The Phenomenon of Misuse of Artificial Intelligence Techniques

ظاهرة الانحراف عن تقنيات الذكاء الاصطناعي



Bedri Faiçal [1*] **Kabouh Lessaad**, [2]

[1] Faculty of Law, University of Algiers 1, Algeria

f.bedri@univ-alger.dz

https://orcid.org/0009-0008-7040-5544

[2] PhD student, Faculty of Law, University of Sfax, Tunisia

kabkrimo@gmail.com

https://orcid.org/0009-0006-6550-4818

Date of transmission: 11/03/2026 date of acceptance: 25/05/2026 date of publication: 01/06/2026

****

Abstract:

This study examines the phenomenon of misuse of artificial intelligence techniques from a specialized criminal law perspective. It adopts a descriptive-analytical method to review and analyze the relevant legal provisions and doctrinal literature, and it also draws on a comparative approach to examine selected foreign legislative experiences and policy models in this field. The study concludes that misuse of AI technologies represents an expanding threat that calls for a comprehensive, integrated response at the legal, technical, institutional, and ethical levels. While existing laws can accommodate certain manifestations of this misuse, they require substantive development to keep pace with rapid technological change. Prevention and public awareness are likewise central to curbing the phenomenon, alongside effective prosecution and deterrent sanctions.

key words: misuse of artificial intelligence techniques; AI-related crimes; criminal liability; cybercrime

الملخص

تناولت هذه الدراسة ظاهرة الانحراف عن تقنيات الذكاء الاصطناعي من منظور قانوني جنائي متخصص. واعتمدت الدراسة على المنهج الوصفي التحليلي لاستعراض وتحليل النصوص القانونية والمراجع الفقهية المتعلقة بالموضوع، كما استعانت بالمنهج المقارن للاطلاع على التجارب والتشريعات المقارنة في هذا المجال. توصلت إليها الدراسة تؤكد على أن ظاهرة الانحراف عن تقنيات الذكاء الاصطناعي تشكل تهديداً متزايداً يتطلب مواجهة شاملة ومتكاملة على المستويات القانونية والتقنية والمؤسسية والأخلاقية. وأن القوانين الحالية، رغم صلاحيتها لاستيعاب بعض صور الانحراف، إلا أنها بحاجة إلى تطوير جوهري لمواكبة سرعة التطور التكنولوجي. كما أن الوقاية والتوعية تلعب دوراً محورياً في الحد من هذه الظاهرة، إلى جانب الملاحقة القضائية الفعالة والعقاب الرادع.

الكلمات المفتاحية: الانحراف عن تقنيات الذكاء الاصطناعي، جرائم الذكاء الاصطناعي، المسؤولية الجنائية، الجرائم الإلكترونية

* **Corresponding Author**

Introduction:

The contemporary world is experiencing an unprecedented technological transformation driven by artificial intelligence (AI). These technologies are now woven into most spheres of human activity, reshaping the economic, social, and legal arrangements of modern societies[1]. At the same time, AI has delivered tangible gains in daily life, improving the quality and efficiency of services in sectors such as healthcare, education, industry, and security. This rapid diffusion, however, has brought with it a parallel set of legal and criminal law challenges that existing frameworks were not designed to confront in full.

Within this broader context, a more troubling development has become increasingly visible: the diversion of AI technologies from lawful objectives by certain individuals and groups, and their deployment in criminal conduct. AI therefore operates as a double-edged instrument. It can support crime prevention and anticipatory security practices, yet it can also function as an enabling infrastructure for emerging forms of criminality marked by technical sophistication and heightened harmfulness. The result is a set of foundational questions for criminal law, particularly whether traditional doctrines can accommodate these new offence patterns, and whether current statutory provisions remain adequate for defining AI-related crimes and allocating criminal liability.

AI misuse poses a direct challenge to contemporary criminal law because offences committed through these systems display features that complicate criminalization and prosecution[2]. Offender anonymity, the transboundary character of the conduct, evidentiary fragility, and the potential involvement of multiple actors (developer, manufacturer, operator, user) together unsettle conventional attribution models and necessitate a reconsideration of conventional legal concepts.

Research Problem

The study's core research problem is framed in the following terms: how can criminal law respond to the misuse of artificial intelligence technologies, and how far are existing criminal provisions capable of addressing the newly emerging

[1] Jassas, Loubna, and Murad Shihmat. "Artificial Intelligence and Crime: Between Enablement and Prevention." *Algerian Journal of Humanities and Social Sciences*, vol. 8, no. 2, 2024, p. 63.

[2] Al-Miri, Abd al-Razzak Ahmad Mouhammad. *Criminal Liability for Artificial Intelligence Crimes*. Arab Democratic Center, Berlin, 2024, pp. 12–18.

offences committed through these technologies? From this central problem flow several subsidiary questions :

1. What is meant by the misuse of AI technologies, and what are its principal forms and manifestations?
2. What factors contribute to the diversion of individuals and groups from lawful uses of AI technologies toward criminal ends?
3. How can criminal liability be determined where multiple actors participate in the development and use of AI?
4. Which substantive and procedural criminal law mechanisms are capable of addressing this phenomenon and limiting its spread?

The study contributes to Arabic legal scholarship by engaging a contemporary subject that has not yet attracted sustained attention in Arab research. It also develops a rigorous analysis of the relationship between technological development and evolving criminal phenomena. Practically, the discussion offers insights that may assist legislators in drafting provisions calibrated to AI-related offences, and it may support judges and investigators in grasping the evidentiary structure of these crimes and the mechanisms through which they can be established in criminal proceedings. The study is undertaken at a time when AI adoption is accelerating globally, which makes sustained criminal law analysis of these technologies an immediate and pressing necessity.

This study pursues several objectives. It first seeks to define the misuse of AI technologies and to specify the characteristics that distinguish this phenomenon in criminal law terms. It then identifies the principal forms of misuse and the types of offences committed through AI techniques. In addition, it analyzes the factors and drivers that contribute to the spread of such conduct, before examining the legal foundations for criminal liability in AI-related crimes.

The study adopts a descriptive-analytical approach by presenting the concept of misuse of AI technologies, analyzing its main forms, and examining the legal texts most directly relevant to the subject. It is complemented by a comparative method that reviews selected foreign criminal legislation addressing AI-related offences, with the aim of drawing on international experiences and identifying transferable best practices[1].

Structure of the Study

[1] Abd al-Aziz. “Criminal Liability for Artificial Intelligence Crimes.” Master’s thesis, University of Batna, 2024, pp. 3–5.

The study is organized into two main sections:

- **Section One: The conceptual framework of misuse of AI technologies.** This section comprises two subsections. The first defines the concept, its legal nature, and the contributing factors. The second surveys key manifestations of misuse in offences affecting persons and property.
- **Section Two: The criminal law response to misuse of AI technologies.** This section also comprises two subsections. The first examines criminalization, punishment, and criminal liability. The second tackles preventive measures and criminal law countermeasures.

Section One: Conceptual Framework for AI Misuse

This section sets out the theoretical and conceptual foundations for understanding the misuse of artificial intelligence techniques from a specialized criminal law perspective. It seeks to define the nature of this misuse and distinguish it from conventional forms of criminality, to analyze the multiple factors that drive it, and to outline its most salient manifestations across different domains. It also serves as a necessary introduction to the subsequent section, which examines the criminal law response to this phenomenon.

Subsection One: Concept and Nature of AI Misuse

Part One: Definition and Distinctive Features

Misuse of artificial intelligence techniques may be understood as the deployment of these technologies, or their outputs, in ways that exceed either the lawful purpose defined by legislation or the functional purpose for which the systems were designed. In operational terms, this misuse typically consists in leveraging AI's computational and analytical capacities to perpetrate criminal conduct, to facilitate its commission, or to conceal its effects and traces. It may arise through several modalities, including the use of intelligent algorithms to commit offences against persons, property, and public interests, as well as the use of AI tools to infringe privacy or circumvent the security protections of information systems[1].

This phenomenon departs from conventional patterns of criminality in ways that carry clear doctrinal implications for criminal law:

1. Transnational reach: offenders may act from within one state while targeting victims in other jurisdictions, complicating territorial competence, jurisdictional allocation, and the identification of the applicable law.

[1] Jassas, Loubna, and Murad Shihmat, *op. cit.*, pp. 63–76.

2. Anonymity and constraints on traceability: digital environments facilitate concealment of identity, impersonation, and the relatively swift erasure of evidentiary traces.
3. Partial or full system autonomy: where an AI system operates with limited or no direct human intervention, attributing criminal responsibility becomes less straightforward and may require re-examining established notions of agency.
4. Automation and scalability: once configured to execute a specific offence or exploit a defined vulnerability, an AI-enabled system can replicate the same conduct at exceptional speed and across a wide victim set[1].

Part Two: Drivers of Misuse of Artificial Intelligence Techniques

The phenomenon of AI misuse is shaped by a set of interacting factors that reinforce one another and collectively structure this pattern of offending. These drivers may be grouped into three principal dimensions:

1. **Individual dimension and personal motivations:** The motivations leading individuals to divert AI technologies toward criminal ends are heterogeneous. They include the illicit pursuit of rapid financial gain, particularly among those facing economic pressure or seeking wealth without lawful effort. They also include intent to harm others, whether grounded in personal hostility or retaliatory aims. In other cases, curiosity and the desire to test technical capacity, including the display of competence through breaching security systems[2], function as sufficient incentives. Social, cultural, and educational backgrounds further condition how these motivations form, and permissive ethical orientations may facilitate the rationalization of criminal conduct.
2. **Technical dimension and accessibility:**

   The broad diffusion of AI and the relative ease of obtaining tools and expertise operate as major enabling conditions. Many intelligent algorithms and applications are available online at low cost, including open-source resources that require limited financial investment. Technical knowledge has also become widely accessible through online learning platforms and free academic courses. Remote operation, often conducted behind multiple interfaces, can reduce the likelihood of identifying the offender's identity

[1] Ibrahim, Mouhammad. "The Security and Societal Risks of Deepfakes and Response Mechanisms." *Journal of Law*, Alexandria University, 2025, pp. 45–78.

[2] Mahmoud, Mahmoud Abd al-Aziz. "The Repercussions of Cybercrime from the Perspective of Victims in Saudi Society." *Journal of Social Sciences Studies*, King Saud University, 2023, pp. 120–145.

or location. Moreover, AI systems permit offences to be executed rapidly and at scale, thereby increasing both potential profit and the magnitude of resulting harm[1].

3. **Legal and institutional dimension:**

This dimension reflects the limits of traditional criminal law provisions and the lag in legislative adaptation to technological change. Core penal codes were drafted before AI became operationally significant and therefore provide few specialized rules tailored to this mode of offending. Legislative gaps and legal ambiguities may create avenues for offenders to evade criminal liability. Institutional constraints further intensify these vulnerabilities: law enforcement and judicial bodies may face resource limitations, insufficient specialized training in cyber-enabled crime, and weak international cooperation. Together, these constraints can reduce the effectiveness of prosecution and punishment, sustaining the incentives that continue to drive misuse[2].

Subsection Two: Manifestations of Misuse of AI Techniques

Part One: Misuse in Offences Against Persons and Private Life

Offences against persons constitute a principal setting in which artificial intelligence techniques are diverted to unlawful purposes. One of the most visible illustrations is deepfake technology, which relies on deep learning algorithms and artificial neural networks to generate synthetic digital content that can appear highly authentic. In operational terms, deepfakes are used to produce falsified video or audio recordings attributed to real individuals, typically to defame, blackmail, damage reputations, or destabilize victims' professional and family lives[3]. Documented incidents also confirm the creation of fabricated pornographic material attributed to victims without their knowledge or consent, a practice that often produces acute psychological and social harm.

A further form of misuse involves digital identity impersonation. Here, offenders deploy AI-enabled tools to create counterfeit accounts and profiles under the names of real persons across social media and other digital platforms. These false identities may be used to lure victims, cultivate trust as a preliminary step toward exploitation, or perform acts in the victim's name that undermine

---

[1] "Latest Cybercrime Statistics." *Center for Artificial Intelligence and Cybersecurity Studies*, 2025, pp. 34–56.

[2] Al-Hayti, Ruslan Ahmad. "Artificial Intelligence and Serious Cybercrimes: A Study of Emerging Threats." *Journal of Security Studies*, 2024, pp. 78–102.

[3] Al-Sharkawi, Osama. "Deepfake Technology in Phishing Attacks." *Cerebra Cybersecurity Center*, 2025.

reputation. In more technically elaborate cases, impersonation becomes an entry point for targeted fraud through spear phishing, where messages are tailored on the basis of analysis of the victim's personal data and behavioural patterns, thereby encouraging disclosure of sensitive information or inducing illicit financial transactions[1].

Misuse also appears in cyber extortion, understood as coercively obtaining money or information from individuals or firms by threatening to disclose private matters or confidential data via social media platforms[2]. AI enables more advanced variants by learning the victim's digital behaviour, mapping interests and personal relationships, and generating customized extortion messages designed to increase the likelihood of compliance.

Related conduct arises in cyberstalking, where AI systems, facial recognition technologies, and automated tracking are used to analyze online activity and monitor movements, interests, and patterns of digital interaction. The resulting information can then be mobilized to harass, threaten, or extort victims in ways that may be difficult to detect at early stages. In higher-risk contexts, geolocation techniques are used to trace victims in the physical world, creating a direct threat to life and bodily safety[3].

Part Two: Misuse in Offences Against Property and Institutions

The financial and economic domain is among the spheres most routinely targeted by AI-enabled misuse. Algorithmic trading systems, for instance, can be leveraged in sophisticated fraudulent operations that manipulate the prices of stocks, currencies, or digital assets at high speed. This conduct frequently takes the form of market manipulation, where rapid, fictitious buy and sell orders are placed to generate artificial volatility, allowing offenders to profit from price movements they have intentionally produced in accordance with their market positions[4].

AI techniques are also deployed to exploit vulnerabilities in electronic payment systems. Intelligent applications can identify weaknesses in security protocols and execute unauthorized transfers, moving funds through complex networks of fictitious accounts and fragmenting amounts into smaller transactions

---

[1] Moustafa, Muhammad Ali. "The Legal Nature of Online Defamation Committed through Artificial Intelligence Tools." *Journal of Legal Studies*, Zagazig University, 2024, pp. 156–189.
[2] Saleh, Ramadan. "The Criminal Law Response to Cyber Extortion and Violations of Private Life." *Journal of Law*, 2024, pp. 210–245.
[3] Moussa, Mouhammad Abd al-Rahman. *Artificial Intelligence and Legal Liability for Acts Resulting Therefrom*. Modern Legal Consultations Office, 2025.
[4] *Artificial Intelligence and Serious Cybercrimes*. European Applied Research Laboratory for Artificial Intelligence and Security, 2024.

to conceal their true origin. This practice is commonly described as digital money laundering.

Another recurrent manifestation concerns the forgery of documents and digital signatures. Through generative AI, offenders can generate contracts, invoices, certificates, and digital signatures with a level of verisimilitude that complicates detection. These capacities facilitate fraud against individuals and institutions, particularly in contexts where electronic transactions are increasingly routine but verification mechanisms remain insufficiently robust[1].

At the institutional level, misuse extends to AI-powered ransomware. In such cases, AI-supported malicious software is engineered to adapt to conventional defensive environments and bypass intrusion-detection systems. Attacks may involve exfiltrating sensitive data or encrypting it and then demanding ransom for decryption, disrupting essential services and organizational information systems. In parallel, intelligent tools may be used to extract large databases and confidential information from corporate, financial, and governmental entities, thereby creating serious risks to economic security and national security[2].

Henceforth, these forms of misuse in offences affecting property and institutions are diverse and technically complex. They often presuppose advanced expertise and specialized knowledge, which amplifies the risks posed to the economic and security stability of states and organizations.

Section Two: Criminal Law Responses to the Misuse of AI Techniques

Building on Section One, which defined the misuse of artificial intelligence techniques, clarified its legal character, and mapped its principal manifestations, this section turns to the applied question of criminal law response. That question has become more pressing as AI systems develop rapidly and are increasingly implicated in criminal conduct. Criminal justice systems are therefore required to pursue two parallel lines of action: refining the rules that govern criminalization and punishment, while also strengthening preventive and enforcement capacities. For this reason, the section is structured into two subsections. The first examines criminalization and punishment in relation to AI misuse; the second tackles prevention and criminal countermeasure mechanisms.

---

[1] Mahmoud, Baha al-Din. “Preventing Fraudulent Content: A Deepfake Detection Program.” ComplyCube, 2025.

[2] Al-Bediri, Mouhammad. “Risks Associated with the Use of Deepfakes by Terrorist Organizations.” *International Journal of Security Studies*, United Arab Emirates University, 2024, pp. 88–125.

Subsection One: Criminalization and Punishment for Misuse of Artificial Intelligence Techniques

Part One: Criminal Provisions Applicable to AI-Related Offences

Criminal justice systems face a sustained difficulty in dealing with AI-related offences because general penal code provisions were not drafted to accommodate this increasingly prevalent form of technologically mediated criminality. Even so, a broad range of AI-enabled conduct can still be prosecuted under traditional offences, so long as the statutory elements are satisfied. Fraud committed through intelligent algorithms, for example, remains governed by the ordinary provisions on fraud. Likewise, defamation and insult carried out through deepfake techniques fall within offences designed to protect honour and reputation[1].

In practice, however, this reliance on general rules reveals structural constraints. One persistent challenge concerns proof of *mens rea* in offences executed through automated processes, particularly where direct human intervention is not present at each operational stage. Causation poses comparable problems: when the technical sequence is complex, linking the criminal result to a specific actor's conduct becomes more demanding both legally and evidentially. The principle of legality, captured in the maxim "no crime and no punishment without a legal provision," further narrows the space for prosecution when new forms of conduct are not expressly addressed by the legislature. The consequence is a set of normative gaps that offenders may exploit to evade liability[2].

Against this backdrop, many legal systems have moved toward specialized frameworks for cybercrime and information technology offences, designed to capture at least some forms of technology-enabled wrongdoing. In Algeria, Law No. 09-04 on the special rules for the prevention of and fight against offences connected to information and communication technologies criminalized a range of acts involving attacks on information systems and personal data. In Egypt, Law No. 175 of 2018 on combating information technology crimes introduced offences related to the integrity of data, information, and information systems. In the United Arab Emirates, Federal Decree-Law No. 34 of 2021 on combating rumours and cybercrimes introduced criminal provisions directed at the use of modern technologies in criminal activity.

---

[1] Ben Ouda, Haskar. "The Problem of Applying Rules of Criminal Liability to Artificial Intelligence Crimes." *Journal of Legal and Political Research*, Saida University, 2022, pp. 115–130.

[2] Bouznoun, *op. cit.*, p. 67.

At the international and comparative levels, legislative approaches have also shifted toward more comprehensive regulation of AI use. The European Union's Artificial Intelligence Act (AI Act), issued in 2024, is a prominent example: it adopts a risk-classification model to calibrate regulatory oversight, prohibits certain high-risk uses, and imposes stringent obligations on developers and operators. In parallel, the United Nations concluded in 2024 a Convention on Combating Cybercrime, presented as the first binding international instrument in this area, which includes provisions on criminalizing conduct committed through modern technologies and mechanisms for international cooperation in identifying, tracing, and prosecuting offenders[1].

Part Two: Criminal Liability for AI Techniques Misuse

Criminal Liability for AI-Related Offences

Attributing criminal liability in AI-related offending remains one of the most contested issues in contemporary criminal law. The difficulty is not merely technical; it is structural. AI systems are typically produced, deployed, and maintained through a chain of actors, and that architecture can blur responsibility, especially when harmful outcomes emerge from interactions between design choices and downstream use. For this reason, criminal law scholarship generally works with a differentiated attribution model, identifying several potentially responsible parties, notably the programmer or developer, the manufacturer, the operator, and the end user. Liability is then assessed in light of each actor's role and the extent of causal contribution[2].

Liability on the part of the programmer or developer becomes plausible when a design defect or a coding decision is directly implicated in the commission of the offence, whether the defect reflects intent or negligence. Where the algorithm is deliberately designed to facilitate criminal conduct, the developer's responsibility may align with that of a principal offender. If, instead, the relevant defect is traceable to negligent design or a failure to adopt necessary precautions, liability may arise on the basis of non-intentional fault, provided the legal conditions governing negligence-based responsibility are satisfied. The operator's or owner's liability can likewise be engaged, either when the system is knowingly

[1] Dahshan, Yasser Ibrahim. "Criminal Liability for Artificial Intelligence Crimes." *Journal of Sharia and Law*, College of Law, United Arab Emirates University, 2020, pp. 215–280.

[2] United Nations Office on Drugs and Crime (UNODC). *United Nations Convention on Cybercrime*. Hanoi, October 2024.

used for unlawful purposes or when oversight duties are not discharged and that omission materially contributes to criminally relevant harm[1].

End-user liability is typically the least ambiguous: it arises where the user intentionally deploys AI techniques to commit offences, for example by using deepfake tools to blackmail or defame victims. In such cases, the user bears full criminal liability as a principal offender, while the AI system functions as an instrument under the user's control. Some scholars have nonetheless proposed attributing criminal responsibility to AI itself in scenarios of complete operational autonomy. This position faces foundational obstacles under prevailing doctrine, most notably the premise that criminal responsibility presupposes free will and cognitive capacity, attributes that automated systems are not recognized to possess according to current laws[2].

An AI-mediated offence remains governed by the general constituent elements of crime, although technological particularities often sharpen the doctrinal questions. The *actus reus* consists of criminal conduct that may take the form of a positive act, such as using an algorithm for hacking or fraud, or an omission, such as failing to adopt necessary safeguards to prevent harm. It also requires a criminal result and a causal link between conduct and result. The *mens rea* consists of intent, including knowledge and volition in intentional offences, or negligence in offences grounded in breach of a duty of care. Sanctions vary with the gravity of the conduct and the seriousness of the harm. They range from fines to imprisonment and may include supplementary penalties, including confiscation of devices and software used in the offence, or prohibition from engaging in a specific activity[3].

Subsection Two: Mechanisms of Prevention and Criminal Countermeasures

Part One: Procedural Mechanisms for Addressing the Misuse of Artificial Intelligence

Detecting and investigating AI-related crimes requires specialized technical capabilities that go beyond the traditional methods used for ordinary offences. The digital nature of these crimes obliges investigators to master digital analytics, handle electronic evidence competently, and understand how algorithms and

[1] Zaoui, Manal. "Criminal Liability for the Use of Artificial Intelligence." Master's thesis, University of Skikda, 2024, pp. 45–60.
[2] Abd al-Aziz, *op. cit.*, pp. 78–95.
[3] "Issues in the Use of Artificial Intelligence in Criminal Investigations." Master's thesis, University of Ghardaia, 2023, pp. 102–118.

intelligent systems operate. Many states have therefore established dedicated cybercrime units, staffed with qualified technical personnel and equipped with advanced tools capable of tracing offenders and collecting and analyzing digital evidence. AI itself has also contributed to the development of criminal investigative tools, notably through machine-learning algorithms used to process large datasets, detect criminal patterns, and anticipate potential offences[1].

Evidentiary proof is often the decisive bottleneck in this field. Digital evidence differs from traditional proof in ways that create both technical and legal strain: it may be modified, deleted, or replicated with relative ease; it can be manipulated without leaving immediately visible traces; and it typically requires specialized expertise to extract, preserve, analyze, and present before courts. Alongside these forensic constraints, legal issues remain central, particularly the lawfulness of acquisition and the probative value of electronic evidence. Admissibility standards and conditions of judicial reliance vary across jurisdictions. Contemporary legislation has therefore moved toward more explicit regulation of digital evidence, defining requirements for validity and evidentiary weight, while also introducing safeguards intended to protect individual rights against abusive or disproportionate electronic evidence-gathering[2].

The transboundary profile of AI-related offences makes international judicial cooperation a practical precondition of effective enforcement. A perpetrator may act from one state, target victims in a second, and rely on servers located in a third. This configuration complicates jurisdictional allocation and forces coordination among criminal justice authorities. States have accordingly developed international and regional cooperation instruments in the cybercrime domain, most notably the Budapest Convention on Cybercrime (2001) and the 2024 United Nations Convention on Cybercrime. In parallel, INTERPOL performs an operational coordinating role through specialized platforms that facilitate information exchange and support cross-border enforcement operations against cyber-enabled crime[3].

Part Two: Preventive and Institutional Mechanisms to Limit Misuse

[1] Al-Madini, Mouhammad ben Khalifa. “The Role of Artificial Intelligence in Proving Crimes and Preventing Them: A Jurisprudential Study.” *Journal of the Islamic University for Sharia and Legal Studies*, vol. 32, no. 1, 2024, pp. 180–215.

[2] Abd al-Nour, and Omar Hamas. “Artificial Intelligence as a Mechanism for Criminal Proof.” *Academic Journal of Legal Research*, vol. 16, no. 1, 2025, pp. 55–78.

[3] “International Cooperation to Combat Cybercrime: Effectiveness and Challenges.” *Journal of Legal and Political Studies*, vol. 10, no. 2, 2024, pp. 210–235.

Regulatory oversight of AI development and deployment remains a central preventive strategy for limiting diversion toward criminal ends. In practice, this oversight typically imposes binding obligations on developers and manufacturers to implement safety and security standards at the design stage, to conduct risk assessments prior to market deployment, and to ensure a degree of algorithmic transparency that permits explanation, review, and audit. It also reaches the governance of high-risk applications, including constraints on the use of facial recognition in public spaces without clear safeguards, and limits on AI systems making decisions with significant implications for individual rights in the absence of meaningful human oversight[1].

Institutional design matters to the same extent. At the domestic level, many states have established specialized bodies charged with supervising the AI sector and ensuring compliance with legal and ethical requirements. At the international level, organizations such as the United Nations, the European Union, and the Organisation for Economic Co-operation and Development have worked toward regulatory frameworks and guiding principles intended to promote responsible and secure AI use. INTERPOL also supports these efforts by enabling operational coordination among law enforcement agencies and providing platforms for exchanging information and expertise in cybercrime control[2].

Legal and ethical awareness functions as an additional preventive mechanism with tangible deterrent effect. When users understand the legal risks associated with abusive AI use, and when penalties for AI-enabled offences are communicated clearly, the likelihood of deviant conduct can be reduced before harm occurs. Complementing this, integrating ethics into the education and training of AI specialists supports the emergence of a professional culture grounded in responsibility and integrity. Effective awareness strategies require coordinated engagement by educational institutions, media organizations, civil society actors, and competent public authorities, so that messages about responsible and secure AI use remain clear, consistent, and practically actionable[3].

Conclusion

The misuse of artificial intelligence techniques constitutes one of the most pressing challenges confronting contemporary criminal law in an era of rapid

[1] French Ministry for Europe and Foreign Affairs. “France’s Activities in Combating Cybercrime.” Paris, 2024.
[2] INTERPOL. “Cooperation Services in Combating Cybercrime.” Lyon, 2024.
[3] Kacem, Mourad Mouhammad Ghalib. “The Role of Artificial Intelligence in Combating Cybercrime: A Comparative Study.” *Al-Quds Open University Journal*, 2024, pp. 145–170.

digital transformation. This study has sought to map this emerging phenomenon through a comprehensive analysis of its concept, causes, and principal manifestations, and then to examine the mechanisms made available within the criminal justice framework to address it through criminalization, sanctioning, and prevention.

The study yields several central findings, which may be summarized as follows:

First: The misuse of AI techniques is neither marginal nor a distant future concern. It is a lived and evolving reality in modern societies. Its particular gravity lies in the convergence of advanced technical capabilities with easy access to tools and knowledge, together with the cross-border reach of its effects, which significantly complicates effective control.

Second: Although traditional criminal law rules can accommodate certain forms of misuse through interpretive adaptation, they reveal a substantive deficit when confronted with the distinctive nature of AI-related offending. This deficit is reflected in the difficulty of absorbing new technical developments at adequate speed and in the challenges of applying conventional doctrines to offences in which AI constitutes an integrated component of the offence's material structure.

Third: Determining criminal liability in AI-related crimes remains among the most difficult issues facing the criminal justice system. The plurality of intervening actors (developer, manufacturer, operator, user) makes it necessary to revisit concepts of perpetration, participation, and causation, and to develop legal models that take account of fault and negligence within technically complex settings.

Fourth: Traditional procedural mechanisms (detection, investigation, and proof) require substantive development in order to meet the nature of digital and technically complex evidence. Establishing specialized units with high-level technical expertise, modernizing standards for digital evidence, and strengthening international cooperation are operational necessities rather than optional reforms.

Fifth: Prevention remains the most effective tool for confronting misuse of AI techniques. Early-stage oversight of the development and deployment of these technologies, the imposition of stringent security and transparency standards, and sustained awareness-building among specialists and users regarding legal and ethical responsibilities all contribute to limiting misuse before it occurs.

Sixth: Contemporary legislation has begun to move toward adopting specific provisions for AI-related crimes. These initiatives nevertheless require continuous updating to keep pace with rapid technological change, and deeper

international convergence to ensure effective prosecution and sanctioning given the transboundary character of these offences.

Recommendations

On the basis of the study's findings, the following recommendations are proposed:

1. Accelerate the adoption of comprehensive, specialized legislation addressing AI-related crimes in a systematic and balanced manner, reconciling the protection of innovation and technological development with the security of individuals and society. Such legislation should reflect leading comparative and international best practices.
2. Develop specialized human and technical capacity for detecting and investigating AI-related crimes through intensive training programs, the establishment of dedicated units, and the provision of advanced tools for digital analysis and computer forensics.
3. Integrate AI crime and its associated legal and ethical issues into university curricula in law and criminal sciences, as well as into training programs for AI specialists and engineers, with a view to strengthening legal awareness and ethical responsibility.
4. Adopt stringent safety, security, and transparency standards in the design and development of AI systems, conduct regular risk assessments, and promote ethical-by-design practices that take account of the social and legal consequences of AI products.
5. Strengthen international cooperation and coordination in combating AI-related crimes by developing harmonized international standards, reinforcing mutual legal assistance and cooperation agreements, and expanding structured information- and expertise-sharing among law enforcement authorities across jurisdictions.
6. Implement public awareness initiatives addressing the legal, security, and ethical risks of AI misuse, encouraging reporting of suspicious conduct, and promoting a culture of responsible, safe, and ethically grounded use of these technologies.

References

1. Ibrahim, Mouhammad. "Security and Societal Risks of Deepfakes and Response Mechanisms," *Journal of Law,* Alexandria University, 2025, pp. 45–78.
2. "Latest Cybercrime Statistics," Center for Artificial Intelligence and Cybersecurity Studies, 2025, pp. 34–56.

3. "Problematic Issues in the Use of Artificial Intelligence in Criminal Investigations," Master's Thesis, Ghardaïa University, 2023, pp. 102–118.
4. INTERPOL. "Cooperation Services in Combating Cybercrime," Lyon, 2024.
5. Al-Boudairi, Mouhammad. "Risks Associated with the Use of Deepfakes by Terrorist Organizations," *International Journal of Security Studies*, United Arab Emirates University, 2024, pp. 88–125.
6. Ben Aouda, Haskar. "The Problem of Applying Rules of Criminal Liability to AI Crimes," *Journal of Legal and Political Research*, Saïda University, 2022, pp. 115–130.
7. Bouznoun. "AI Entities in Criminal Law Thought," *Journal of Legal Studies*, University of Algiers, 2024, p. 45.
8. "International Cooperation to Combat Information Crime: Effectiveness and Challenges," *Journal of Legal and Political Studies*, Vol. 10, No. 2, 2024, pp. 210–235.
9. Jassas, Loubna, and Shehmat, Mourad. "Artificial Intelligence and Crime: Between Enablement and Prevention," *Algerian Journal of Humanities and Social Sciences*, Vol. 8, No. 2, 2024, pp. 63–76.
10. Dahshan, Yasser Ibrahim. "Criminal Liability for Artificial Intelligence Crimes," *Journal of Sharia and Law*, College of Law, United Arab Emirates University, 2020, pp. 215–280.
11. "Artificial Intelligence and Serious Cybercrimes," European Applied Research Laboratory for Artificial Intelligence and Security, 2024.
12. Zawi, Manal. "Criminal Liability for the Use of Artificial Intelligence," Master's Dissertation, Skikda University, 2024, pp. 45–60.
13. Al-Sharkawi, Oussama. "Deepfakes in Phishing Attacks," Cerebra Cybersecurity Center, 2025.
14. Saleh, Ramadan. "The Criminal Law Response to Cyber Extortion and Violations of Private Life," *Journal of Law*, 2024, pp. 210–245.
15. Abd al-Aziz. "Criminal Liability for Artificial Intelligence Crimes," Master's Thesis, Batna University, 2024, pp. 3–5.
16. Abd al-Nour, and Omar Hamas. "Artificial Intelligence as a Mechanism of Criminal Proof," *Academic Journal of Legal Research*, Vol. 16, No. 1, 2025, pp. 55–78.
17. Kacem, Murad Muhammad Ghalib. "The Role of Artificial Intelligence in Combating Cybercrime: A Comparative Study," *Al-Quds Open University Journal*, 2024, pp. 145–170.
18. Mouhammad Ali Moustafa. "The Legal Nature of Online Defamation via Artificial Intelligence Tools," *Journal of Legal Studies*, Zagazig University, 2024, pp. 156–189.
19. Mahmoud Baha al-Din. "Preventing Fraudulent Content: A Deepfake Detection Program," ComplyCube, 2025.
20. Mahmoud Abdelaziz Mahmoud. "Impacts of Cybercrime from the Victims' Perspective in Saudi Society," *Journal of Social Sciences Studies*, King Saud University, 2023, pp. 120–145.
21. Al-Madfaa, Halima. "The Personal Scope of Criminal Liability for Artificial Intelligence Errors," *The Legal Journal*, Cairo University, 2024, pp. 89–120.

22. Al-Madini, Mouhammad ben Khalifa. “The Role of Artificial Intelligence in Proving Crimes and Preventing Them: A Juristic Study,” *Journal of the Islamic University for Sharia and Legal Studies,* Vol. 32, No. 1, 2024, pp. 180–215.
23. United Nations Office on Drugs and Crime. “United Nations Convention on Cybercrime,” Hanoi, October 2024.
24. Moussa, Mouhammad Abd al-Rahman. “Artificial Intelligence and Legal Liability for Acts Resulting Therefrom,” Modern Legal Consultations Office, 2025.
25. Al-Miri, Abdelrazzak Ahmad Mouhammad. “Criminal Liability for Artificial Intelligence Crimes,” Arab Democratic Center, Berlin, 2024, pp. 12–18.
26. Al-Hayti, Raslan Ahmad. “Artificial Intelligence and Serious Cybercrimes: A Study of Emerging Threats,” *Journal of Security Studies*, 2024, pp. 78–102.
27. French Ministry of Foreign Affairs. “France’s Activities in Combating Cybercrime,” Paris, 2024.