

ARTIFICIAL INTELLIGENCE IN CRIMINAL JUSTICE GOVERNANCE: OPPORTUNITIES AND LEGAL CHALLENGES (A COMPARATIVE STUDY)

Abouelwafa Ibrahim^{*}, Fatiha Mohammed Gourari^{*},
Gehad Mohamed AbdelAziz^{**}, Adham Hashish^{***}

^{*} College of Law, United Arab Emirates University, Al Ain, UAE

^{**} College of Law, United Arab Emirates University, Al Ain, UAE; Faculty of Law, Zagazig University, Zagazig, Egypt

^{***} Corresponding author, Institute of Public Administration, Riyadh, Saudi Arabia

Contact details: Institute of Public Administration, P. O. Box 205, Riyadh 11141, Saudi Arabia



Abstract

How to cite this paper: Ibrahim, A., Gourari, F. M., AbdelAziz, G. M., & Hashish, A. (2026). Artificial intelligence in criminal justice governance: Opportunities and legal challenges (A comparative study). *Corporate Law & Governance Review*, 8(2), 77–88.
<https://doi.org/10.22495/clgrv8i2p7>

Copyright © 2026 The Authors

This work is licensed under a Creative Commons Attribution 4.0 International License (CC BY 4.0).
<https://creativecommons.org/licenses/by/4.0>

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

Received: 19.10.2025
Revised: 05.01.2026; 20.01.2026; 23.02.2026
Accepted: 23.03.2026

JEL Classification: K14, K20, K42, O33, O38
DOI: 10.22495/clgrv8i2p7

This article examines the opportunities and challenges of artificial intelligence (AI) in predictive policing and criminal justice, with a comparative analysis of applications in France, the UAE, and the UK. These technologies span crime prevention, evidence collection, and judicial decision-making. Adopting a comparative theoretical legal approach, the study analyzes relevant legal frameworks to determine their adequacy. While AI enhances law enforcement efficiency, it raises significant concerns regarding privacy, procedural justice, and evidence integrity. The findings emphasize that integrating AI into justice systems requires precise legal regulation to balance technological innovation with constitutional rights. The study concludes that establishing clear definitions for predictive justice and ensuring the legitimacy of AI-generated evidence are essential. Furthermore, AI integration must adhere to principles of transparency and accountability, supported by continuous auditing and judicial oversight. Ultimately, this paper proposes a normative analytical framework that aligns AI innovation with fundamental rights and the rule of law.

Keywords: Predictive Justice, Artificial Intelligence, Criminal Justice, Algorithmic Risk Assessment, Surveillance and Privacy, Criminal Procedure, Human Rights and Technology

Authors' individual contribution: Conceptualization — A.I., G.M.A., and A.H.; Methodology — G.M.A. and A.H.; Validation — F.M.G. and A.I.; Formal Analysis — G.M.A. and A.H.; Investigation — A.I., F.M.G., G.M.A., and A.H.; Resources — G.M.A. and A.H.; Writing — Original Draft — A.H.; Writing — Review & Editing — A.I., F.M.G., and G.M.A.; Visualization — G.M.A. and A.H.; Supervision — G.M.A. and A.H.; Project Administration — A.I., G.M.A., and A.H.

Declaration of conflicting interests: The Authors declare that there is no conflict of interest.

1. INTRODUCTION

In recent years, artificial intelligence (AI) has become a fundamental component across various sectors, including justice, and more specifically, the criminal justice system. The concept of predictive justice, which involves using algorithms to assess the likelihood of crimes being committed in certain areas and the probability of recidivism (Wu & Lin, 2025), has sparked intense debates and questions

concerning its ethical and practical implications (Galli & Sartor, 2023). While some view it as a significant opportunity to enhance the efficiency of the criminal justice system, others express concerns about the potential emergence of algorithmic biases and their impact on fundamental principles of justice and human rights (Blount, 2024).

Among the most prominent modern applications of information systems are AI technologies. These represent the most advanced

innovations produced by the human mind in the last five decades of the previous century. AI is the ability to model computational systems that can operate in various contexts and situations without direct human intervention. These systems exhibit behavior that simulates human intelligence, producing specific effects through independent and autonomous decision-making. What most clearly distinguishes AI programs from other types of software is their exceptional ability to learn, acquire experience, and make decisions independently, without direct human supervision. In addition, they possess inference skills and adaptability to their surrounding environment (El-Kady, 2024a).

This paper examines how AI can be integrated into criminal justice systems to ensure transparency, accountability, and compliance with fundamental rights while preserving the rule of law. First, it addresses the legal and theoretical framework governing AI use in predictive policing and in evidence gathering. It then analyses using AI in the investigation phase and its legality. It then addresses the use of AI in specific cases, such as stop, arrest, search, smart crime scene, and trial. The concluding section reflects on the need for striking a reasonable balance between implementing innovative policing and investigative mechanisms and safeguarding fundamental rights and freedoms.

The structure of the paper is as follows. Section 2 reviews the relevant literature. Section 3 outlines the research methodology. Section 4

presents the results. Section 5 discusses the results. Section 6 provides the conclusions of the study.

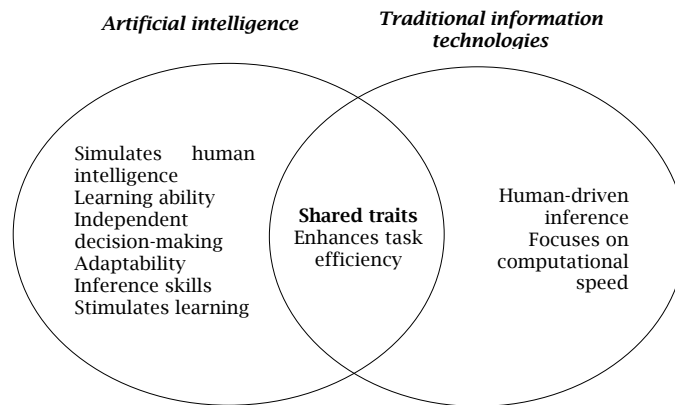
2. LITERATURE REVIEW

AI comprises software, technologies, and machines that simulate human intelligence, designed to accomplish any given task most intelligently, in the shortest time, and with the highest level of precision (Susskind & Susskind, 2022). This marks a significant turning point that goes beyond what is traditionally known as information technology (IT), wherein a human being carries out the inferential process, and where the primary reason for using computers is their exceptional speed (Kandeel, 2020).

Nevertheless, a fundamental distinction remains between human capabilities and AI. Human beings alone can invent and create new models, utilizing various mental processes, including innovation, creativity, and different forms of reasoning. In contrast, the computational model that AI can represent is merely a simulation of a pre-existing model first conceived by the human mind and then subsequently programmed.

Accordingly, AI is just a simulation of human intelligence and an attempt to understand its nature. Human intelligence is characterized by the ability to reason, analyze, and adapt to problems and situations. This is achieved by developing computer programs or applications that mimic human behavior described by natural intelligence — hence the term “artificial intelligence”.

Figure 1. Comparing AI vs. traditional IT



Source: Authors' elaboration.

Moreover, the tremendous and rapid technological advancements in AI technologies and applications may lead to a stage where advanced programming allows these systems to make decisions independently that deviate from their original programming design, whether intentionally or due to error. These applications may even result in intentional crimes without the intervention of the programmer, owner, or operator. Other crimes may occur due to the assistance or negligence of any of them (Chakraborty, 2025).

The UAE has established several strategies related to AI. It has also created the Artificial Intelligence Council, appointed a Minister of State for Artificial Intelligence, and launched several initiatives in this regard. On October 17, 2024, the Federal Public Prosecution announced the

development of an innovative digital system based on AI to enhance the efficiency and speed of its procedures. This system is distinguished by its ability to conduct precise legal research, including the analysis and reorganization of facts in criminal cases, the provision of observations on images, audio recordings, and video clips, as well as their transcription. It also enables the immediate retrieval of information and judicial principles, linking them to case facts and criminal precedents, and presenting legal and jurisprudential opinions, thus contributing to a comprehensive simplification of legal processes (Hashish, 2024).

In addition, the Ministry of Justice, in partnership with the Government Development and the Future Office, as well as the Office of Artificial Intelligence, Digital Economy, and Remote Work

Applications within the UAE Government, announced — concurrently with the events of “GITEX 2024” — the launch of the “Virtual Lawyer” project powered by AI. This project supports legal institutions in developing legal pleadings in simple cases and enhances the justice sector’s preparedness for future opportunities and developments (Bhatt et al., 2024). It also reflects the impact of these changes on the justice sector and legal professions, utilizing advanced technologies and AI to develop new governmental models that accelerate service delivery and enhance the litigation experience in a digital and interactive environment. The Virtual Lawyer is the first project in the UAE and the Arab region. It aims to create added value by increasing legal awareness among community members.

3. RESEARCH METHODOLOGY

This article employed a comprehensive legal research methodology, integrating descriptive and analytical theoretical analysis with a comparative legal approach. The study encompassed a diverse range of materials, including legal texts, judicial rulings, and official policy documents issued by national authorities in countries such as the UAE, France, and the UK. Among the legal texts examined were constitutional provisions from the UAE Constitution, as well as statutory laws, such as the UAE Code of Criminal Procedure and the French Code of Criminal Procedure.

The study also included an analysis of secondary sources, comprising books and articles addressing concepts such as predictive justice and AI, alongside policy reports related to specific applications of AI in the field of criminal justice, including systems like COMPAS, HART, PredPol, PAVED, SALVAC, Connect, and the No-Fly List.

Furthermore, the comparative legal methodology was applied to the countries above, with a focus on the legal frameworks governing the use of AI. Reference was made to legal databases, such as Legifrance and Brocardi.it, Westlaw, and LexisNexis, which provided access to legal texts and judicial decisions across multiple jurisdictions.

4. RESULTS

The analysis reveals that, despite increasing legislative attention to AI in certain jurisdictions, existing legal frameworks remain insufficient to address the distinctive characteristics and implications of AI systems in criminal justice. Although some national legislations include provisions regulating AI, these instruments largely conceptualize AI as a conventional technological tool attributable solely to human users. This approach fails to account for the autonomous or semi-autonomous nature of advanced AI systems, leaving regulatory gaps in accountability and responsibility for AI-generated outcomes.

A key finding of the study is the absence of a comprehensive legal framework governing criminal liability for harms or offences arising from the use of AI. None of the legal systems examined provides a transparent allocation of responsibility among programmers, manufacturers, system operators, or rights holders of AI technologies. Furthermore,

the analysis indicates a lack of legal provisions enabling direct regulatory or corrective measures against AI systems themselves, such as suspension, restriction, or prohibition of use, even when an AI system is identified as a causal factor in criminal conduct or damage.

The evaluation of predictive policing and risk assessment tools — including COMPAS, HART, PredPol, PAVED, and SALVAC — demonstrates that these applications offer measurable benefits in crime prevention, investigative efficiency, and decision-support processes. In particular, the tools enhance risk assessment during investigations and trials and contribute to more efficient evidence collection. However, the study finds that the legal and constitutional recognition of these technologies and their outputs remain limited. In several jurisdictions, decisions informed by AI systems lack apparent legal legitimacy, and the admissibility or evidentiary value of AI-generated outcomes is insufficiently defined.

A comparative analysis further reveals significant variation among the legal systems studied in their institutional readiness to integrate AI into criminal investigations and adjudication. While France has a comparatively more developed legal framework for AI use in criminal justice, the findings indicate that further clarification is required, particularly regarding transparency obligations and the scope of judicial oversight. Effective supervisory mechanisms over police practices, prosecutorial decision-making, and evidence-gathering processes remain underdeveloped.

Finally, the results underscore the persistent challenge of balancing technological innovation with the protection of fundamental rights and freedoms. The deployment of AI in criminal justice raises substantial concerns related to privacy, procedural fairness, and equality before the law. The study identifies the preservation of evidence integrity, safeguards against algorithmic bias, and the protection of fair trial guarantees as critical conditions for the legitimate use of AI-assisted decision-making within criminal proceedings.

5. DISCUSSION

5.1. Managing predictive policing systems using AI technologies

The process of evidence and clue collection using AI systems, as practiced in France, is worth noting. Various AI-based systems collect evidence and indicators that judicial authorities can rely on to bring charges. This practice begins with judicial police units, which utilize sequential analysis files that depend on programs for the automated processing of personal data, enabling the collection of evidence and the identification of perpetrators. This is achieved by establishing links between individuals, events, or crimes.

One example of these systems — still in need of further development through advances in AI — is the SALVAC program (Système d’Analyse des Liens de la Violence Criminelle or Criminal Violence Link Analysis System). This is a sequential analysis system that has been used since 2003 by the National Police and National Gendarmerie, enabling links to be made between acts of criminal violence,

such as homicide, attempted murder, rape, and sexual assault. It also includes data related to criminal disappearances, the discovery of unidentified bodies, as well as data on the modus operandi, timing of events, victim behavior, and

statements made by perpetrators. At its operational level, this program has stored more than 15,000 files, divided into over 150 categories, analyzed by 11 specialized analysts.

Table 1. Key predictive policing tools and their functions

<i>Tool</i>	<i>Country</i>	<i>Function</i>	<i>Stage of use</i>
COMPAS	USA	Risk assessment in sentencing	Trial/Sentencing
HART	UK	Recidivism prediction	Pre-trial/Investigation
PredPol	UK/USA	Crime hotspot mapping	Prevention
SALVAC	France	Threat detection	Prevention/Surveillance
PAVED	France	Predictive analysis of violence	Investigation
Connect	UK	Financial and data analysis	Investigation
No-Fly	USA	Suspect identification	Pre-crime prevention

Source: Authors' elaboration.

In reality, it cannot yet be said that the use of this program constitutes a full implementation of AI systems, as the current use of AI within it remains limited. The program relies on a database that only partially represents the connections between the stored files and is still manually populated by investigators, with the results also being analyzed by human intelligence. However, future developments are anticipated to enable the broader application of AI advancements in mass data analysis, whether through the complete automation of data input or the use of AI-driven algorithms to analyze this data (Kandeel & Elrefae, 2023).

It might be hard to detect a legal or judicial definition of predictive policing in any legislative text or court's decision. However, certain doctrinal efforts, various reports, or foreign expertise-based analyses allow the theoretical framework of predictive justice to be outlined (El-Kady, 2024b). For example, a report by the Higher Studies Centre of the French Ministry of the Interior, published in March 2019, defined predictive policing as the use of data and other indicators by police forces to

calculate the probability of a crime occurring in the future. It may also involve calculating the likelihood of an individual — previously flagged due to suspected unlawful activity — committing a future offense, thereby justifying preventive measures.

This type of information is highly valuable, as it not only helps prevent crime but also enhances the strategic deployment of police forces. In his parliamentary report on AI, MP Cédric Villani described this model of predictive policing as one that applies predictive techniques and big data analysis to prevent crime.

It is worth noting that, despite the absence of a clear and specific definition of predictive policing under French law, practices involving AI technologies to process personal data for crime prevention, investigation, and law enforcement are emerging. Consequently, the legal basis for predictive policing is analogous to the legal bases underpinning current uses of specific technologies, such as augmented video, video surveillance, and facial recognition.

Table 2. Comparison of legal approaches to predictive policing in France, the UAE, and the UK

<i>Jurisdiction</i>	<i>Legal definition of predictive policing</i>	<i>Judicial authorization required</i>	<i>Constitutional privacy protections</i>
France	No statutory definition	Yes	Yes (General Data Protection Regulation, French Constitution)
UAE	No statutory definition	Varies	Yes (Article 31 of the Constitution)
UK	No statutory definition	Varies	Yes (Data Protection Act of 2018)

Source: Authors' elaboration.

According to the CNIL (France's Data Protection Authority), augmented video technology refers to devices connected to algorithmic processing software, enabling automated analysis. This differs from biometric data processing, such as facial recognition. Augmented video technology allows the real-time, automatic detection of specific behaviors or events in public spaces, thereby facilitating police operations.

In 2017, the French National Gendarmerie successfully tested a program called Predvol (also known as PAVED 5), specifically designed to analyze burglaries and vehicle attacks. This system was developed by the Central Criminal Intelligence Directorate of the Gendarmerie, utilizing closed Ministry of the Interior crime databases spanning the past seven years and public socio-economic data from the National Institute of Statistics and Economic Studies (INSEE).

The PAVED system is based on the near repeat theory, a concept frequently used in the development of predictive algorithms. This theory assumes that if an offense occurs in a specific area, there is a statistical likelihood that similar violations will recur in the exact location. The program ultimately generates maps highlighting crime "hot spots", using color gradients from blue to red, based on the estimated level of delinquency risk in each area.

5.2. Evidence gathering by AI-based systems

AI is a tool capable of gathering or generating evidence or clues. However, such clues only attain the status of criminal evidence through the probative value attached to them by the judge (Hashish, 2025), which must be based on their conviction (Huq, 2022).

In France and the UAE, the principle of freedom of proof prevails in criminal proceedings. Article 27 of the French Code of Criminal Procedure permits any method of proof that the judge accepts, based on his conviction. Therefore, evidence collected or generated by AI is presumptively admissible, subject only to the legality of the investigative procedures and the requirement of prior authorization for its use. Accordingly, the use of algorithms in criminal investigations requires judicial authorization, just as other investigative measures do.

Considering the inadequacy of traditional investigation and surveillance methods in addressing specific types of crime, modern mechanisms and tools are being employed to confront emerging forms of criminal activity (Rigano, 2019). It must be noted that, in such cases, where the offense has not yet occurred, it is strictly prohibited to arrest individuals preemptively. Instead, administrative oversight measures, such as providing support through healthcare or social service professionals, may be taken (Afify et al., 2023). For instance, individuals with a medical history of psychological or mental disorders may be offered counseling. Predictive policing may also identify individuals who are at a higher risk of committing crimes. Similarly, potential victims may be contacted through social services to provide support and prevent crimes that might target them.

In this context, it is worth noting that COMPAS, one of the AI applications used in risk assessment, is relied upon for predicting hotspots where violent crimes are likely to occur. It is also appropriate to refer to other predictive policing tools used during the preliminary investigative phase. One is the No-Fly List, a big data application that collects and analyzes information on potential terrorists to prevent criminal acts. Additionally, algorithms are used to detect fraud, money laundering offenses, and illicit activities on the Dark Web (El-Kady, 2025).

The first category includes predictive policing tools designed to prevent specific types of crime that exhibit regular patterns, such as burglary, street violence, and vehicle theft. These tools are based on their ability to accurately determine the location and time at which such crimes are committed and to reproduce this information on a geographical map in the form of hotspots monitored by police patrols in real-time. This process is referred to as predictive policing or predictive crime mapping (Završnik, 2020).

Most software in this field relies on historical evidence of crime locations, such as police reports. It employs advanced techniques that combine data from diverse sources, including reported crime data and survey findings on criminal behavior.

It is worth mentioning that predictive tests conducted in the UK to identify likely sites of theft, burglary, and physical assault demonstrated that the software PredPol was 78% accurate, compared to 51% accuracy using traditional methods.

5.3. Use of AI technologies in the investigation phase

Big data analytics applications are increasingly being used during the investigation stage. This is very critical especially in complex offenses committed in the financial sector (El-Gheriani & Hashish, 2025), for example, or by companies conducting ordinary course of business (El-Gheriani & Farag, 2014) which

might violate sophisticated laws such as competition law (El-Gheriani & Hashish, 2023), environmental law (Al Shamisi, 2025; Ibrahim, 2025; Daran et al., 2023) or intellectual property law (Fayed et al., 2025). Among these tools is Connect, which is used in the UK to analyze billions of records generated from financial transactions to detect correlations or activity patterns. Another example is the International Child Sexual Exploitation Database (ICSE DB) managed by Interpol, which aids in identifying victims and perpetrators by analyzing certain image features, such as furniture and other objects in abusive images, or by analyzing background audio noise in video footage.

This tool has proven effective in combating crime, enabling searches that once took months of investigative work to be completed within minutes, even with high complexity and massive data volumes.

5.4. Legality of law enforcement officers' use of modern technologies in investigations and inquiries

A question may arise regarding the use of technical methods by law enforcement officers during criminal investigations and inquiries, especially considering Article 36 of Federal Decree by Law No. (38) of 2022, Promulgating the Criminal Procedures Law, which provides that:

“Law enforcement officers must accept all notifications and complaints submitted regarding crimes. They and their subordinates must gather statements and conduct necessary inspections to facilitate the investigation of the incidents reported to them or those of which they are aware by any means. They must take all necessary precautionary measures to preserve evidence of the crime”.

In this context, “robot” refers to the intelligent robot, distinct from the automated or electronic robot. The latter is defined as “an electronic program created or modified for efficiently and rapidly executing automated tasks” (as defined in Federal Decree-Law No. (34) of 2021 on Countering Rumors and Cybercrimes, as amended by Federal Law No. (5) of 2024). The automated or electronic robot is pre-programmed with predictable actions and lacks intelligent cognitive functions.

In contrast, the intelligent robot is a physical machine with AI acting as its “brain”, granting it autonomy in its operations. It is not designed to perform a fixed, predetermined sequence of actions. Instead, it is programmed with AI algorithms capable of deep learning and operating based on changing external variables, making its behavior difficult to predict. It is autonomous and not restricted to specific automated tasks (Amoroso & Tamburrini, 2018).

Accordingly, law enforcement officers may legitimately use intelligent robots as technical tools, for example, in identifying suspects or analyzing biometric data such as voice and iris prints.

There is no doubt regarding the legality of using such means, provided they do not infringe upon the rights and freedoms of others. The legitimacy of such use has become a settled matter in policing practices. Indeed, one may argue that these robots and other modern technological tools, by analogy, constitute subordinates and assistants to law enforcement officers within the meaning of Article 36 of Federal Decree by Law

No. (38) of 2022, Promulgating the Criminal Procedures Law, provided their use occurs in the presence or under the supervision of such officers.

Thus, if a deficiency exists or a new tool emerges that falls within the scope of a procedural rule by analogy, such analogy is permissible, even if it is not in the accused's favor. Having committed a crime, the accused must expect any lawfully designed procedure aimed at uncovering the truth about the crime, provided the procedure is legally grounded. It does not infringe upon his rights or freedoms.

Investigative actions are limited to gathering information and evidence related to the crime and its perpetrator. They do not affect the person to whom they are applied and are devoid of coercion or compulsion.

Police forces may utilize intelligent robots or vehicles to gather data and make autonomous decisions regarding observation or intervention. At first glance, this act appears highly significant and effective in achieving policing objectives. However, it also raises several legal issues that are likely to emerge during criminal trials, two of which are particularly notable.

The first issue concerns the extent to which surveillance conducted through such methods may affect constitutional guarantees related to the right to privacy (al-Mutairi, 2022). Under these practices, robotic police officers, autonomous police vehicles, or unmanned aerial vehicles (Kandeel et al., 2022) could be equipped to carry out actions involving facial recognition, vehicle license plate tracking, audio and video recording, and other measures. These actions may occur either before or after the commission of crimes. In all cases, such measures — likely to raise legal concerns — may be conducted without the competent authority's required legal authorization. Suppose these procedures are carried out without the permission, consent, or approval of the individuals subject to them. In that case, they may violate the right to privacy protected under Article 31 of the Constitution of the United Arab Emirates (n.d.). Accordingly, there is a need for parliamentary attention and debate that focuses on developing a proper legal framework to balance constitutional rights and emerging practices using AI in criminal justice (El-Wafa et al., 2024).

The second issue concerns the integrity and chain of custody of evidence, including the principle of evidentiary traceability, a well-established judicial standard that criminal courts apply before issuing convictions. When applied to evidence obtained through AI, the legal question likely to arise before criminal courts will center on ensuring that the evidence generated by AI tools — acting independently of human intervention — meets the standards of integrity and traceability of origin and that it has not been tampered with at any stage, whether during acquisition, storage, or retrieval. Otherwise, the legally prescribed consequence would be to exclude the evidence if any irregularities are found.

5.5. The robot's independent stop (*istiqāf*) without intervention by a judicial police officer

The act of stopping and questioning (i.e., investigative stop) is based on suspicion or doubt regarding an individual's behavior. In this context, AI

technologies can play a significant role in detecting suspicious behavior, as they perform the same task carried out by a law enforcement officer in inferring the existence of suspicion or doubt.

These predictive algorithms, designed to anticipate the commission of crimes, can be integrated into surveillance cameras to send alerts to the police when a person is in a dark street and acts suspiciously. Consequently, stopping this individual could prevent the commission of a crime. In this way, the police can act preemptively and take proactive measures to prevent and thwart criminal activity.

However, the primary concern is not whether AI technologies can play a significant role in detecting suspicious behavior, but whether they can conduct the investigative stop autonomously and independently. Such a practice would not fit the traditional interpretation of criminal procedure provisions.

Like most criminal procedural laws, the UAE Federal Code of Criminal Procedure does not contain any provisions regulating the use of intelligent AI robots in criminal procedures. This raises the question of the legality of a robot carrying out specific administrative measures independently, without human intervention. For instance, what if a robot were to stop a person based on facial recognition technology identifying the individual as a security suspect or as someone who, according to predictive analytics derived from facial metrics and criminal history, is likely to commit a crime? In such a scenario, the robot police officer might proceed to stop the person. This raises questions concerning the legality of such autonomous measures, how to handle situations where it is necessary to escort the person to the police station or detain him until police officers arrive to execute an arrest, and the legality of such detention conducted by the robotic police officer.

Given the absence of provisions in the Federal Code of Criminal Procedure regulating the use of intelligent robots in criminal procedures, there is a clear legislative need to regulate the actions that may be performed by such robots independently of human police officers. This would include enacting legal provisions recognizing the robot as a member of the judicial police with special jurisdiction. Such legislative intervention would serve to uphold the principle of procedural legality, just as with the legality of crimes and punishments, according to Article 27 of the Constitution of the United Arab Emirates (n.d.), which provides that: "The law shall define crimes and punishment".

Procedural legality entails that only written law can be the source of criminal procedures, as such procedures often involve coercive measures against the accused and infringe on fundamental individual rights. Furthermore, these procedures are typically applied to individuals who have not been convicted and may never be convicted. Accordingly, the law must be the source of such procedures. Procedural legality also requires that the law clearly define the formal and substantive conditions necessary to undertake the procedure, failing which, the procedure would be deemed null and void.

That said, procedural legality does not preclude the competent authority from exercising appropriate discretionary powers in applying criminal procedures.

It should be clarified that although the procedures involved in a stop do not entail

physical interference with the person being investigated, it nevertheless constitutes an encroachment on personal liberty. Therefore, such a measure is permissible to a public authority official — even if not a member of the judicial police — if the person voluntarily and willingly places themselves in a situation that raises suspicion and doubt, and if that situation indicates a necessity justifying intervention by the officer to investigate and verify the individual's identity. For the stop to be lawful — and consequently for any measures resulting from it to be deemed valid — it must be based on suspicion. However, if this suspicion is absent, such as when the public prosecution or trial court does not consider the circumstances surrounding the accused as indicative of a suspicious situation, the stop is unlawful. If it leads to a claim of *flagrante delicto* (in blazing offence), such flagrancy would not have arisen lawfully, and any procedural acts based on this alleged flagrancy would be invalid.

For these reasons, stop measures carried out by a robot are unlawful, and any resulting procedures would likewise be void.

5.6. Distinction between AI technology and remote criminal procedures

The preceding analysis is not contradicted by Article 416 of Federal Decree by Law No. (38) of 2022, Promulgating the Criminal Procedures Law, which provides that: “The head of the competent authority or his delegate may carry out procedures remotely at any stage of the criminal case if he deems it necessary to achieve investigation, inquiry, or litigation procedures”.

This is because remote procedures are carried out using non-intelligent automated electronic software systems in the presence of the competent official responsible for executing the method, who remains the actual decision-maker (Kandeel and Khalil, 2022). This differs fundamentally from AI, which is characterized by autonomy. Autonomy is the defining feature that distinguishes AI systems from other electronic programs that operate based on predetermined inputs and perform specific tasks without any decision-making independence.

Unlike AI systems, these traditional programs do not sequentially collect, analyze, or interpret data, nor do they independently make decisions. Such a capability is exclusive to AI systems. While both AI and automated electronic systems share the immaterial (non-physical) nature of their operation, they differ fundamentally in their autonomy in decision-making.

This also applies to what is stipulated in Article 44/1 of Federal Decree-Law No. (14) of 2024 on Traffic Regulation: “To implement the provisions of this Decree-Law, its executive regulations, and the decisions issued in implementation thereof, modern technologies may be used to achieve road safety and to issue fines on vehicles and individuals”.

These modern technologies in road safety and issuing fines on vehicles and individuals refer to electronic programs and applications that operate in the presence and knowledge of the judicial officer and AI programs that operate independently of any human intervention. This is notwithstanding what is

stated in the second paragraph of this article, which reads: “The licensing authority shall establish the electronic and smart programs and applications through which requests for obtaining licenses and permits issued under the provisions of this Decree-Law and its executive regulations are submitted. A decision from the Minister or the head of the licensing authority shall be issued to approve them”.

It is noteworthy that the text in this paragraph uses the term “electronic and smart programs and applications”, unlike the first paragraph, which used the term “modern technologies”. However, this latter phrase is broad enough to include electronic and innovative applications.

5.7. Arrest and search by robots

Assuming that intelligent robots are equipped with the ability to arrest individuals, especially in cases where a crime has been committed in *flagrante delicto*, as permitted under Article 46 of Federal Decree by Law No. (38) of 2022, Promulgating the Criminal Procedures Law, which states:

“A judicial officer may order the arrest of an accused person present, if there is sufficient evidence of their involvement in a crime, in the following cases:

1. Felonies.
2. Misdemeanors committed in *flagrante delicto* are punishable by a penalty other than a fine.
3. Misdemeanors are punishable by a penalty other than a fine if the accused is under any form of surveillance or if there is a risk of the accused fleeing.
4. In misdemeanors related to theft, fraud, dereliction of duty, severe assault, resistance to public authority with force, violation of public morals, and offenses involving weapons, ammunition, explosives, intoxicants, hazardous materials, drugs, or psychotropic substances”.

This assumption is not impossible; the optimal aspiration for the use of robots is to equip them with the necessary force to arrest individuals, to reduce the burden on police officers, especially during dangerous pursuits and raids on criminal gangs, organized crime groups, or terrorist cells. Arresting such individuals and raiding their hideouts is fraught with danger and poses a threat to the safety and security of police officers, as occurred in the USA, where discussions were raised regarding the use of robots to arrest criminals in serious crimes. This was evident in a mass shooting incident in one of the USA states, which ended with the shooter being killed by a bomb dropped by a robot. This incident raised concerns among legal professionals about the new development in law enforcement mechanisms and their impact on the presumption of innocence.

Since this is an inevitable development, legislative intervention must address this evolution. Legal intervention is necessary to establish provisions that regulate the use of the arrest procedure independently of human police officers, if controls are put in place to ensure the justification for the arrest and the procedures that follow it. Until such provisions are established, the robot should be limited to identifying the faces of criminals and individuals wanted for security reasons and sending

this information to judicial authorities to facilitate their arrest by judicial officers.

This also applies to the act of search, as it is one of the investigative procedures that may only be carried out by a judicial officer or a public prosecutor. Dubai Police announced that the department intends to utilize AI technologies to enhance its inspection operations (Al-Amir, 2024). According to this statement and considering the provisions of the Federal Criminal Procedure Code, AI technologies may be used to enhance inspection procedures under the supervision and knowledge of a judicial officer, but not as a substitute for the officer, for the inspection and its results to be deemed legally valid.

5.8. The legal definition of in *flagrante delicto* cannot be established through smart machine vision technology

In the context of ongoing technological advancements and the increasing use of AI in police work, a technology known as machine vision has emerged. It is a series of algorithms functioning as a flowchart or a series of questions designed to match the observed object at a crime scene with hundreds of thousands of reference images of humans, vehicles, and machinery in various positions, angles, and movements. Intelligent recording of the crime may occur under Article 43 of Federal Decree by Law No. (38) of 2022, Promulgating the Criminal Procedures Law, which states:

“1. A crime shall be considered in *flagrante delicto* if it is being committed or has just been committed.

2. A crime shall also be deemed in *flagrante delicto* if the victim follows the perpetrator, or if the public follows the perpetrator with shouting immediately after the crime, or if the perpetrator is found shortly thereafter in possession of tools, weapons, property, or objects indicating that they are the perpetrator or an accomplice, or if traces or signs indicating so are found at that time”.

This article appears in Chapter Two of Part One, titled Judicial Officers and Their Duties, of Book Two on Investigation and Collection of Evidence. Therefore, a condition for the legal validity of in *flagrante delicto* is that the judicial officer must personally observe the act, meaning they must witness one of the forms of in *flagrante delicto* with their senses, because they are personally responsible for affirming its occurrence. Their assessment is subject to the discretion of the public prosecutor and the oversight of the trial court. It is not sufficient for the officer to have learned of it secondhand or through the observations of subordinate officers. A fortiori, it is not enough to capture a state of in *flagrante delicto* via ordinary surveillance cameras or through machine vision technology, as there is a risk that the account may be inaccurate, the footage may be fabricated or inauthentic, or the *flagrante delicto* status may not have been precisely determined. This renders the procedures taken by the judicial officer lacking a valid legal basis.

The law aims to confine the concept of in *flagrante delicto* within a narrowly defined scope that serves the public interest. It seeks to balance

two competing interests: first, allowing judicial officers to take actions such as arrest and search before the crime scene evidence disappears, without needing prior authorization from the Public Prosecution; and second, safeguarding individual freedoms so that such exceptional powers — ordinarily within the jurisdiction of the investigative authority — are not exercised except in the narrowest of circumstances.

Accordingly, the observation by an intelligent machine of a case of in *flagrante delicto* does not constitute a legal state of *flagrante delicto*; rather, it constitutes a means of proof of the commission of the crime or a presumption thereof, which remains subject to the discretion of the Public Prosecution and, subsequently, the review of the trial court.

5.9. The smart crime scene

A traditional crime scene is where the crime was committed, and the resulting evidence was discovered. In contrast, a smart crime scene is a location where one or more technologies or applications of AI are used to identify the perpetrator, determine the crime scene, and collect fingerprints. This form of examination, conducted via AI technologies, requires legislative intervention through specific provisions, as the Criminal Procedure Code only addresses the examination of the traditional crime scene. This is because such an examination involves the physical documentation of the condition of an object, place, or person through direct observation or sensory inspection by the individual carrying out the procedure, intending to collect physical traces indicative of the commission of a crime, identify the perpetrator, or uncover the truth in complex civil (Shalaby et al., 2022; Eldakak, 2023; Kandeel & Eldakak, 2024) and administrative (Shouaib et al., 2024; Al Jahoori, 2024; Abouahmed et al., 2023; Makeen, 2023; Kandeel et al., 2023) disputes.

In this sense, the crime scene examination constitutes direct evidence when conducted by a judicial officer, public prosecutor, or judge, because they inspect the container of the material evidence, relying on their faculties of perception and cognition. This direct evidentiary quality does not exist in the virtual crime scene or when the examination is conducted via AI technologies or applications.

5.10. The use of AI in preliminary investigations

AI technology may be employed during preliminary investigations through voiceprint recognition technology for identity verification. The voiceprint is particularly relevant to certain types of crimes, such as those where the perpetrator can be identified by their distinctive vocal characteristics during the investigation process. This is especially true in crimes such as insult (*sabb*), defamation (*qadhif*), threats, and other verbal offenses, where the spoken words form the basis of criminality or constitute the subject matter of the crime.

Moreover, voice may serve as compelling evidence in criminal investigations. For instance, the victim’s voice may constitute strong proof of resistance or an explicit declaration of non-consent to the act. Similarly, voice evidence may indicate

the presence of accomplices or participants in the commission of the crime and help identify individuals present at the crime scene, which may ultimately lead to the identification of the perpetrator.

AI technologies surpass the capabilities of traditional mechanical or computer-linked systems in analyzing audio data. AI ensures high-speed and exact analysis of a person's identity during the preliminary investigation. It also excels in overcoming various obstacles that typically hinder voice analysis, such as poor recording quality, overlapping voices, or intentional alterations in tone or pitch made by the suspect to avoid recognition.

China is among the leading countries in adopting facial recognition technologies, utilizing AI-powered facial recognition systems to identify or confirm individuals based on digital images or video footage. It is currently the most extensive user of facial recognition technology in the world, followed by the USA, Singapore, Malaysia, and the UAE, which has recently begun adopting AI technologies for border surveillance and protection (Qin et al., 2025).

It is worth noting that the admissibility of voice attribution evidence following its recording is contingent upon prior authorization from the competent authority, namely the public prosecutor. Article 73(2) of Federal Decree by Law No. (38) of 2022, Promulgating the Criminal Procedures Law provides that: "A member of the Public Prosecution may, with the approval of the Public Prosecutor, monitor and record communications, including wired and wireless communications".

This constitutes the procedural element of admissibility. The technical element follows, which involves the study of speech defects and individual speech characteristics. A phonetics expert must examine these inherent elements of the voice aurally during the comparative analysis. This type of examination, in addition to physical analysis techniques based on vocal frequency layers, plays a crucial role in supporting the attribution of the voice.

The investigative authority must record conversations between individuals concerning the commission of a crime. It cannot be delegated to judicial or administrative police officers. The public prosecutor may not delegate such action unless it obtains prior approval from the UAE's Public Prosecutor, since the authority to carry out this act is strictly limited. According to Article 68(1) of Federal Decree by Law No. (38) of 2022, Promulgating the Criminal Procedures Law, a public prosecutor's delegation is restricted to investigative procedures for which the prosecutor is competent. However, once permission is obtained from the Public Prosecutor, such delegation may occur lawfully.

5.11. Use of AI technologies during trial proceedings

There are two tools worth mentioning in this domain as they are heavily relied upon to assist judges during trials (Dement & Inglis, 2024). They are HART and COMPAS.

The first, HART (Harm Assessment Risk Tool), is a risk assessment tool based on machine learning. It utilizes police archives to analyze officers'

decisions during a specific period and determine whether certain suspects reoffend.

Based on approximately thirty factors, this tool evaluates whether suspects are at low, medium, or high risk of reoffending. During the evaluation of this tool over a specific time period — analyzing suspect behavior two years after the offense — HART was found to be 98% effective in predicting low-risk cases and 88% effective in predicting the risk of recidivism. Importantly, the results of this tool are meant to be advisory for the judge, and the police will regularly audit HART's performance and reliability.

The second tool in the field of recidivism risk assessment is COMPAS, which assists the judge in determining the sentence to be imposed on the offender. The algorithm comprises 137 questions, which are either answered by the defendant or drawn from their criminal records. These questions cover a broad range of topics, such as whether there is a phone in the household, difficulty paying bills, family history, and the defendant's criminal background.

The algorithm classifies individuals from 1 (low risk) to 10 (high risk). It supports judicial decision-making, and its results are just one of several factors the judge considers when determining the appropriate sentence.

6. CONCLUSION

This paper is subject to several limitations. First, the analysis is primarily normative and conceptual, and does not include an empirical evaluation of AI systems currently used in criminal justice practice. Second, the rapid evolution of AI technologies may affect the long-term applicability of some of the regulatory and oversight mechanisms discussed.

Although some countries' legislation has included provisions regulating AI (Manin et al., 2024), significant shortcomings remain in addressing its various aspects (Abdelsalam et al., 2025; Topchyi et al., 2025). This is primarily because such legislation has often treated AI applications as merely technological programs attributable to their users, who are considered responsible for the outcomes. In doing so, these laws equate intelligent programs with other non-intelligent software, despite the former being distinguished by their full or near-complete autonomy from human intervention. Furthermore, there is no specific law defining legal liability for acts constituting crimes resulting from AI technologies, nor is there a transparent allocation of responsibility among the programmer, the manufacturer, or the rights holder of the AI system. Moreover, there are no legal provisions establishing the imposition of direct measures on the AI system itself — such as suspending or banning its use — when it is deemed the cause of a crime (Issakhankyzy et al., 2024) or causes damage (Alqodsi & Gura, 2023; Eldakak et al., 2024; Mohamed, 2024).

The study evaluated certain AI applications, such as COMPAS, HART, PredPol, PAVED, SALVAC, used in predictive policing. The initial assessment revealed tangible benefits alongside legal challenges. Key benefits included the effectiveness of these applications in crime prevention, risk assessment, and decision-making efficiency, particularly in

estimating an individual's criminal risk during investigations or trials and enhancing evidence collection (Morgante, 2016). However, the study also found that the legal and constitutional recognition of these tools, their outcomes, and the legitimacy of decisions based on them remain limited in several countries. Consequently, there is an urgent need to establish a legal definition and framework to regulate predictive policing and the use of AI in criminal procedures generally.

The study highlighted significant findings, noting variations among the legal systems examined regarding their readiness to support decision-making in investigations or trials, as well as the legitimacy of using these applications and the evidence derived from them. While France has a more advanced legal framework, the study

indicated that it still requires clearer and more transparent measures, as well as effective mechanisms for judicial oversight of police operations, prosecutorial activities, and decisions made during the evidence-gathering and investigation stages.

Finally, the study highlighted the challenges and concerns associated with striking a reasonable balance between implementing innovative policing and investigative mechanisms and safeguarding fundamental rights and freedoms, particularly those related to privacy and procedural justice. Critical guarantees include maintaining evidence integrity, protecting against algorithmic bias, and upholding constitutional safeguards related to fair trials (Quattrocchio et al., 2020).

REFERENCES

- AbdelAziz, G. M., & Abouahmed, A. (2024). The punitive power of independent administrative authorities: Focus on financial and tax violations (A comparative study). *Access to Justice in Eastern Europe*, 7(2), 301–324. <https://doi.org/10.33327/AJEE-18-7.2-n000216>
- AbdelAziz, G. M., & Hashish, A. (2024). Using sanctions in enforcing Digital Markets Act in the EU. In R. E. Khoury & N. Nasrallah (Eds.), *Intelligent systems, business, and innovation research* (Studies in systems, decision and control, Vol. 489, pp. 775–783). Springer. https://doi.org/10.1007/978-3-031-36895-0_65
- AbdelAziz, G. M., & Shalaby, A. (2023). Legal challenges of cryptocurrency. In B. A. M. Alareeni & I. Elgedawy (Eds.), *Artificial intelligence (AI) and finance* (Studies in systems, decision and control, Vol. 488, pp. 890–898). Springer. https://doi.org/10.1007/978-3-031-39158-3_83
- Abdelsalam, M., Abouahmed, A., Shatat, A., Hashish, A., & AlQodsi, E. (2025). Blockchain and smart public procurement contracts: A comparative legal analysis of digital transformation in the public sector. *Access to Justice in Eastern Europe*, 8(4), 242–274. <https://doi.org/10.33327/AJEE-18-8.4-a000137>
- Abouahmed, A., Eldakak, A., & Zakaria, A. (2023). Using electronic auctions for contracting in the UAE federal government procurements. In B. A. M. Alareeni & I. Elgedawy (Eds.), *Artificial intelligence (AI) and finance*. (Studies in systems, decision and control, Vol. 488, pp. 884–889). Springer. https://doi.org/10.1007/978-3-031-39158-3_82
- Afify, A. M., Tannar, H., Zakria, A. A., Hashish, A., & El-Wafa, T. A. (2023). Unveiling the right to health in Egypt: Exploring the transformations and challenges in Egyptian constitutional law and policy. *Academic Journal of Interdisciplinary Studies*, 12(6), 95–112. <https://doi.org/10.36941/ajis-2023-0156>
- Al Jahoori, S. A. H. N. (2024). Assessing the legal ramifications of the COVID-19 pandemic on administrative contracts in the United Arab Emirates: Comparative review. *Access to Justice in Eastern Europe*, 7(3), 461–484. <https://doi.org/10.33327/AJEE-18-7.3-a000313>
- Al Shamisi, H. M. (2025). Legal reflections on compensation for environmental damage in UAE law (Analytical study): Green future prospects and challenges. In E. Alqodsi & A. Abdallah (Eds.), *Legal frameworks and educational strategies for sustainable development* (pp. 45–66). IGI Global Scientific Publishing. <https://doi.org/10.4018/979-8-3693-2987-0.ch004>
- Al-Amir, N. (2024, October 27). *K9 taetazim astikhdam aldhaka' aliaistinaeii fi eamaliaat altaftish* [K9 plans to use artificial intelligence in inspection operations]. Albayan. <https://www.albayan.ae/news/uae/dubai/5282>
- Ally, A. M. (2025). Artificial intelligence (AI) and financial technology (FinTech) in Tanzania; legal and regulatory issues. *International Journal of Law and Management*. Advance online publication. <https://doi.org/10.1108/IJLMA-07-2024-0251>
- Al-Mutairi, N. H. (2022). The right to privacy in the digital age as expressed in a Muslim country: A case study of Kuwait. *Arab Law Quarterly*, 38(1-2), 110–137. <https://doi.org/10.1163/15730255-bja10108>
- Alqodsi, E. M., & Gura, D. (2023). High tech and legal challenges: Artificial intelligence-caused damage regulation. *Cogent Social Sciences*, 9(2), Article 2270751. <https://doi.org/10.1080/23311886.2023.2270751>
- Amoroso, D., & Tamburrini, G. (2018). The ethical and legal case against autonomy in weapons systems. *Global Jurist*, 18(1), Article 20170012. <https://doi.org/10.1515/gj-2017-0012>
- Bhatt, H., Bahuguna, R., Swami, S., Singh, R., Gehlot, A., Akram, S. V., Gupta, L. R., Thakur, A. K., Priyadarshi, N., & Twala, B. (2024). Integrating industry 4.0 technologies for the administration of courts and justice dispensation — A systematic review. *Humanities and Social Sciences Communications*, 11(1), Article 1076. <https://doi.org/10.1057/s41599-024-03587-0>
- Blount, K. (2022). Using artificial intelligence to prevent crime: Implications for due process and criminal justice. *AI & Society*, 39(1), 359–368. <https://doi.org/10.1007/s00146-022-01513-z>
- Chakraborty, S. (2025). *Exploring AI implications on law, governance, and industry*. IGI Global Scientific Publishing. <https://doi.org/10.4018/979-8-3373-3384-7>
- Daran, D. E. D., Al Ajlani, R., Zia-ud-Din, M., & Elhajraoui, F. E. (2023). Management of biodiversity in Pakistan protected areas and its legal implications. *Journal of Wildlife and Biodiversity*, 7, 1–13. <https://doi.org/10.5281/zenodo.14273594>
- Dement, C., & Inglis, M. (2024). Artificial intelligence-assisted criminal justice reporting: An exploratory study of benefits, concerns, and future directions. *Criminology and Criminal Justice*. <https://doi.org/10.1177/17488958241274296>

- Eldakak, A. (2023). The power of the employer to terminate employment contracts: A comparative study between the UAE and Egypt. *Arab Law Quarterly*, 37(5), 599-619. <https://doi.org/10.1163/15730255-bja10132>
- Eldakak, A., Alremeithi, A., Dahiyat, E., El-Gheriani, M., Mohamed, H., & Abdulrahim Abdulla, M. I. (2024). Civil liability for the actions of autonomous AI in healthcare: An invitation to further contemplation. *Humanities and Social Sciences Communications*, 11(1), Article 305. <https://doi.org/10.1057/s41599-024-02806-y>
- El-Gheriani, M., & El Farag, M. S. A. (2014). The rise and fall of Egypt's Code de Commerce: A critical examination of the purpose and content of Egypt's Commercial Code after the establishment of the economic courts. *International Journal of Private Law*, 7(2), 137-158. <https://doi.org/10.1504/IJPL.2014.060087>
- El-Gheriani, M., & Hashish, A. (2023). Egypt amends its Competition Law to establish a pre-merger control system. *Journal of European Competition Law and Practice*, 14(2), 106-112. <https://doi.org/10.1093/jeclap/lpad014>
- El-Gheriani, M., & Hashish, A. (2025). Harnessing the crypto-horse. Factors affecting a friendly regulator of the crypto-industry: Dubai as a test case. *Information & Communications Technology Law*, 34(3), 1-21. <https://doi.org/10.1080/13600834.2025.2452718>
- El-Kady, R. (2024a). Artificial intelligence and criminal law. In M. Tavares, G. Azevedo, J. Vale, R. Marques, & M. Bastos (Eds.), *Artificial intelligence approaches to sustainable accounting* (pp. 34-52). IGI Global Scientific Publishing. <https://doi.org/10.4018/979-8-3693-0847-9.ch003>
- El-Kady, R. (2024b, July). Artificial intelligence from the criminal law perspective. In A. E. Hassanien, A. Darwish, M. F. Tolba, & V. Snášel (Eds.), *Proceedings of the 10th International Conference on Advanced Intelligent Systems and Informatics 2024 (AISI 2024)*. Lecture notes on data engineering and communications technologies, Vol. 233, pp. 162-173). Springer. https://doi.org/10.1007/978-3-031-77299-3_16
- El-Kady, R. (2025, January). Leveraging artificial intelligence for enhanced detection and mitigation of illicit activities on the dark web. In A. E. Hassanien, R. Y. Rizk, A. Darwish, M. T. R. Alshurideh, V. Snášel, & M. F. Tolba (Eds.), *Proceedings of the 11th International Conference on Advanced Intelligent Systems and Informatics (AISI 2025)* (AISI 2025. Lecture notes on data engineering and communications technologies, Vol. 238, pp. 79-89). Springer. https://doi.org/10.1007/978-3-031-81308-5_8
- El-Wafa, T. A., Khalil, A., & Hashish, A. (2024). Parliamentary question: Insights from the Federal National Council in the UAE. *Heliyon*, 10(6), Article 27671. <https://doi.org/10.1016/j.heliyon.2024.e27671>
- Fayed, A., Zakaria, A., & Abouahmed, A. (2025). Innovations of artificial intelligence in light of the applicable copyright law: Realistic solutions and future prospects. A comparative study of UAE, Egyptian, and French laws. *Access to Justice in Eastern Europe*, 8(1), 241-263. <https://doi.org/10.33327/AJEE-18-8.1-a000116>
- Federal Decree by Law No. (38) of 2022, Promulgating the Criminal Procedures Law. (2022). Government of United Arab Emirates. <https://uaelegislation.gov.ae/en/legislations/1609>
- Federal Decree-Law No. (34) of 2021 on Countering Rumors and Cybercrimes. (2021). Government of United Arab Emirates. <https://uaelegislation.gov.ae/en/legislations/1526>
- Federal Decree-Law No. (14) of 2024 on Traffic Regulation. (2024). Government of United Arab Emirates. <https://uaelegislation.gov.ae/en/legislations/2598>
- Galli, F., & Sartor, G. (2023). AI approaches to predictive justice: A critical assessment. *Humanities and Rights Global Network Journal*, 5(2), 165-217. <https://www.humanitiesandrights.com/journal/index.php/har/article/view/118>
- Hashish, A. (2024). Some observations on the 2021 New Penal Code of the United Arab Emirates. *International Journal of Public Law and Policy*, 10(2), 145-154. <https://doi.org/10.1504/IJPLAP.2024.137774>
- Hashish, E. (2025). Smart inference-driven risks: Legal challenges under the GDPR and the Egyptian PDPL. *Balkan Social Science Review*, 26(26), 227-253. <https://doi.org/10.46763/BSSR252626227h>
- Huq, A. Z. (2022). Can a machine sentence justly? *Criminal Justice Ethics*, 41(3), 268-277. <https://doi.org/10.1080/0731129X.2022.2136867>
- Ibrahim, A. (2025). Climate change and legal responsibility for greenwashing. In E. Alqodsi & A. Abdallah (Eds.), *Legal frameworks and educational strategies for sustainable development* (pp. 67-84). IGI Global Scientific Publishing. <https://doi.org/10.4018/979-8-3693-2987-0.ch005>
- Issakhankyzy, A., Alibayeva, G. A., Sabitova, A. A., Zhetpisov, S. K., & Shansharbayeva, B. S. (2024). Legal mechanism for regulating responsibilities in the information sphere. *International Journal of Electronic Security and Digital Forensics*, 16(1), 14-27. <https://doi.org/10.1504/IJESDF.2024.136014>
- Kandeel, M. E. (2020). The impact of the UAE legislator's use of telecommunications technology on judicial notices. *The Lawyer Quarterly*, 10(4), 521-532. <https://tlq.ilaw.cas.cz/index.php/tlq/article/view/435>
- Kandeel, M. E., & Eldakak, A. (2024). Legal dangers of using ChatGPT as a co-author according to academic research regulations [Special issue]. *Journal of Governance and Regulation*, 13(1), 289-298. <https://doi.org/10.22495/jgrv13i1siart3>
- Kandeel, M. E., & Elrefae, G. (2023, December). The impact of artificial intelligence on achieving the efficiency of justice "AI & Speedy Justice". In *2023 24th International Arab Conference on Information Technology (ACIT)* (pp. 01-05). IEEE. <https://ieeexplore.ieee.org/abstract/document/10453918>
- Kandeel, M. E., & Khalil, A. (2022). The one-day court: Settling small civil cases in the UAE. *Arab Law Quarterly*, 37(1-2), 175-193. <https://doi.org/10.1163/15730255-bja10106>
- Kandeel, M. E., Abouahmed, A., & Zakaria, A. (2023). The premature expiration of arbitration litigation in investment disputes. *Corporate Law and Governance Review*, 5(1), 17-28. <https://doi.org/10.22495/clgrv5i1p2>
- Kandeel, M. E., Hamza, E. A., & Elrefae, G. (2024, December). AI governance: A general perspective. In *Global Congress on Emerging Technologies (GCET-2024)* (pp. 195-201). IEEE. <https://ieeexplore.ieee.org/abstract/document/10934585>
- Kandeel, M. E., Salameh, H. B., Elrefae, G. A., & Qasim, A. (2022, November). Regulations for UAV operation in social applications and services: A general perspective. In *2022 Ninth International Conference on Social Networks Analysis, Management and Security (SNAMS)* (pp. 1-6). IEEE. <https://ieeexplore.ieee.org/document/10062752>
- Makeen, M. F. (2023). Defects in the moral rights regimes of the countries of the Middle East. *Arab Law Quarterly*, 39(1-2), 45-88. <https://doi.org/10.1163/15730255-bja10126>

- Manin, S., Sabikenov, S., & Manina, Y. (2024). Essence, concept, and types of national legislation in the field of information technology. *International Journal of Electronic Security and Digital Forensics*, 16(1), 1-13. <https://doi.org/10.1504/IJESDF.2024.136023>
- Mohamed, H. (2024). The iRobo-Surgeon conundrum: Comparative reflections on the legal treatment of intraoperative errors committed by autonomous surgical robots. *Law, Innovation and Technology*, 16(1), 194-217. <https://doi.org/10.1080/17579961.2024.2313802>
- Morgante, G. (2016). Criminal law and risk management: From tradition to innovation. *Global Jurist*, 16(3), 315-350. <https://doi.org/10.1515/gj-2015-0013>
- Qin, H. X., Wang, Y., & Hui, P. (2025). Identity, crimes, and law enforcement in the Metaverse. *Humanities and Social Sciences Communications*, 12(1), Article 194. <https://doi.org/10.1057/s41599-024-04266-w>
- Quattrocchio, S., Anglano, C., Canonico, M., & Guazzone, M. (2020). Technical solutions for legal challenges: Equality of arms in criminal proceedings. *Global Jurist*, 20(1), Article 20190058. <https://doi.org/10.1515/gj-2019-0058>
- Rigano, C. (2019). Using artificial intelligence to address criminal justice needs. *National Institute of Justice Journal*, 280, 1-10. <https://www.ojp.gov/pdffiles1/nij/252038.pdf>
- Ryberg, J. (2024). Sentencing, artificial intelligence, and condemnation: A reply to Taylor. *Criminal Justice Ethics*, 43(2), 131-145. <https://doi.org/10.1080/0731129X.2024.2373604>
- Sewilam, H. A. (2025). FinTech for the poor: The case of Egypt. *Arab Law Quarterly*. Advance online publication. <https://doi.org/10.1163/15730255-bja10187>
- Shalaby, A. G., AbdelAziz, G. M., & Kandeel, M. E. (2022). Using artificial intelligence to resolve disputes through online arbitration. In *2022 9th International Conference on Social Networks Analysis, Management and Security (SNAMS)*. IEEE. <https://doi.org/10.1109/SNAMS58071.2022.10062524>
- Shouaib, M., Eldakak, A., & Alabdouli, E. A. (2024). Effect of the civil law severability doctrine on administrative contract theory: A study of French and Egyptian laws. *Heliyon*, 10(6), Article 27995. <https://doi.org/10.1016/j.heliyon.2024.e27995>
- Solove, D. J. (2025). Artificial intelligence and privacy. *Florida Law Review*, 77(1), Article 1. <https://scholarship.law.ufl.edu/flr/vol77/iss1/1>
- Susskind, R., & Susskind, D. (2022). *The future of the professions: How technology will transform the work of human experts*. Oxford University Press.
- Taylor, I. (2023). Justice by algorithm: The limits of AI in criminal sentencing. *Criminal Justice Ethics*, 42(3), 193-213. <https://doi.org/10.1080/0731129X.2023.2275967>
- The Constitution of the United Arab Emirates. (n.d.). <https://uaelegislation.gov.ae/en/legislations/1000>
- Topchy, R., Ibrahim, A., & Hashish, A. (2025). The digital transformation of the legal system in the United Arab Emirates: A comparative study of judicial transformation of the UAE and GCC countries. *Court Law Review*, 1(1), 1-23. <https://doi.org/10.33327/CLR/3061-0907/2025/1-00008>
- Wu, W., & Lin, X. (2025). Access to technology, access to justice: China's artificial intelligence application in criminal proceedings. *International Journal of Law, Crime and Justice*, 81, Article 100741. <https://doi.org/10.1016/j.ijlcj.2025.100741>
- Završnik, A. (2020). Criminal justice, artificial intelligence systems, and human rights. *ERA forum*, 20(4), 567-583. <https://doi.org/10.1007/s12027-020-00602-0>