement of technology (Mitchell, 2023). The normative stage acts as the structured legal foundation for the rest of the research study components.

The primary sources are criminal codes, cybercrime laws, criminal procedure laws, and rules on evidence in the UAE, Saudi Arabia, Jordan, Egypt, and Morocco; as are accessible, appellate/supreme court decisions are also reviewed. The collection also includes company/corporate governance documents to the extent that they set criteria for directing board monitoring and compliance functions pertinent to criminal risk. The Arab Convention on Combating Information Technology Crimes, the UN Convention on Transnational Organized Crime, and most recently approved 2024 UN Cybercrime Convention are reviewed with respect to cooperation and e-evidence requirements. Doctrinal analysis is supplied through peer-reviewed scholarship and secondary reports. The collection is finalized with respect to 30 June 2025; subsequent changes are referenced to indicate limitations.

The process entails intensive readings in legislation and international instruments to identify definitions, categorizations, and processes that are then interpreted in terms of purposes to establish legislative intention and coverage (Dhali et al., 2023). Particular emphasis is placed on those areas that are silent, vague, and contradictory with respect to AI-aided behavior, neuroscientific evidence, and transboundary digital processes (Shiyyab & Morshed, 2024).

"This stage provides in-depth 'legal maps' that set out the current state of law in each jurisdiction on key matters arising in the research". For example, while the UAE Cybercrime Law no. 34 of 2021 has made harmful cyber content illegal through Article 22, it has failed to include AI-created content within that legislation, contrary to Singapore's legislation — Protection from Online Falsehoods and Manipulation Act (2019).

3.3. Comparative legal analysis

During this stage, there is a systematic comparison with UAE-SKCC-APCC provisions and international best practices (EU, USA, Singapore, and Italy)

through the application of the three pillars above. Convergence, divergences, and transplanted best practices are determined to ensure that Arab laws are placed within the new international normative foundations and that there is also conformity with international requirements (Alkouatli, 2024).

The five Arab countries that were chosen in terms of legal and economic heterogeneity and digital governance plans are the UAE, Saudi Arabia, Jordan, Egypt, and Morocco. These countries are to be compared with international best practices such as the European Union (AI Act and eEvidence), the USA (Texas State Bill 20 on AI-generated content), Singapore (OFMA), and Italy (neuroscientific evidence law).

A comparative-functional analysis evaluates the treatment of common techno-legal challenges by various regimes, focusing on corporate bodies and the role of boards and compliance regimes. The thematic analysis is conducted in relation to the following axes: 1) criminalization of AI-related activities; 2) treatment of neuroscientific evidence; 3) international cybercrime law enforcement (mutual legal assistance and simplified e-evidence sharing). Methodologically, this analysis evaluates substantive (definition of crimes and entity attribution models) and procedural (admissibility rules and due process rules) matters to highlight areas of convergence and divergent practices to be transplanted to enable regional-level reforming (Wang et al., 2024).

This step produces a map indicating the degree to which Arab normative systems converge with and diverge from international best practice. The results form the basis for reform hypotheses outlined within subsection 3.5 and ascertain that similar reform is possible without violating constitutional and process requirements.

3.4. Computational legal text analysis

At this stage, there is the incorporation of technology to facilitate analysis of the law. In contrast to doing research through the doctrinal method and comparative approaches that are carried out manually without the use of technology, computer-based approaches are particularly useful in areas such as AI-offences and neuroscience evidence that are steadily evolving with new terminology and models (Contini et al., 2024).

The corpus consists of primary legislation such as criminal codes, criminal procedure codes, cybercrime laws, and rules on evidence from the UAE, Saudi Arabia, Jordan, Egypt, and Morocco; as well as regional and international treaties pertinent to e-evidence and cooperation. Benchmark documents include the EU AI Act itself, state-level AI content legislation in the USA, deepfakes law in Singapore, and provisions on neuroscientific evidence in Italy. Sources are taken from official gazettes and official websites; metadata also details enactments and amendments. The Arabic-language documents are processed to be machine-readable with translations to English; these are double-checked within documents to ensure terminological consistency. Corporate governance documents are included if they contain board responsibilities pertinent to criminal liability. The corpus is indexed to changes no later than 30 June 2025; post updated to reflect current accuracy as a limitation.

NLP techniques are employed, involving tasks such as tokenization, lemmatization, and stop-word removal. Named Entity Recognition identifies concepts in law, technology terms, and process types. Keyword analysis examines the correlation between terms such as “artificial intelligence”, “deepfake”, “neuroimaging”, and “digital evidence”. Semantic similarities in models that use multi-lingual word vectors evaluate definitions across various laws with variations in definition and meaning (Mumcuoğlu et al., 2021).

To better illustrate this difference, the search term “artificial intelligence” was found only 18 times within the five Arab countries’ bodies of law combined, while it was found 212 times in the USA and European corpora with operative verbs such as “liability,” “transparency,” and “risk management” accompanying it. The neuroscientific terms “fMRI,” “EEG”, and “neuroprediction” did not occur within the Arab set of evidentiary codes at all, which confirms what is true within the traditions.

These results provide quantitative maps of the density of legal terms, coincidence graphs, and comparison graphs to show the divergences in definition. Triangulation verifies that those countries with lower AI specificity and evidence safeguards are linked with lower lexical density in significant statutes. Doctrinal analysis, comparison mapping, and data mapping act as validation mechanisms to increase trust and improve transparency (Mitchell, 2023; Contini et al., 2024).

3.5. Normative-prescriptive framework development

In this stage, there is an integration of results that come from the doctrinal analysis, comparison analysis, and computational analysis to produce comprehensive and coherent recommendations. The stage seeks to bridge the gap that exists between the present shortcomings and requirements that are needed to make criminal law Arab-world compliant and adaptive (Scherlis, 2023).

The model combines thematic results derived from previous stages. Doctrinal analysis results include areas that lack provisions in laws covering crimes in relation to AI technology, science, and international enforcement. Comparative analysis results include novel models derived from laws of other countries. Results include areas that are statistically deficient within the definition of laws.

Draft legislation to criminalize the use of harmful AI-generated content, allow neuroscientific evidence within scientific validity requirements, and change rules regulating international cooperation for digital evidence transfer (Romero Moreno, 2024).

Guidelines on judicial interpretations that ensure technological flexibility without undermining the constitutional provisions and teachings of Islamic law (Yue et al., 2023).

Procedural guidance that ensures protection from biased algorithms, proportionality in investigative measures, and transparency in the use of AI technologies by the law.

The proposals are international best practices (including the United Nations Office on Drugs and Crime [UNODC] guidance and Council of Europe instruments) and are tested against Arab League model laws to facilitate regional harmonisation. They are stress-tested by means of hypothetical “what if” simulations with regard to 1) AI-related crimes, 2) neuroscience evidence within criminal

proceedings, and 3) e-evidence Mutual Legal Assistance (MLA) requests. They are tested on criteria that include legality, due process requirements, operational workability, and governance considerations.

3.6. Ethical and data considerations

The research strictly adheres to universally accepted ethical principles in law studies and only uses publicly accessible laws and authentic documents. Therefore, there are no potential threats to personal data and privacy concerns. The legislative documents are applied with utmost accuracy and adhere to strict categorization between the authentic legislative documents and the interpretations obtained from them (Doyle et al., 2022).

The data that supports every law — every statute, every international treaty, every court opinion — is taken straight from these authoritative sources and preserved in encrypted data management environments that are strictly controlled (Morshed, 2025b). The machine-ready formats are retained in original form and translation form to guarantee accuracy with respect to every machine-derived output (Morshed, 2025c, 2025d). Further, there are metadata holdings to trace the origin and history with respect to each piece (Eke et al., 2022).

The study adheres to all copyright laws and data protection provisions in each country. When there are reproduction constraints, only permitted excerpts are taken. Computer analysis is carried out only with corpora that are accessible over the internet and are compliant with all international standards on intellectual property rights.

The entire process from data collection to analysis has been documented. The partial results from computations (frequency results and similarity results) are placed in an archive to make them accessible to other people during peer review. The blending of methodologies has been clearly explained to ensure that every recommendation can be linked to its evidence (Ştefan, 2024).

Other techniques might also be used in the same study. Sometimes, research on the same topic might involve the use of various methods, like the socio-legal research approach that uses interviews. This research approach might highlight the workings of the different AI-related crimes, the effect of neuroscience in courts, and cross-jurisdictional processes. Also, the comparative approach might involve the coding of various statutes in order to provide numerical representation in the specificity of the crime. Additionally, the research might also involve the use of the doctrinal approach. This might involve the consideration of higher court judgments. However, the approach that was used in the research study is the most applicable one.

4. RESULTS

4.1. Overview of results

Based on doctrinal, comparative, and computational analysis approaches, results include those that concern crimes facilitated by artificial intelligence technology, neuroscience-based evidence, and the enforcement thereof across the UAE, Saudi Arabia, Jordan, Egypt, and Morocco within the corporate law and governance perspective.

Doctrinal mapping reveals that AI-related activities are governed by technology-neutral cybercrime laws, neuroscience evidence that is uncodified in rules of evidence, and international cooperation that is operationalized inconsistently — factors that introduce uncertainties with regard to the board's oversight role, internal controls/forensic readiness measures, and use of compliance-as-a-means-of-mitigation defenses in corporate cases. A comparative analysis with the EU, USA, Singapore, and Italy follows in terms of the lack of laws' specificity and enforcement with regard to entity attribution methodologies, evidence admissibility and chain-of-custody requirements, and provider cooperation requirements.

These results are supported by computational analysis that finds areas in which there are gaps within current AI and neuroscience terminology and semantic inconsistencies that impede "governance grade" clarity. Overall, the results expose conceptual, procedural, and definitional gaps that limit legal effectiveness and corporate predictability, motivating the reform blueprint on board responsibilities, compliance criteria, forensic-readiness standards, and e-evidence cooperation set out next.

4.2. Doctrinal analysis findings

4.2.1. AI-enabled crimes

Across all five Arab jurisdictions, AI-related conduct is addressed through broad, technology-neutral cybercrime provisions (e.g., unlawful access, digital fraud, dissemination of harmful content) rather than AI-specific offences (such as deepfake creation, algorithmic manipulation, or autonomous cyber intrusions). In the absence of tailored definitions and attribution rules for multi-actor, automated environments, enforcement defaults to judicial interpretation, producing variable outcomes and limited legal certainty in cases involving complex algorithmic processes. For corporate defendants, this under-specification leaves entity-liability pathways (identification, vicarious or "failure-to-prevent" analogues) unclear, weakens ex-ante incentives to implement AI-focused internal controls and compliance programmes, and complicates forensic readiness (logging, model/version provenance, audit trails) necessary to establish or rebut attribution (Abdelaziz, 2025).

4.2.2. Neuroscience-based evidence

Neuroscientific methods (fMRI, EEG, neuroprediction) are uncodified within the evidentiary laws in the five Arab countries and are admitted (or excluded) on a case-by-case basis, as the discretion of the court dictates whenever these technologies come to court. In the current state of indeterminable terms of admissibility — validity, reliability, relevance, limits to scope, and proportion to privacy — the outcome intended by judicial deliberation varies unpredictably between premature admission without safeguards and blanket exclusion of relevant science. Corporate implications: there are no predictable rules within internal investigations to

introduce — let alone contest — neuro-adjacent opinions; there are no foundations within corporate audit bodies to base policies on consent, data management, and challenge rights; and there are no predictable rules within litigation planning to reflect the weight to be accorded to such evidence (Perkins et al., 2023).

4.2.3. Cross-border enforcement

A set of legal bases to facilitate collaboration has been established — primarily through the Arab Convention on Combating Information Technology Crimes and various bilateral/multilateral mutual legal assistance treaties (MLATs) — but there are challenges in the enforcement process, such as delays in mutual legal assistance requests, sovereignty concerns, and the capacity to analyse evidence to facilitate the exchange of e-evidence.

The inconsistency affects corporate entities as MNCs cannot develop predictive approaches to managing data location and data preservation; board governance and corporate efforts to comply are left without clear expectations with regard to collaboration, timelines, and data format and translation; data analysis readiness (log retention and chain-of-custody analysis) is also negatively impacted due to potential threats to litigation and law enforcement (Al-Kasassbeh et al., 2024).

4.3. Comparative analysis findings

4.3.1. Alignment with benchmark jurisdictions

Compared with the EU, the USA, Singapore, and Italy, the selected Arab jurisdictions show partial alignment on generic cybercrime prohibitions but diverge markedly in precision, procedural safeguards, and adaptability to emerging technologies. Benchmark systems have targeted provisions for AI-generated harms (e.g., EU AI Act interfaces; Singapore's deepfake regime), structured admissibility standards for neuroscience, and streamlined cross-border e-evidence mechanisms. By contrast, Arab frameworks rely on broad, technology-neutral clauses with few explicit references to AI-specific threats or neuroscientific tools, reducing comparability and interoperability with global models. Corporate implications: under-specification blurs entity-attribution pathways, decouples effective compliance programmes from mitigation credit, and leaves admissibility/chain-of-custody thresholds for digital/neuro evidence uncertain; it also frustrates provider-cooperation and data-location planning. Boards, therefore, lack determinate oversight benchmarks and forensic-readiness requirements, increasing enforcement and litigation risk for corporate defendants (Romero Moreno, 2024).

4.3.2. Transferable best practices

Drawing on benchmarks, the EU's risk-based AI regime and harmonised digital-investigation safeguards can be localised to codify board-level AI-risk oversight, require logging/retention/audit trails, and tie effective compliance programmes to mitigation credit; the USA practice on explicit criminalisation of AI-generated harms and neuroscience-evidence protocols would clarify entity-attribution and set predictable admissibility/chain-of-custody standards for corporate investigations; Singapore's rapid, tech-specific updates (e.g., deepfake rules and provider-cooperation duties) would harden incident-response service level agreements (SLAs) and cross-border forensic readiness; and Italy's jurisprudential integration of neuroscience within existing safeguards offers a template for HR/internal-investigation policies (consent, proportionality, data handling, challenge rights). Adapted to constitutional, Sharia, and procedural contexts, these elements would close definitional and procedural gaps while giving boards and compliance functions determinant standards for AI-risk governance, evidence handling, and e-evidence cooperation (Kokolaki & Fragopoulou, 2025).

4.4. Computational legal text analysis findings

4.4.1. Corpus characteristics

The compiled corpus comprised in-force, consolidated primary legislation — penal codes, criminal-procedure statutes, cybercrime laws, and evidentiary rules — together with companies/corporate-governance instruments allocating board and compliance duties, across the UAE, Saudi Arabia, Jordan, Egypt, and Morocco; relevant regional treaties and international instruments were also included. Benchmark texts (the EU AI Act, selected USA state AI-content statutes, Singapore's deepfake provisions, and Italian rules on neuroscientific evidence) were incorporated for cross-reference. All sources were obtained from official gazettes, government/regulator portals, and verified legal databases; enactment/amendment metadata were recorded. Materials were converted to machine-readable format (optical character recognition [OCR] where required), and Arabic texts were translated into English with back-checks for terminological consistency. For replicability, the corpus was frozen on 30 June 2025 (Ligthart et al., 2023).

4.4.2. Lexical and semantic patterns

Keyword-frequency analysis of the bilingual corpus shows sparse and inconsistent use of AI-specific terminology across Arab statutes: tokens such as "artificial intelligence", "deepfake", and "algorithmic decision-making" appear rarely and often in non-operative contexts, while neuroscience terms (e.g., "neuroimaging", "EEG", "fMRI", and "neuroprediction") are virtually absent. By contrast, collocation networks in benchmark jurisdictions exhibit dense linkages between technology terms and operative evidentiary/procedural predicates (e.g., admissibility, reliability, chain-of-custody, expedited preservation). For corporate actors, this weak lexical signal reduces governance-grade clarity — blurring entity-attribution pathways for AI-enabled misconduct, decoupling effective compliance programmes from mitigation criteria, and leaving forensic-readiness and provider-cooperation duties under-specified — thereby undermining comparability and cross-border operability (Romero Moreno, 2024).

4.4.3. Definitional and semantic gaps

Semantic-similarity analysis shows cross-jurisdictional drift in core terms — e.g., "digital evidence" varies in scope and predicates — complicating cross-border cooperation and admissibility. Several sets of best-practice definitions (again, particularly those that are AI-related) do not formally correlate to direct statutory provisions within Arab-language documents, indicating the tendency to sub-specify topics that fall within the realm of twenty-first-century technologies and the failure to use harmonious terminology. In the case of entities operating within these bodies' corporate, such terminological diversification affects Shadow Chinformatics pathway attribution and further detracts from readiness and planning within MLAT and e-evidence processes as measures reflective of effective planning to foresee forensic-readiness on the part of providers (Chiara, 2022).

4.5. Integrated findings

The confluence of the strands of doctrinal rules, comparison, and computation identifies that there is a pattern of underspecification, fragmented processes, and mismatches in definition with regard to regulating AI-powered crimes, neuroscience-based evidence, and international enforcement in the five Arab countries.

From the doctrinal perspective, national models ensure the fundamental cybercrime laws and MLA rules but do not define AI crimes, exclude neuroscience considerations from evidence statutes, and use international instruments inequitably. As regards businesses, these result in ambiguous entity attribution processes, poor correlation between credible compliance and mitigation measures, and vague standards with regard to forensic preparedness (system logging and preservation) and provider cooperation.

Comparatively speaking, best practices (EU/US/Singapore/Italian models) distinguish themselves through AI-specific policies, rules of admissibility (including neuroscientific evidence), and standardized e-evidence rules. The conflict puts Arab models behind the "global curve" compared to baselines that change with technology and denies Arab Oversight Boards' "determinative" oversight markers (for example, "Compliance-as-Mitigant" thresholds, and "chain of custody" integrity requirements), the legal mandate necessary to govern the issues of admissibility, and liability apportioning.

In computational terms, the sparse use of terms from AI and neuroscience and a semantic shift in key terms such as "digital evidence" obstructs the sharing of data predictably across international boundaries and within internal company investigations.

In combination, loose-worded legislation acknowledges and perpetuates process weaknesses. These results form the basis of the reform agenda below to codify board-level risk management review for AI and e-evidence exchange mechanisms in terms that ensure that each recommendation is context-appropriate (Dosad, 2024; Yang et al., 2024).

4.6. Reform-relevant insights

Introduce AI-specific offenses and the concept of entity attribution. Going beyond technology-neutral provisions to proscribe AI-facilitated crimes such as deepfakes and algorithmic manipulation, as well as autonomous hacking. A harmonized terminology among Arab countries will increase homogeneity in interpretation and facilitate international cooperation.

Codify neuroscience admissibility with governance safeguards. Integrate validity/reliability criteria, relevance, proportionality, and privacy concerns within the boundaries set by fMRI/EEG/neuro-prediction (NP) tests. Set parameters pertinent to corporate investigations (consent and data management rights), within the constructs outlined by constitutional law and Islamic and due-process tenets. Operationalise cross-border e-evidence. Translate treaty commitments into practice by legislating expedited preservation, direct-to-provider orders, time limits, format/translation standards, and reciprocity. Couple this with capacity upgrades in digital forensics and provider-cooperation SLAs to improve timeliness and integrity of evidence for multinational matters.

Embed compliance and board oversight in statute. Tie effective compliance programmes (risk assessment, policies, monitoring, remediation) to mitigation/sentencing credit; codify board-level AI-risk oversight and enterprise forensic-readiness duties (logging, retention, audit trails, incident playbooks). This creates ex-ante incentives and predictable ex-post evaluation criteria for corporate defendants.

Localise with legitimacy. Import proven mechanisms from benchmark systems only as adapted to domestic constitutional constraints, Sharia-based reasoning, and procedural architecture. The aim is legal certainty and institutional confidence while preserving normative coherence at home and enabling meaningful access to global enforcement networks.

5. DISCUSSION

Focusing on the corporate perspective, it is clear that the outcome shows that AI-facilitated criminality, neuroscientific evidence, and international electronic evidence are conditionally mediated by statutory design choices that distribute the liability to entities, define attribution within entities, and construct evidence architecture for entity cases. Regarding the five Arab countries, the doctrinal analysis ensures that the current tendency to include technology-neutral cybercrime laws instead of applying offence-specific clauses to deepfakes, algorithmic manipulation, and autonomous hacking is understood (Al-Dulaimi & Mohammed, 2025). Instead, these drafts defer corporate liability to post-judicial adjudication (identification or attribution models), rather than applying pre-judicial corporate governance to map violation factors to enforcement responsibilities. In other words, unlike other models in the EU and the USA that include AI-offense drafts with clear charging uncertainty and standardised assessments if companies are charged (Feldstein, 2024; Kokolaki & Fragopoulou, 2025), computational analysis verifies

that there is little AI lexicon and poor co-occurrence to liability terms in Arabic models, suggesting that AI-Specificity and Entity-Liability Clarity are low and that *H1* holds true.

The evidential aspect follows the same trend. In line with Bhriguvanshi et al. (2025) and Petoft et al. (2023), there are no codified rules on the admissibility of fMRI images, EEG signals, and neuroprediction within the surveyed regimes; instead, courts' discretion is here to stay. In other regimes, such as Italy and the USA, these types of evidence are integrated with systematic measures within the safeguards of reliability and proportionality (Paraschiv et al., 2024). In corporate law, the lack thereof diminishes the evidential role of neuro-related variables in favor of court discretion. The results of computational analysis reflect the slight use of neuroscience terms within Arab legislation to reinforce *H2*.

At the transnational level, the e-evidence chain operability still faces challenges. The sovereignty challenges and frictions in the process persist (Alkhafagy et al., 2023; Al Makhmari et al., 2024). In terms of expedited preservation requests, direct provider requests, and deadlines that are binding and thus enforceable in the Arab context compared to other documents such as the Budapest Convention and the 2024 UN Cybercrime Convention, Arab computer networks are still deficient. Semantic drift analysis in "digital evidence" confirms *H3*. Methodologically, the integration of NLP results with doctrinal and comparative analysis adds to probative force. First, NLP identifies definition lacunae and poor term-predicate connections that are inaccessible to traditional analysis (Wolniak et al., 2024; Mumcuoğlu et al., 2021), while doctrinal anchors identify the requisite legal effect (Romero Moreno, 2024). The overlap between low rates of lexical density and lower index values in AI-specificity, safeguards, and operability confirms *H4*. Taking all findings together, there emerge risks to governance if there are no AI-specific offenses, mitigation-of-compliance clauses, neuroscience criteria for admissibility, and operable e-evidence solutions.

6. CONCLUSION

This study advances theory at the intersection of criminal law, technology, and corporate liability in four ways.

First, by triangulating doctrinal, comparative, and computational analysis, it shows how technology-neutral drafting interacts with attribution to legal persons, clarifying where offence architecture fails to encode organisational responsibility for AI-enabled conduct. Second, it demonstrates the analytic payoff of a hybrid legal method: operational constructs (e.g., AI-specificity, evidentiary safeguards, cross-border operability) translate black-letter texts into reproducible measures, yielding a template for evaluating statutory responsiveness in rapidly digitising systems. Third, it contributes to harmonisation theory by evidencing that legal interoperability depends not only on formal commitments but also on semantic alignment — that is, the presence of shared definitions and stable vocabularies for digital evidence, AI conduct, and novel scientific proof. Fourth, it re-situates neuroscience within corporate proceedings as an evidentiary design problem, emphasising how the absence of codified admissibility criteria destabilises the treatment of scientific inputs in cases involving legal persons. Collectively, these contributions enrich comparative criminal-law scholarship with a governance-aware account of how text structure organisational exposure in technology-mediated offences.

The results carry immediate consequences for legal and institutional practice.

For legislators: move from general cybercrime clauses to AI-specific offence definitions and explicit attribution pathways for legal persons (including due diligence and failure-to-prevent models); codify admissibility standards for neuroscientific evidence (validity, reliability, proportionality, privacy); and embed cross-border operability tools (expedited preservation, direct-to-provider orders, time limits, format/translation standards) alongside harmonised terminology.

For judiciaries and prosecutors: issue practice directions and gatekeeping checklists for digital and neuroscientific materials; promote consistent articulation of chain-of-custody, proportionality, and reliability tests; and align charging practice with any AI-specific provisions to reduce ex post interpretive variance.

For regulators and corporate actors: articulate board-level oversight of AI and digital evidence; tie effective compliance programmes to enforcement incentives; and institutionalise forensic readiness (logging, retention, audit trails, incident playbooks, provider-cooperation protocols) to support a predictable evidentiary posture in domestic and cross-border matters.

This paper evaluated how the five Arab countries, UAE, Saudi Arabia, Jordan, Egypt, and Morocco, treat the issue of AI-supported criminal behavior, the admissibility of neuroscientific evidence, and cross-boundary digital enforcement in the context of corporate criminal responsibility. By triangulating the methodology on doctrinal research analysis, comparative benchmark analysis, and computational analysis of the texts, the study highlighted the substantive and procedural areas influencing entity responsibility.

The key results highlight that the five countries are highly dependent on technology-neutral cybercrime laws that do not clearly provide for the regulation of harms within the context of AI. Neuroscientific evidence is uncodified and subject to judicial discretion despite the lack of safeguards for relevance, proportionality, and privacy. International digital law enforcement also continues to encounter structural barriers in terms of sovereignty issues, the speed of mutual legal assistance treaties, the lack of harmonized language, and the absence of digital forensics capabilities. These results are also supported by computational analysis that indicates the low usage of terms in the areas of AI and neuroscience research, a semantic shift in the core concept of the definition "digital evidence", and low alignment with international standards.

Implications from the foregoing research outcomes cut across theoretical, practical, and policy aspects. Firstly, from the theoretical perspective, the research proves the adequacies of the formally enacted legal interoperations in the emerging

technologies arenas in being contingent on the semantic consistency of definitional clarity. Henceforth, the research work succeeds in translating core concepts like AI specificity, evidentiary safeguards, and cross-border operability. Thirdly, from the practical viewpoint, the research work clearly indicates the importance of having adequate structures within corporate boards, compliance officers, and supervising agencies to effectively respond to risks in the field of AI. Finally, from the policy perspective, the research work clearly reinforces the importance of explicitly criminalizing misconduct specific to the field of AI research.

Despite its contributions, the study also has some limitations. Firstly, the study is based on the in-force statutes and regulations current as of 30 June 2025. Any subsequent developments may shift the landscape. Secondly, the study does not involve any empirical research, such as interviews or surveys, the results of which might provide a different perspective on how the courts and enforcement agencies deal with these provisions. Thirdly, the computational analysis of the texts may highlight the semantic aspects but may not provide the same context on the implicit traditions of interpretation and the prosecutorial discretion on the corporate liability in technology-related cases.

There are various ways in which future research might capitalize on the shortcomings outlined in the literature. Socio-legal research consisting of interviews with prosecuting counsel, judges, and in-house compliance officers might help distill how crimes related to AI and the exploitation of digital evidence manifest during the course of investigations. Comparative research encompassing more Arab, African, and Asian countries might refine the universality of index measures used in the course of the research. Additionally, future research might also investigate the degree to which simulation dossiers related to regulation impact might fortify the usage efficiency of corporate regulation through the implementation of neuroscience regulations or the use of evidence. In conclusion, the report points to the importance of far-reaching reform efforts aimed at giving effect to AI-related crimes, the structures for entity liability, the place of neurological proof within secure frameworks, and the implementation of digital forms of cooperation. These efforts are crucial in the effort to improve the accountability of the business world, the clarity of the law, as well as its receptiveness to the digital age.

REFERENCES

Abdelaziz, D. K. A. (2025). Criminal liability for the misuse and crimes committed by AI: A comparative analysis of legislation and international conventions. *Journal of Infrastructure, Policy and Development, 9*(1), Article 10722. https://doi.org/10.24294/jipd10722

Ahmed, S., Khan, M. F., Singh, B., Singh, N., & Sharma, B. (2025). Enhancing crime scene analysis: The impact of AI technologies on evidence processing. In C. Kaunert, A. Raghav, K. Ravesangar, & B. Singh (Eds.), *Forensic intelligence and deep learning solutions in crime investigation* (pp. 63–84). IGI Global Scientific Publishing.

Al Makhmari, M., Al-Hammouri, A., Al-Billeh, T., & Almamari, A. (2024). Criminal liability for misuse of social media in Omani and UAE Legislation. *International Journal of Cyber Criminology, 18*(2), 92–106. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/420

Al-Dulaimi, A. O. M., & Mohammed, M. A.-A. W. (2025). Legal responsibility for errors caused by artificial intelligence (AI) in the public sector. *International Journal of Law and Management*. https://doi.org/10.1108/IJLMA-08-2024-0295

Al-Kasassbeh, F. Y., Awaisheh, S. M., Odeibat, M. A., Awaesheh, S. M. A., Al-Khalaileh, L., & Al-Braizat, M. (2024). Digital human rights in Jordanian legislation and international agreement. *International Journal of Cyber Criminology, 18*(1), 37–57. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/318

Alkhafagy, T., Nazem, S. N., Farhan, A. F., Salman, S. D., Khudadad, A. M., Nsaif, A. D., Gatafa, A. A., Sabti, A. A., & Abdelhassan, M. I. (2023). Cybercrime and inheritance legislation in Iraq: Extension of perspectives on inheritance legislation within Iraq. *International Journal of Cyber Criminology, 17*(2), 63–76. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/188/70

Alkouatli, C. (2024). Illuminating data beyond the tangible: Exploring a conceptually-relevant paradigmatic frame for empirical inquiry with Muslim educators. *International Journal of Qualitative Studies in Education, 37*(8), 2466–2484. https://doi.org/10.1080/09518398.2024.2318301

Al-Rai, A. F., AlOmran, N. M., & Al Ansari, M. A. J. (2024). The crime of digital promotion of terrorism through digital platforms and new media: A comparative study of Jordanian and Emirati laws. *International Journal of Electronic Governance, 16*(4), 453–467. https://doi.org/10.1504/IJEG.2024.144636

Bhriguvanshi, A., Leader, H., Sun, X., & Rojtman, A. (2025). Neurobrucellosis mimicking brain tumor in a pediatric patient: A Case Report. *Journal of Child Neurology*. https://doi.org/10.1177/08830738251356669

Blackham, A. (2022). When law and data collide: The methodological challenge of conducting mixed methods research in law. *Journal of Law and Society, 49*(S1), 87–104. https://doi.org/10.1111/jols.12373

Chiara, P. G. (2022). The IoT and the new EU cybersecurity regulatory landscape. *International Review of Law, Computers & Technology, 36*(2), 118–137. https://doi.org/10.1080/13600869.2022.2060468

Contini, F., Ontanu, E. A., & Velicogna, M. (2024). AI accountability in judicial proceedings: An actor–network approach. *Laws, 13*(6), Article 71. https://doi.org/10.3390/laws13060071

Dhali, M., Hassan, S., & Subramaniam, U. (2023). Comparative analysis of oil and gas legal frameworks in Bangladesh and Nigeria: A pathway towards achieving sustainable energy through policy. *Sustainability, 15*(21), Article 15228. https://doi.org/10.3390/su152115228

Dosad, M. (2024). *Understanding ambiguity in statutory language and its impact on judicial interpretation*. https://doi.org/10.2139/ssrn.5033910

Doyle, E., Frecknall-Hughes, J., & Summers, B. (2022). Ethical reasoning in tax practice: Law or is there more? *Journal of International Accounting, Auditing and Taxation, 48*, Article 100483. https://doi.org/10.1016/j.intaccaudtax.2022.100483

Eke, D. O., Bernard, A., Bjaalie, J. G., Chavarriaga, R., Hanakawa, T., Hannan, A. J., Hill, S. L., Martone, M. E., McMahon, A., & Ruebel, O. (2022). International data governance for neuroscience. *Neuron, 110*(4), 600–612. https://doi.org/10.1016/j.neuron.2021.11.017

El-Kady, R. (2025). Challenges of criminal liability for artificial intelligence systems. In H. Bajraktari (Ed.), *Exploration of AI in contemporary legal systems* (pp. 1–42). IGI Global Scientific Publishing. https://www.igi-global.com/chapter/challenges-of-criminal-liability-for-artificial-intelligence-systems/365941

Feldstein, S. (2024). Evaluating Europe's push to enact AI regulations: How will this influence global norms? *Democratization, 31*(5), 1049–1066. https://doi.org/10.1080/13510347.2023.2196068

Gaffar, H., & Al Mamari, S. (2024). From Roman law to Sharia: Comparative perspectives on the evolution of quasi-contracts in Western and Islamic jurisdictions. *Griffith Law Review, 33*(3), 209–234. https://doi.org/10.1080/10383441.2025.2487728

Hussein, S., & Al-Obeidi, A. (2023). Robotics and AI systems: Legal personality for AI system under UAE Law and Islamic jurisprudence. In *2023 24th International Arab Conference on Information Technology (ACIT)* (pp. 1–8). IEEE. https://doi.org/10.1109/ACIT58888.2023.10453710

Kokolaki, E., & Fragopoulou, P. (2025). Unveiling AI's threats to child protection: Regulatory efforts to criminalize AI-generated CSAM and emerging children's rights violations. *arXiv.* https://doi.org/10.48550/arXiv.2503.00433

Ligthart, S., Ienca, M., Meynen, G., Molnar-Gabor, F., Andorno, R., Bublitz, C., Catley, P., Claydon, L., Douglas, T., Farahany, N., Fins, J. J., Goering, S., Haselager, P., Jotterand, F., Lavazza, A., McCay, A., Wajnerman Paz, A., Rainey, S., Ryberg, J., & Kellmeyer, P. (2023). Minding rights: Mapping ethical and legal foundations of 'neurorights'. *Cambridge Quarterly of Healthcare Ethics, 32*(4), 461–481. https://doi.org/10.1017/S0963180123000245

Lin, L. S. F. (2025). Organisational challenges in US law enforcement's response to AI-driven cybercrime and deepfake fraud. *Laws, 14*(4), Article 46. https://doi.org/10.3390/laws14040046

Mitchell, M. (2023). Analyzing the law qualitatively. *Qualitative Research Journal, 23*(1), 102–113. https://doi.org/10.1108/QRJ-04-2022-0061

Morshed, A. (2025a). Navigating tradition and modernity: Digital accounting and financial integration in family-owned enterprises in the Arab Gulf. *Sustainable Futures, 9*, Article 100680. https://doi.org/10.1016/j.sftr.2025.100680

Morshed, A. (2025b). Cultural norms and ethical challenges in MENA accounting: The role of leadership and organizational climate. *International Journal of Ethics and Systems, 41*(3), 630–656. https://doi.org/10.1108/IJOES-08-2024-0247

Morshed, A. (2025c). Ethical challenges in designing sustainable business models for responsible consumption and production: Case studies from Jordan. *Management & Sustainability: An Arab Review.* https://doi.org/10.1108/MSAR-09-2024-0131

Morshed, A. (2025d). Sustainable energy revolution: Green finance as the key to the Arab Gulf States' future. *International Journal of Energy Sector Management*. https://doi.org/10.1108/IJESM-10-2024-0007

Morshed, A., & Khrais, L. T. (2025). Cybersecurity in digital accounting systems: Challenges and solutions in the Arab Gulf Region. *Journal of Risk and Financial Management, 18*(1), Article 41. https://doi.org/10.3390/jrfm18010041

Morshed, A., & Ramadan, A. (2023). Qualitative analysis of IAS 2 capability for handling the financial information generated by cost techniques. *International Journal of Financial Studies, 11*(2), Article 67. https://doi.org/10.3390/ijfs11020067

Mumcuoğlu, E., Öztürk, C. E., Ozaktas, H. M., & Koç, A. (2021). Natural language processing in law: Prediction of outcomes in the higher courts of Turkey. *Information Processing & Management, 58*(5), Article 102684. https://doi.org/10.1016/j.ipm.2021.102684

Munro, V. E., Bettinson, V., & Burton, M. (2024). Coercion, control and criminal responsibility: Exploring professional responses to offending and suicidality in the context of domestically abusive relationships. *Social & Legal Studies, 33*(3), 392–419. https://doi.org/10.1177/09646639231198342

Paraschiv, E.-A., Băjenaru, L., Petrache, C., Bica, O., & Nicolau, D.-N. (2024). AI-driven neuro-monitoring: Advancing schizophrenia detection and management through deep learning and EEG analysis. *Future Internet, 16*(11), Article 424. https://doi.org/10.3390/fi16110424

Perkins, E. R., Bradford, D. E., Verona, E., Hamilton, R. H., & Joyner, K. J. (2023). The intersection of racism and neuroscience technology: A cautionary tale for the criminal legal system. *Policy Insights from the Behavioral and Brain Sciences, 10*(2), 279–286. https://doi.org/10.1177/23727322231196299

Petoft, A., Abbasi, M., & Zali, A. (2023). Loss of free will in the Iranian criminal justice system: Interdisciplinary analysis of law and neuroscience. *Social Neuroscience, 18*(5), 292–296. https://doi.org/10.1080/17470919.2023.2244727

Raji, I., & Sholademi, D. B. (2024). Predictive policing: The role of AI in crime prevention. *International Journal of Computer Applications Technology and Research, 13*(10), 66–78. https://doi.org/10.7753/IJCATR1310.1006

Rajković, N. (2024). The danger of the interpretation of facts: Legal uncertainty in the Spanish saga cases. *Laws, 13*(3), Article 27. https://doi.org/10.3390/laws13030027

Ribeiro Daquila, J. R. (2024). *Multiple intelligences: A perspective of music in the improvement of Emirati English and the interinfluence between Emirati English and Emirati Arabic* [Doctoral thesis, Universidad Complutense de Madrid]. Universidad Complutense de Madrid. https://hdl.handle.net/20.500.14352/104936

Richmond, K. M., Muddamsetty, S. M., Gammeltoft-Hansen, T., Olsen, H. P., & Moeslund, T. B. (2024). Explainable AI and law: An evidential survey. *Digital Society, 3*(1), Article 1. https://doi.org/10.1007/s44206-023-00081-z

Romero Moreno, F. (2024). Generative AI and deepfakes: A human rights approach to tackling harmful content. *International Review of Law, Computers & Technology, 38*(3), 297–326. https://doi.org/10.1080/13600869.2024.2324540

Salhab, H., Zoubi, M., Khrais, L. T., Estaitia, H., Harb, L., Al Huniti, A., & Morshed, A. (2025). AI-driven sustainable marketing in Gulf Cooperation Council retail: Advancing SDGs through smart channels. *Administrative Sciences, 15*(1), Article 20. https://doi.org/10.3390/admsci15010020

Scherlis, G. (2023). Party regulation in Latin America: A change of normative paradigms. *Party Politics, 29*(1), 77–88. https://doi.org/10.1177/13540688211050490

Shams, A. (2026). The role of international law in reshaping cyber criminology: Case study "Draft United Nations Convention Against Cybercrime 2024". In F. Ortiz-Rodriguez, S. K. Shandilya, C. M. Vargas Orozco, J. I. Ibarra Costilla, and J. Llamas Covarrubias (Eds.), *Reshaping criminology with AI* (pp. 125–154). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-8871-6.ch007

Shiyyab, F. S., & Morshed, A. Q. (2024). The impact of credit risk mitigation on the profits of investment deposits in Islamic banks. In N. Mansour & L. Bujosa (Eds.), *Islamic finance: New trends in law and regulation* (pp. 117–129). Springer. https://doi.org/10.1007/978-3-031-48770-5_11

Ștefan, E. E. (2024). Integrity and transparency in the work of public authorities: Aspects of comparative public law. *Juridical Tribune, 14*(4), 564–583. https://doi.org/10.62768/TBJ/2024/14/4/03

Taylor, R. R., Murphy, J. W., Hoston, W. T., & Senkaiahliyan, S. (2025). Democratizing AI in public administration: Improving equity through maximum feasible participation. *AI & Society, 40*(5), 3653–3662. https://doi.org/10.1007/s00146-024-02120-w

Wang, S., Li, Y., & Khaskheli, M. B. (2024). Innovation helps with sustainable business, law, and digital technologies: Economic development and dispute resolution. *Sustainability, 16*(10), Article 3910. https://doi.org/10.3390/su16103910

Wolniak, R., Stecuła, K., & Aydın, B. (2024). Digital transformation of grocery in-store shopping-scanners, artificial intelligence, augmented reality and beyond: A review. *Foods, 13*(18), Article 2948. https://doi.org/10.3390/foods13182948

Yang, X., Wang, Z., Wang, Q., Wei, K., Zhang, K., & Shi, J. (2024). Large language models for automated Q&A involving legal documents: A survey on algorithms, frameworks and applications. *International Journal of Web Information Systems, 20*(4), 413–435. https://doi.org/10.1108/IJWIS-12-2023-0256

Yue, S., Chen, W., Wang, S., Li, B., Shen, C., Liu, S., Zhou, Y., Xiao, Y., Yun, S., Huang, X., & Wei, Z. (2023). DISC-LawLLM: Fine-tuning large language models for intelligent legal services. *arXiv*. https://doi.org/10.48550/arXiv.2309.11325