Research Journal in Advanced Humanities

RJAH

https://doi.org/10.58256/9xebs084

Open Access

Check for updates

RESEARCH ARTICLE

Section(s): *Digital Humanities; Legal Studies*

Violation of the right to privacy through artificial intelligence entities under the uae's anti-cybercrime act

Ashraf Fatehi Al-Rai[1], Nermin Maala[2], Ghenaa Almatri[3] & Maya Khater[4]*

[1]Public Law Department, College of Law, Abu Dhabi University, United Arab Emirates

[2]Public Law Department, College of Law, Abu Dhabi University, United Arab Emirates

[3]Dubai Customs and Ports, United Arab Emirates

[4] Public Law Department, College of Law, United Arab Emirates University, United Arab Emirates

*Correspondence: maya.khater@uaeu.ac.ae ORCID ID: 0000-0002-5892-9176

ABSTRACT

This study analyzes the legal framework for protecting the right to privacy, specifically in light of the widespread use of artificial intelligence (AI) technologies, within UAE legislation. The research centers on the extent to which substantive and procedural criminal protection is efficient and effective in addressing violations arising from the use of AI entities, especially given these systems' significant ability to collect and analyze vast amounts of personal data, thereby influencing the behavior of individuals in society. The study adopts an analytical and descriptive approach, supported by a comparative perspective. The findings indicate that the right to privacy is fundamental one that ensures individuals' control over their personal data and information. It was also found that AI technologies have created new forms of crimes, notably with the increasing spread of publishing personal images without consent and defamation through deep-fake technologies, which reflects the growing international concern that surrounds this issue. The study highlights the importance of enhancing societal awareness of digital privacy and the necessity of its protection, as well as recommending the establishment of specialized courts to handle cybercrimes. It also emphasizes the need to strengthen international cooperation to define the legal responsibilities of AI entities.

KEYWORDS: artificial intelligence, cybercrime, personal data protection, right to privacy, UAE Law

Research Journal in Advanced Humanities

Volume 7, Issue 1, 2026

ISSN: 2708-5945 (Print)

ISSN: 2708-5953 (Online)

ARTICLE HISTORY

Submitted: **4 January 2026**

Accepted: 28 **March 2026**

Published: 09 **April 2026**

HOW TO CITE

Al-Rai, A., Maala, N., Al-Matari, G., & Khater, M. (2026). Violation of the right to privacy through artificial intelligence entities under the uae's anti-cybercrime act. *Research Journal in Advanced Humanities, 7*(1). https://doi.org/10.58256/9xebs084

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

Introduction

The world is experiencing a rapid and unprecedented technological transformation, with artificial intelligence becoming increasingly present across all aspects of life (Adel et al., 2024; Qutieshat et al., 2026). As its applications continue to expand, this development is no longer merely a technological option but has evolved into a daily reality that shapes the experiences of individuals and societies. AI systems have become deeply embedded in modern practices and are now a core element of institutional functions and regulatory frameworks, reflecting their growing role in shaping both present realities and future directions (Al-Rai et al., 2026a).

Artificial intelligence technologies can process and analyze vast quantities of personal data extremely quickly (Abou Adel, 2022). This enhances their effectiveness in delivering advanced technological remedies and plays a pivotal role in supporting numerous sectors, particularly security, healthcare, and public services. Such developments, however, necessitate the establishment of appropriate legal frameworks to ensure the responsible and secure use of these technologies (El-Erian et al., 2026; Khater et al., 2025).

Despite the tangible benefits that AI technologies provide across multiple sectors, they raise simultaneous serious concerns over the protection of human rights, especially the right to respect for private life. Which is recognized as one of the fundamental rights guaranteed by national constitutions as well as international conventions and treaties. Consequently, regulating the use of AI technologies has become essential for maintaining a balanced relationship between technological innovation and the preservation of fundamental rights and freedoms (Al-Rai et al., 2026b).

Given the capacity of various AI systems and entities to collect, analyze, and process massive amounts of personal data, identify behavioural patterns, and even predict individual decisions and choices—sometimes influencing them—a new form of surveillance and intrusion into individuals' private lives has emerged. This new form of monitoring exceeds traditional surveillance methods significantly in terms of depth, precision, and scope.

Considering the contemporary technological environment, addressing the protection of private life from the potential interference of AI entities has become increasingly necessary. Privacy is considered one of the most significant personal rights protected under national legal systems and international instruments, as it guarantees individuals the freedom to shape their personal lives without unlawful interference and safeguards the confidentiality of their communications and personal affairs from unauthorized access or use (Nggilu et al., 2025).

By recognizing the importance of protecting the individual's right to privacy, this study aims to examine the criminal legal framework—both procedural and substantive—that provides protection against potential violations that may be committed or facilitated through artificial intelligence entities, with a specific emphasis on the legislative approach adopted by the United Arab Emirates.

The research focuses on assessing the extent to which substantive and procedural criminal laws are effective in protecting the right to privacy against violations arising from artificial intelligence entities.

It seeks to determine the adequacy and effectiveness of substantive and procedural criminal protection of the right to privacy in addressing offences committed through AI entities. In addition, it explores whether effective international legal provisions exist that provide procedural protection for personal data, thereby guaranteeing an individual's right to privacy. Finally, it examines the legislative stance of the United Arab Emirates concerning the protection of privacy and personal life within the digital environment.

It addresses the effectiveness of the substantive and procedural criminal protection afforded to private life by identifying various acts that constitute offences against privacy, analyzing the legal basis for their criminalization, and outlining the conditions and procedures required to protect this right against potential violations at the international level. It also aims to analyze the position of the UAE legislator in protecting the right to privacy within the digital environment against potential infringements.

The study adopts both analytical and descriptive approaches in examining the fundamental concepts related to private life and its inviolability, as well as the nature of artificial intelligence entities. It further analyzes relevant international legal provisions to identify forms of violations and offences affecting the right to privacy and to determine the legal basis for their criminalization and protection under criminal law. In addition, the study highlights and analyzes the legislative approach adopted in the United Arab Emirates concerning the protection of the individual's right to privacy and the inviolability of private life.

The Conceptual Framework of Privacy and Artificial Intelligence

The right to privacy is widely recognized as one of the fundamental rights that is closely connected to human personality and individual dignity. Considering the remarkable technological developments witnessed in recent years, notably in the field of artificial intelligence technologies, growing attention has been directed toward the protection of this right. This heightened concern arises from the unprecedented capacity of AI technologies to collect, analyze, and process vast quantities of personal information and data, thereby creating new challenges related to potential violations of individuals' private lives and their inviolability.

The right to a private life represents one of the most essential of an individual's rights. It is also a right shared equally among all persons: Just as every individual enjoys the right to privacy and the protection of their private life, others possess the same entitlement. Consequently, no individual has the authority or legal justification to interfere in the private life of another person, regardless of the form such interference may take (Al-Kaabi, 2021; Khater, 2023).

This article examines the conceptual framework of private life and artificial intelligence. The first section addresses the concept of the right to privacy by defining the right itself and identifying its essential elements. The second is devoted to explaining the concept of artificial intelligence and clarifying its meaning.

At the outset, it should be noted that the concept of "right," in terms of determining its nature, content, and elements, has long been the subject of debate among legal scholars due to differences in their theoretical schools and doctrinal approaches. Nevertheless, a general legal definition of a right may be derived thus: A right is a legal power granted by law to a specific person that enables them to demand a certain performance by another person or refrain from a particular act. This authority may relate to a material interest or a moral interest, and the law guarantees its protection (Jallad, 2013).

A right may also be defined as a legal authority arising from a relationship of a personal nature, enabling one person to require another person, or a group of persons, to realize a specific interest, whether voluntarily or through legal compulsion (Hassani, 2018). With regard to the right to privacy, legal scholarships offer numerous definitions. For example, one doctrinal view defines private life as everything that does not relate to public life, or in other words, all matters that are not considered part of the public sphere (Al-Ahwani, 1978).

However, this definition has been subject to criticism because it lacks clear criteria that could distinguish between what constitutes public life and what falls within the domain of private life. Another definition describes the right to privacy as the individual's right to solitude and intimacy, that is, the right to personal seclusion, confidentiality, and discretion (Al-Shahawi, 2005). Other legal scholars have defined private life as the sphere of personal conduct that must remain secure from interference by public authorities or third parties seeking to uncover any secrets associated with such behaviour (Sorour, 1986).

The right to privacy also refers to the individual's authority to determine how their personal life should be conducted in a manner that suits their preferences, with minimal interference from others. The individual retains the power to decide when, how, and to what extent information relating to their personal affairs may be disclosed to others. Any intrusion into such matters without the individual's consent constitutes an infringement upon their freedom and their right to the protection of their private life (Attia, 1977). It may be defined as the individual's right to enjoy a private life in complete confidentiality—whether in relation to family or social life—and to protect it from any form of unlawful interference, surveillance, disclosure, or intrusion by individuals or authorities. This includes the protection of the individual's home and all matters aligned with their personal life, thereby safeguarding human dignity and personal freedom.

This right encompasses several essential elements that must be protected from violations and encroachments. Article 12 of the Universal Declaration of Human Rights provides that no person shall be subjected to arbitrary interference with their privacy, family, home, or correspondence, nor to attacks upon their honour and reputation. In addition, every individual has the right to the protection of the law against such interference or attacks.Based on this principle, the core elements of the right to privacy include the inviolability of the home, the confidentiality of communications and correspondence, family and personal life, health-related information, personal images, and aspects of an individual's professional life.

One of the most prominent characteristics of the right to privacy, particularly in the digital environment, is that it is a personal right intrinsically linked to the individual's personality. Consequently, it cannot be

transferred, waived, sold, bequeathed, or otherwise disposed of. In common with other fundamental personal rights, it is not subject to prescription or limitation periods that would lead to its extinction over time (Hazzam, 2022). On the other hand, there is no single universally accepted definition of artificial intelligence that encompasses all its dimensions. Therefore, it is useful to examine the concept from both technical and linguistic perspectives, drawing on definitions found in Arabic and foreign dictionaries. From a technical perspective, artificial intelligence refers to a system or machine programmed through computer-based algorithms according to a set of rules designed to perform specific tasks or functions. Such systems receive inputs and process them automatically in a manner that corresponds to the instructions embedded within the program (Mamdouh, 2021).

Artificial intelligence is generally considered a broad and comprehensive concept encompassing a series of technological developments that have emerged over the past few decades. For this reason, no single definition adequately captures all of its aspects. Some Arabic lexicons explain the concept by first defining human intelligence as the ability to analyze, synthesize, distinguish, choose, adapt to different situations, and draw conclusions through reasoning and understanding. The term artificial, on the other hand, refers to something that is manufactured or created, rather than occurring naturally. Artificial intelligence may therefore be defined as the capacity of a machine or device to perform activities that normally require intelligence, such as logical reasoning, problem-solving, and self-correction (Al-Obaidi, 2022). The Merriam-Webster Dictionary defines artificial intelligence as: A branch of computer science dealing with the simulation of intelligent behaviour in computers. The capability of a machine to imitate intelligent human behaviour.

Similarly, the Oxford English Dictionary defines artificial intelligence as the theory and development of computer systems capable of performing tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and language translation. The Encyclopaedia Britannica defines artificial intelligence as the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. Based on these definitions, artificial intelligence may be broadly described as technology that seeks to simulate or replicate aspects of human intelligence through machines capable of performing tasks in a manner resembling human cognitive processes. Some scholars view AI as an application of computer science, while others consider it an independent field within computing. Its development accelerated significantly from the mid-1970s onwards, giving rise to numerous sub-disciplines and research areas, beginning with early attempts to simulate complex tasks such as playing chess (Ibrahim & Al-Rashid, 2022).

Artificial intelligence encompasses a broad range of technologies and capabilities, including perception, cognition, language processing, computational reasoning, decision-making, planning, and autonomous problem-solving. It is often preferable to view artificial intelligence not as a single technology but as a collection of tools and systems designed to enhance traditional human attributes such as intelligence, analytical capacity, and other cognitive skills (Al-Obaidi, 2022).

Artificial intelligence also has the potential to contribute significantly to the achievement of the United Nations Sustainable Development Goals, including sustainable economic development, social progress, and the promotion of justice and equality. Nevertheless, the deployment of such technologies may also generate wide-ranging social, economic, and ethical implications. For this reason, governments and international organizations have increasingly sought to promote the responsible use of artificial intelligence while simultaneously establishing strict regulatory frameworks concerning data protection, privacy, and ethical compliance.

AI systems rely heavily on the availability of vast amounts of information accessible through the internet and other public data sources, including human communications and interactions. These systems analyze such data using algorithms designed to simulate aspects of human cognitive processes. Through this process of large-scale data analysis and machine learning, AI systems can generate human-like text and performing tasks that resemble human reasoning and decision-making.

Despite extensive scholarly debate, it remains difficult to formulate a single comprehensive definition of artificial intelligence. However, from a legal scholarship perspective, artificial intelligence generally refers to systems capable of inference, acquiring new knowledge, applying learned information, perceiving and analysing surrounding environments, and improving performance through learning from previous experiences and examples. Notably, most national legal systems still lack explicit legislative provisions that specify the legal

nature or status of artificial intelligence. Nevertheless, certain legal scholars suggest that AI systems may be viewed as technologically distinct entities whose functions and characteristics can be assessed and regulated within existing legal frameworks (Zein, 2023).

The Legal Implementations and Violations of Privacy Through Artificial Intelligence

Since the right to privacy and the inviolability of private life constitute essential human rights and form the ethical foundation of many legal systems, it has become necessary for criminal law to provide explicit legal provisions and principles aimed at safeguarding this right and protecting it from unlawful interference. At the international level, numerous legal principles, conventions, and regulatory frameworks address acts that may constitute violations of the right to privacy, as well as the legal mechanisms available to prevent and remedy such violations. These legal structures are increasing their focus on contemporary technological developments—including crimes committed through modern technological tools and digital systems that may infringe upon human rights and individual privacy (Khater, 2024).

Major Offences Affecting Privacy through Artificial Intelligence

Based on the definitions previously presented covering the right to privacy and the concept of artificial intelligence, it becomes evident that AI systems operate through the processing and analysis of extensive volumes of data and information—procedures that inevitably require access to personal data that may relate to individuals' private lives. These systems function through technologies designed to simulate human cognitive abilities, including logical reasoning, analysis, learning, and inference. Consequently, the interaction between AI technologies and personal data raises complex legal questions over the protection of privacy, especially where criminal law is concerned.

Most of the data required for the operation of AI systems is of a personal nature, so obtaining such information must generally be contingent on the explicit consent of the individuals concerned. Any unauthorized access to or use of such data may constitute a criminal offence involving the violation of personal privacy. In this context, several forms of privacy-related offences may arise through the misuse of artificial intelligence technologies, including the following:

Surveillance and Electronic Eavesdropping

This category includes various forms of monitoring conducted through AI-enabled technologies that track individuals, their locations, or their personal activities. Examples include smart-home systems and voice-activated digital assistants such as Amazon Alexa or Google Home, which may collect extensive personal data while providing their services. Such data may subsequently be stored, analyzed, or used for purposes beyond those originally intended.

Similarly, tracking technologies and data-collection tools, such as cookies used by many websites employing AI-driven personalization systems, may gather substantial information about individuals' online behaviour. Although cookies are often used to improve user experience or deliver targeted advertising, they may also be misused in ways that violate individuals' privacy.

Publication of Personal Images Without Consent

One of the most common privacy violations in the digital environment involves the unauthorized publication or distribution of personal photographs. Personal images form an integral part of an individual's private life and must therefore be protected from misuse. Publishing such images without the explicit consent of the person concerned constitutes a violation of their right to privacy and may amount to a criminal offence in many legal systems.

Defamation and Reputational Harm Through Artificial Intelligence

Another form of privacy violation occurs when individuals exploit data collected through AI systems to fabricate or manipulate information to damage the reputation of others. This may involve publishing false or misleading information through social media platforms or other digital channels (AlOmran et al., 2025; Al-Rai et al., 2025).

Such offences may also involve the misuse of AI-based technologies, for instance deepfake technology, which can generate highly realistic but fabricated audio, video, or visual content. These manipulated materials may falsely depict individuals in compromising or misleading situations, thereby causing reputational harm, psychological distress, or public humiliation. The creation and dissemination of such content constitute a serious infringement upon personal privacy and dignity (Saleh, 2023).

International Efforts to Protect the Right to Privacy

The above offences are part of a broader context of international efforts aimed at strengthening the protection of the right to privacy. Numerous international conventions, treaties, and legal instruments emphasize the obligation of states to respect this right and to establish appropriate legal safeguards within their domestic legal systems. Among the earliest international initiatives in this field was the guidance issued by the United Nations in 1989 concerning the use of computer technologies in the processing of personal data, which sought to regulate mechanisms for data auditing and to ensure respect for privacy in an era of expanding technological capabilities.

Subsequently, the United Nations General Assembly adopted additional frameworks to address the regulation of personal data and privacy in the digital environment. The General Assembly's adoption of a resolution on "The Right to Privacy in the Digital Age," which highlighted the growing challenges presented by digital technologies to the protection of personal privacy, was a notable initiative. Further developments occurred in 2018, when the UN reaffirmed the importance of safeguarding the right to privacy within the digital environment as part of its broader commitment to protecting fundamental human rights.

These international initiatives emphasize that the protection of privacy must be maintained even in the context of rapid technological development. They also reaffirm the principles contained in the International Covenant on Civil and Political Rights, which recognizes the right of individuals to protection against arbitrary or unlawful interference with their privacy.

In addition to the United Nations, the European Union has played a prominent role in developing legal frameworks aimed at protecting personal data and privacy. These are some of the most significant legal instruments in this area:

- The Budapest Convention on Cybercrime, which established international cooperation mechanisms to combat cybercrime.
- The General Data Protection Regulation, widely regarded as one of the most comprehensive legal frameworks for the protection of personal data worldwide.
- The EU Artificial Intelligence Act, which represents one of the most advanced global regulatory initiatives governing the development and deployment of artificial intelligence technologies.

There have also been numerous efforts by international conferences and academic forums to address the issue of privacy protection in the face of technological advancement, focusing on strategies to strengthen legal safeguards and mitigate the risks posed by emerging digital technologies.

Procedural Criminal Protection of Private Life

Procedural protection represents the second form of criminal protection granted to rights. It differs from substantive criminal protection in that the latter focuses on criminalization and punishment by defining acts that constitute violations of rights and determining the penalties imposed for such acts. Procedural protection, by contrast, concerns the regulation of mechanisms and the procedures that must be followed to ensure the effective implementation of substantive protection, including the processes of investigation, trial, and the enforcement of judicial decisions.

Procedural protection therefore involves the establishment of practical and formal rules governing criminal investigations, as well as the principles that must be observed in order to safeguard interests deemed worthy of legal protection. It also encompasses a set of procedural guarantees designed to maintain a balance between the interests of society and the state on the one hand, and the rights and freedoms of individuals on the other, ensuring that such rights are protected without undue infringement (Al-Rai & AlOmran, 2026).

This chapter examines procedural criminal protection at the international level, and reviews its manifestations within the national legal framework applied in the United Arab Emirates. It seeks to clarify

the extent to which the principles embodied in Emirati legislation are consistent with those recognized in international legal scholarship and regulatory frameworks.

Procedural Criminal Protection at the International Level

Among the most significant legal instruments adopted at the international level to ensure the procedural protection of private life is the General Data Protection Regulation (GDPR), which represents a major change in personal data protection and digital privacy.

The GDPR introduced a set of clear, comprehensive, and stringent rules governing the processing and analysis of personal data. All entities that process personal data, whether operating within or outside the European Union, are required to comply with the principles established by the regulation whenever they process data related to individuals within the EU.

For example, Article 5 of the Regulation establishes several fundamental principles governing the processing of personal data. These include the principles of lawfulness, fairness, and transparency in data processing. Personal data must also be collected for specified, explicit, and legitimate purposes and must not be processed in a manner incompatible with those purposes. Additionally, the Regulation introduces the principle of data minimization, which requires that the personal data collected should be limited to what is necessary for the purposes for which it is processed. It also obliges data controllers to ensure the appropriate security of personal data, including protection against unauthorized or unlawful processing through suitable technical and organizational measures.

In addition, Article 7 of the Regulation requires that personal data should be processed based only on the explicit consent of the data subject, and the data controller must be able to demonstrate that such consent has been obtained. Article 9 further prohibits the processing of certain categories of sensitive personal data, including data relating to racial or ethnic origin, political opinions, religious beliefs, biometric or genetic data, as well as information concerning health, sexual life, or sexual orientation. Article 10 also restricts the processing of data related to criminal convictions and security measures, which may only be processed under the supervision of competent public authorities.

Article 33 of the Regulation contains a notably significant procedural safeguard: It requires data controllers to notify the competent supervisory authority of any personal data breach within 72 hours of becoming aware of the breach, particularly where such breach may pose a risk to the rights and freedoms of natural persons, including the right to privacy. Article 34 requires that the affected data subjects be informed of the breach without undue delay whenever the breach is likely to result in a high risk to their rights and freedoms.

The Legislative Position in the United Arab Emirates

The legislator in the United Arab Emirates has demonstrated significant readiness to address issues related to data protection and privacy in the digital environment (Al-Rai & AlOmran, 2024). This commitment is reflected in UAE Federal Decree-Law No. 45 of 2021 on Personal Data Protection, which establishes a comprehensive legal framework governing the collection and processing of personal data.

This law sets out several fundamental principles governing the processing of personal data, including the principles of lawfulness, fairness, transparency, and purpose limitation. Personal data must be collected for clearly specified and legitimate purposes and not be processed in a manner incompatible with those purposes. The data collected must be adequate, relevant, accurate, and limited to what is necessary for the purposes for which it is processed. The law also requires that such data be stored securely and protected from unauthorized access, misuse, or unlawful processing, and that it not be retained beyond the period necessary to achieve the purposes for which it was collected.

The law further obliges data controllers and processors to implement appropriate organizational and technical measures to ensure the protection of personal data and preserve its confidentiality and integrity. These measures must guarantee that personal data is protected from unauthorized access, alteration, destruction, or disclosure. Additionally, data controllers must ensure the deletion of personal data once the purpose of its processing has been fulfilled.

Another important procedural safeguard is the obligation imposed upon data controllers to notify the

competent authority and the concerned data subject of any breach or unauthorized access involving personal data where such breach may affect the individual's right to privacy or compromise the confidentiality and security of their personal information.

The UAE legislator also addressed privacy protection in the digital environment through UAE Federal Decree-Law No. 34 of 2021 on Countering Rumors and Cybercrimes—specifically Article 44—which criminalizes the use of information networks or technological systems with the intent to violate a person's privacy or interfere with their private or family life without their consent.

The provision identifies several acts that constitute such offences, including:

- Intercepting, recording, transmitting, broadcasting, or disclosing conversations, communications, or audio-visual materials without authorization.
- Taking photographs of others in public or private places, or creating, copying, publishing, or storing electronic images without consent.
- Publishing electronic news, images, comments, or information—even if accurate—with the intention of harming an individual.
- Capturing or publishing images of accident victims, the deceased, or victims of disasters without authorization from the concerned parties.
- Tracking or disclosing the geographical location data of individuals without authorization.

The UAE legislator also strengthened penalties for offences involving the digital manipulation of images or recordings with the intent to defame or harm individuals. Such acts may result in imprisonment for a period of not less than one year and a fine of not less than 250,000 UAE dirhams, reflecting the seriousness with which such offences are treated under the law.

The researcher considers that the provisions introduced by the UAE legislator constitute a strong deterrent against acts that infringe upon individuals' private lives. They also reflect a legislative approach aimed at protecting the constitutional right to privacy within the digital environment while keeping pace with contemporary technological developments through comprehensive and forward-looking legal regulation.

Conclusion

This study highlights the critical importance of substantive and procedural criminal protection in addressing crimes related to artificial intelligence systems and entities. It emphasizes the necessity for criminal protection to include guarantees for the confidentiality of personal data and its safeguarding against any potential violations, based on internationally recognized legal principles and standards at both the substantive and procedural levels. In this context, the research examines the legislative approach adopted in the United Arab Emirates concerning the protection of personal data, highlighting the extent to which UAE legislation aligns with international legal principles and contemporary regulatory developments.

The study concludes that the rapid development of AI technologies has led to the emergence of new forms of violations of the right to privacy, such as surveillance and eavesdropping, the unauthorized publication of personal images or information, reputational harm through the dissemination of misleading content, and the creation or dissemination of false information without the consent of the individual concerned. In response, international agreements and national legislation—especially in the United Arab Emirates—are working to establish comprehensive legal frameworks for the protection of personal data and digital privacy.

The study recommends strengthening public awareness programs, workshops, and training initiatives aimed at raising societal awareness of the risks associated with digital privacy. Greater international cooperation is also needed among legal scholars, criminal law experts, and specialists in technology and artificial intelligence to assess the legal status of AI-based systems, clarify their legal responsibilities, and establish clear standards for the admissibility and evaluation of digital evidence derived from AI technologies. Finally, the study recommends the establishment of specialized courts dedicated to cybercrime and technology-related offences in order to address the rapidly evolving nature of digital crimes and ensure that judicial systems are capable of effectively responding to offences arising from the misuse of modern technologies.

Funding:
The publication fees for this research were funded by Abu Dhabi University.

Acknowledgments:
The authors thanks Abu Dhabi University, Dubai Customs and Ports, and United Arab Emirates University for their guidance and assistance in preparing this research.

Conflicts of Interest: The authors declare no conflict of interest.

Author Biodata
Dr. Ashraf F. Al-Rai is an accomplished legal scholar with over 20 years of experience in Criminal Law, Cybercrime, Media Law, and Artificial Intelligence. He holds a Ph.D. in Criminal Law and is pursuing a second Ph.D. in International Criminal Law at the Autonomous University of Madrid. He is an Assistant Professor at Abu Dhabi University and a former Visiting Scholar at the University of Malaya. Dr. Al-Rai has authored 8 books and published widely in Scopus-indexed journals. His work focuses on digital legislation, AI, cyberlaw, and hate speech, integrating law, technology, and media to advance ethical AI and digital governance.

Dr. Nermin Maala is an Assistant Professor of Public Law, Abu Dhabi University | Associate Professor of Criminal Law, Alexandria University. She earned her Ph.D. in Law from Alexandria University. Throughout her career she has held pivotal leadership roles, including Managing Director of English and French Legal Programs and Deputy Director of the Alexandria Center for Arbitration. Her research and teaching portfolio is diverse, covering UAE Criminal Procedure Law, International Criminal Law, Criminology, and Administrative Law. She is also recognized for her contributions to training police personnel and supervising advanced post-graduate research (Master's and Ph.D. levels).

Dr. Ghanaa Al Matri is an Emirati legal expert specializing in customs law, criminal law, and digital transformation. She has built her career at Dubai Customs since 2006, currently serving as a Senior Legal Researcher in customs investigations. She holds a Ph.D. in Law and is pursuing further studies in Sharia and judicial fields. She also holds professional certifications in legal consultancy, arbitration, and digital innovation. Her work focuses on customs crimes, legal compliance, and integrating law with modern technologies.

Dr. Maya Khater is an Associate Professor of Public International Law at the College of Law, United Arab Emirates University (UAEU). She holds a PhD in Law from Damascus University in 2011. Throughout her career, she has held several academic and administrative positions, including Vice Dean for Admission, Registration, and Student Affairs, and Assistant Dean of the College. Dr. Maya has taught law courses in both Arabic and English. Her areas of expertise include Public International Law, Human Rights Law, International Humanitarian Law, Artificial Intelligence and Law, and International Environmental Law.

Authorship and Level of Contribution
Ashraf Al-Rai: Writing: Original draft; conceptualization; literature review; drafting the introduction and conceptual framework; methodology development; supervision.

Nermin Maala: Comparative legal analysis; organizational analysis; draft review; data interpretation.
Ghina Al-Matari: Comparative legal analysis; organizational analysis; draft review; academic editing.
Maya Khater: Research design; comparative methodology; integrating the ethical and responsibility frameworks; final draft review; and correspondence.

References

Abou Adel, M. (2022). Towards an advanced interactive e-learning for the language. Arab World English Journal (AWEJ), Special Issue on CALL, (8), 330–340. https://dx.doi.org/10.24093/awej/call8.22

Adel, M. A., Boudjadi, K., Abouelnour, M. M., & Alhourani, M. I. (2024). The contribution of smartphone apps to develop teaching the Arabic language "Arabic is my language's app" as a sample. Forum for Linguistic Studies, 6(6), 1175–1190. https://doi.org/10.30564/fls.v6i6.7408

Al-Ahwani, H. K. (1978). The right to respect for private life: The right to privacy (A comparative study). Cairo, Egypt: Dar Al-Nahda Al-Arabia.

Al-Kaabi, A. S. (2021). Criminal protection of the right to private life in light of the Qatari legislation on combating cybercrime. Qatar: College of Law, Qatar University.

Al-Obaidi, O. A. K. (2022). Contemporary applications of crimes resulting from artificial intelligence (1st ed.). Egypt: Arab Center for Publishing and Distribution.

AlOmran, N. M., Al-Rai, A., & Alhendi, N. I. (2025). Freedom of expression and criminal liability for journalists under Jordanian legislation. Constitutional Review, 11(1), 118–165. https://doi.org/10.31078/consrev1115

Al-Rai, A. F., & AlOmran, N. M. (2024). Criminal protection of electronic signatures from forgery in Jordanian and UAE legislation. International Journal of Electronic Governance, 16(2), 246–262. https://doi.org/10.1504/IJEG.2024.140786

Al-Rai, A. F., & AlOmran, N. M. (2026). Constitutional protections in utilising artificial intelligence systems for investigating and inferring crimes: A comparative study. International Journal of Electronic Security and Digital Forensics, 18(1), 108–124. https://doi.org/10.1504/IJESDF.2026.150188

Al-Rai, A. F., AlOmran, N. M., & Al Ansari, M. A. J. (2025). 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

Al-Rai, A., Imad, D., & Khater, M. (2026a). The legal regulation of cybercrimes related to character assassination under the Jordanian and French legislation. F1000Research, 15, 359. https://doi.org/10.12688/f1000research.177079.1

Al-Rai, A., Maala, N., & Khater, M. (2026b). The authority of Jordanian criminal judge in evaluating evidence derived from artificial intelligence systems. Scientific Culture, 12(2.1), 4501–4510. https://doi.org/10.5281/zenodo.19010702

Atiya, N. (1977, October). The right of individuals to their private life. Journal of Government Legal Affairs, Issue 4.

Cambridge Dictionary. (n.d.). Artificial intelligence. Retrieved from https://dictionary.cambridge.org/dictionary/english/artificial-intelligence

Council of Europe. (2001). Convention on cybercrime (No. 185). Budapest.

El-Erian, M., Imad, D., Sulaiman, S., Qutieshat, E., & Khater, M. (2026). The role of artificial intelligence in enhancing corporate governance and achieving sustainable development. Access to Justice in Eastern Europe, 9(1), 208-232. https://doi.org/10.33327/AJEE-18-9.1-a000177

European Union. (2016). General data protection regulation (EU) 2016/679. Retrieved from http://gdpr-info.eu/

European Union. (n.d.). EU artificial intelligence act. Retrieved from https://artificialintelligenceact.eu/

Fadlila, A. (2012). Legal protection of the right to privacy: A comparative study. Constantine: Faculty of Law, University of the Mentouri Brothers.

Fidler, D. (2015, March). The right to privacy in the digital age: Where do things stand? Retrieved from https://www.cfr.org/blog/right-privacy-digital-age-where-do-things-stand

Hassani, M. N. (2018). Explanation of the criminal law – Special part (6th ed.). Cairo, Egypt: Dar Al-Nahda Al-Arabia.

Hazam, F. (2022). The right to private life in the digital environment: A comparative study. Journal of Comparative Legal Studies, 8(1).

Ibrahim, T., & Al-Rashid, S. T. (2022). Crimes of artificial intelligence entities (1st ed.). United Arab Emirates: Scientific Renaissance Publishing House.

Jallad, S. (2013). The right to privacy between guarantees and controls in Algerian legislation and Islamic

jurisprudence. Algeria: University of Oran.
Khater, M. (2024). Electronic intellectual terrorism and the Islamic efforts to combat it. Islamic Quarterly Journal, 68(1), 59–82.
Khater, M. H. (2023). International perspective on securing cyberspace against terrorist acts. International Journal of Sociotechnology and Knowledge Development, 15(1), 1–11. https://doi.org/10.4018/IJSKD.318706
Khater, M., Aboelazm, K. S., Imad, D., Chami, Y., & Aly, H. (2025). The role of assistive technology in reinforcing the rights of persons with disabilities to employment from a legal perspective. International Journal of Law and Management. Advance online publication. https://doi.org/10.1108/IJLMA-04-2025-0151
Mamdouh, K. (2021). The legal regulation of artificial intelligence (1st ed.). Egypt: Dar Al-Fikr Al-Jami'i.
Nggilu, N. M., Chami, Y., & Khater, M. (2025). Constructing humanitarian-based law: A philosophical analysis of the philanthropic legal paradigm. Yustisia Jurnal Hukum, 14(3), 283–311. https://doi.org/10.20961/yustisia.v14i3.98924
Qutieshat, E., Al Adwan, M., Alshibli, A., Chami, Y., & Khater, M. (2026). Governing legal chatbots: Ethics, professional responsibility, and liability in comparative perspective. Research Journal in Advanced Humanities, 7(1). https://doi.org/10.58256/ppfy4k96
Saleh, Z. (2023, September). The danger of artificial intelligence to the right to privacy and the right to work. Retrieved from https://www.fdhrd.org
Serour, A. F. (1986). Criminal protection of the right to the inviolability of private life. Cairo, Egypt: Dar Al-Nahda Al-Arabia.
Shafii, I. H. (2019). Criminal liability for artificial intelligence crimes: A comparative study. Journal of Legal and Economic Research, 2(3), 479–666.
Shahawi, M. (2005). Criminal protection of the inviolability of private life. Cairo, Egypt: Dar Al-Nahda Al-Arabia.
United Arab Emirates. (2021). Federal decree-law no. 34 of 2021 on combating rumours and cybercrimes. Retrieved from https://uaelegislation.gov.ae
United Arab Emirates. (2021). Federal decree-law no. 45 of 2021 on personal data protection. Retrieved from https://uaelegislation.gov.ae
United Nations General Assembly. (2018). The right to privacy in the digital age (A/RES/73/179). Retrieved from https://digitallibrary.un.org/record/1661346
United Nations. (1948). Universal declaration of human rights. Retrieved from https://www.un.org/en/about-us/universal-declaration-of-human-rights
United Nations. (2013, December 20). The right to privacy in the digital age. Retrieved from https://news.un.org