



Qualis A3 ISSN: 2178-2008

ARTIGO

Listas de conteúdos disponíveis em [DOAJ](#)

Revista Processus de Estudos de Gestão, Jurídicos e Financeiros



Cybercrimes Committed Using Artificial Intelligence in Algerian Legislation: A Critical Analytical Study of Substantive and Procedural Challenges and Prospects for Legislative Reform

Benabbas Nora¹

<https://orcid.org/0009-0002-4492-3299>

University of Algiers 1 Ben Youssef Ben Kheda, Algiers, Algeria.

Email: norajuriste@hotmail.fr

Publication Information

ISSN: 2178-2008

Recebido em: 20-07-2026

Aceito em: 18-08-2026

Publicado em: 28-09-2026

Keywords:

Cybercrime,
Criminal Liability,
Deepfakes,
Digital Evidence,
Principle of Legality.

Abstract

This study addresses a delicate legal problematic emerging from the accelerated evolution of artificial intelligence (AI) technologies: the capacity of the Algerian legislative framework to accommodate cybercrimes committed through autonomous, self-learning systems. The convergence of deep learning algorithms with cyberspace has generated a novel criminal typology characterized by functional autonomy, high velocity, and transnational reach. These features collide with the classical structure of criminal theory, grounded in the duality of *actus reus* and *mens rea*, as well as the principle of legality of offenses and penalties. Employing a critical-analytical methodology applied to Algerian legislative texts—notably the Penal Code, Law No. 09-04 on the prevention and combating of ICT-related crimes, and Law No. 18-07 on personal data protection—supplemented by comparative references to the European framework (particularly the 2024 EU Artificial Intelligence Act) and French legislation, the study concludes that the current Algerian regime suffers from a dual conceptual and procedural deficit. The substantive deficit is linked to the rigidity of legislative terminology in the face of synthetic generation phenomena (e.g., deepfakes), while the procedural deficit is connected to the inability of digital evidence mechanisms to address the algorithmic "black box" problem. The study proposes structural legislative reforms, including the introduction of a specific aggravating circumstance linked to AI use and the expansion of indirect criminal liability in accordance with the "Safety-by-Design" principle.

¹ Doctoral student in Saeed Hamdeen Faculty of Law. University of Algiers 1 Ben Youssef Ben Kheda, Algiers, Algeria (2016); a Master's degree from Faculty of Law, Ben Aknoun, University of Algiers 1 Ben Youssef Ben Kheda, Algiers, Algeria (2013).

1. INTRODUCTION

Throughout its modern history, the phenomenon of crime has arguably never witnessed a structural transformation parallel to that brought about by the Fourth Industrial Revolution, particularly regarding generative artificial intelligence (AI) and machine learning technologies. Criminal acts have migrated from a tangible physical space governed by traditional coordinates of time and space to a complex virtual realm where the roles of human and machine intersect. In this domain, it has become difficult—and sometimes impossible—to determine the true source of criminal behavior. The computer is no longer a mere passive tool in the hands of the perpetrator; in many contemporary applications, it functions as a semi-autonomous entity capable of making decisions, learning from its environment, and modifying its behavior independent of direct human will (Chesterman, 2021).

What exacerbates this issue is that national criminal legislations—including that of Algeria—were originally drafted to combat criminal typologies predicated on a clear causal link between a human actor and a harmful outcome. However, advanced AI systems based on deep neural networks produce decisions that even their original developers cannot interpret with certainty, a phenomenon known as the "Black Box" problem (Boullain, 2021). This phenomenon alone is sufficient to destabilize the epistemological foundations upon which general criminal theory is built, particularly concerning the mental element (*mens rea*) and rules of criminal attribution.

The Algerian legislator recognized relatively early the need to update its legal arsenal to combat cybercrime. The Penal Code was amended by Law No. 04-15 of 2004, which added Section 7 bis concerning "Offenses against Automated Data Processing Systems". This was followed by Law No. 09-04 of 2009 on preventing and combating ICT-related crimes, and Law No. 18-07 of 2018 on the protection of individuals regarding the processing of personal data. Nevertheless, despite their relative progressiveness, these frameworks were drafted when AI applications were still in their infancy. Phenomena such as deepfakes and automated cyberattacks had not yet reached their current level of maturity.

Core Problematic: This study proceeds from the following fundamental question: *To what extent can the current Algerian legislative and procedural framework accommodate cybercrimes committed via AI systems? Are traditional rules of criminalization and criminal attribution sufficient to address the autonomous criminal behavior of algorithms, or does the situation necessitate a radical reformulation of national criminal policy in this domain?*

Research Hypotheses: This research is founded on three integrated hypotheses:

1. The principle of legality in criminal law, with its inherent strictness regarding the narrow interpretation of penal provisions, acts as a substantive barrier to the legal characterization of acts committed by generative AI, particularly fully synthetic image and audio generation.
2. Classical rules of criminal attribution, built upon the duality of human knowledge and will, fail to accommodate the autonomous behaviors of deep learning algorithms, leading to a "Responsibility Gap".
3. The nature of AI-generated digital evidence necessitates a radical review of the procedural framework for criminal investigation and evidence gathering in

Algerian legislation, ensuring a balance between the efficacy of prosecution and the rights of the defense.

Methodology: This study primarily relies on a critical-analytical methodology applied to relevant Algerian legislative texts. A comparative methodology is utilized for supplementary insight, referencing European and French experiences, notably the EU Artificial Intelligence Act (EU AI Act) issued in June 2024, which represents the first comprehensive legislative framework regulating AI uses at an international level.

2. CONCEPTUAL FRAMEWORK AND TYPOLOGIES OF AI-DRIVEN CYBERCRIMES

Serious inquiry into any emerging legal issue requires precise conceptual framing that distinguishes between closely related terms and clearly delineates their legal boundaries. Conflating "traditional cybercrime" with "AI-enhanced cybercrime" leads to confusion in legal characterization and, consequently, to deficiencies in criminal policy.

2.1 Essential Characteristics of AI-Enhanced Cybercrimes

Cybercrimes committed via AI possess characteristics that distinguish them from traditional cybercrimes, casting shadows over the rules of criminalization and attribution. These characteristics can be summarized in three central traits:

First - Decisional Autonomy: Modern AI systems, particularly those based on Deep Neural Networks (DNNs), possess the ability to make decisions based on self-analysis of data without the need for real-time human direction (Chesterman, 2021, pp. 45-52). Boullain (2021) notes that this autonomy produces what he terms "Agency without Intent," where a criminal result is achieved without direct criminal intent (*mens rea*) from any human actor (pp. 78-84). This constitutes the first epistemological crisis for contemporary penology (Tahri, 2020).

Second - Interpretive Opacity (The Black Box Problem): Deep learning algorithms produce decisions that cannot be interpreted with certainty even by their original developers (High-Level Expert Group on Artificial Intelligence [HLEG], 2019). This phenomenon has spawned an independent cognitive field known as Explainable AI (XAI), which seeks to develop mechanisms allowing algorithmic decisions to be understood and tracked. Legally, this opacity leads to a fundamental problem concerning the proof of *mens rea* and the determination of liability.

Third - Transnational and Fluid Nature: AI applications predominantly operate via distributed cloud infrastructure that may span multiple jurisdictions simultaneously. Balkin (2017) suggests that this reality imposes an "Algorithmic Society Law" that necessitates a radical rethinking of the concepts of legal sovereignty and jurisdiction (p. 1228).

2.2 Legal Classification of AI-Enhanced Cybercrimes

The practical applications of AI in criminal behavior are diverse. From a criminological perspective, they can be classified into three major categories, analyzed here in relation to the Algerian legislature's stance:

Category One - Crimes Against Persons via Synthetic Generation: Deepfakes, driven by Generative Adversarial Networks (GANs), constitute the most prominent threat

in this category. These technologies allow for the production of forged videos or audio recordings with an accuracy that is nearly impossible to detect via standard human perception (Citron & Chesney, 2019). They are utilized in various criminal forms, notably sexual extortion, political forgery, voice phishing (Vishing), and defamation.

Referring to the Algerian Penal Code, the legislator criminalized the violation of privacy in Article 303 *bis*, punishing anyone who intentionally captures, transmits, or records private or confidential speech or the image of a person in a private place without their consent. However, the fundamental question arises: Can the complete synthetic generation of a person's image that was never actually "captured"—but rather algorithmically produced—be characterized under the concepts of "capturing" or "recording" mentioned in the text? (Ayache, 2023).

The criminal judge's adherence to the principle of strict interpretation of penal texts—a well-established principle in Algerian criminal jurisprudence (Bousquiea, 2023, pp. 78-82)—renders them unable to expand the concept of "capturing" to include "synthetic generation." Synthesis negates the existence of an original capture; it creates a new image *ex nihilo*. This creates a genuine legislative vacuum that cannot be filled by analogy, as analogy is unanimously prohibited in criminal law by jurisprudence (Bousquiea, 2023).

Category Two - Crimes Against Property via Algorithmic Fraud: AI algorithms are employed to execute highly complex fraud operations utilizing Natural Language Processing (NLP) and voice cloning technologies. Notable applications include automated spear-phishing attacks, which rely on analyzing a victim's social media accounts to craft customized messages that accurately mimic the writing style of their acquaintances (Chesterman, 2021).

The Algerian Penal Code regulates the crime of fraud in Article 372, which requires the use of "fraudulent methods," an "assumed name," or a "false quality" to deceive the victim. While some algorithmic fraud applications could fall under this provision, two fundamental issues emerge: First, the extent to which "fraudulent methods" can be attributed to an AI system operating with relative autonomy; second, proving the criminal intent of the ultimate beneficiary when the algorithmic tool has exceeded its programmed scope.

Category Three - Crimes Against Automated Data Processing Systems: The Algerian legislator regulates this category in Section 7 *bis* of the Penal Code (Articles 394 *bis* to 394 *bis* 7). These articles cover various acts, including unauthorized access or remaining in a system, data modification or deletion, fraudulent data input, and unlawful interception of communications (Khedri, 2021).

Adversarial AI is employed in this category to develop malware capable of self-adapting to and bypassing security systems, known as "Self-Learning Malware" (Boullain, 2021, pp. 156-160). This raises a core issue of attribution: If self-evolving malware breaches a sensitive system based on its own self-analysis, without the developer having included this specific behavior in the original design, can the crime be attributed to the developer?

3. THE ADEQUACY OF ALGERIAN CRIMINAL PROVISIONS IN COMBATING AI CRIME

A serious analysis of the adequacy of Algerian legislative texts requires subjecting them to a dual test: an objective (substantive) test regarding the ability of criminal definitions to accommodate emerging behaviors, and a procedural test regarding the efficacy of investigation and prosecution mechanisms.

3.1 Evaluating the Substantive Legal Arsenal

The Algerian criminal structure is founded on the principle of legality in criminal law (*Nullum crimen, nulla poena sine lege*), constitutionally enshrined in Article 34 of the 2020 Constitutional Amendment and stipulated in Article 1 of the Penal Code. This principle constitutes the greatest barrier to any attempt to expansively interpret penal texts to address emerging behaviors (Bousquiea, 2023, p. 210).

A Critical Reading of Section 7 bis of the Penal Code: Article 394 *bis* punishes anyone who fraudulently accesses or remains in all or part of an automated data processing system. Applying this text to AI actions raises two integrated issues:

- **The Problem of "Fraud" (Fraude):** The text requires the element of "fraud," which presumes human deceit grounded in consciousness and will (Zouaoui, 2020, pp. 122-128). If an AI algorithm breaches an information system based on a self-guided analysis of security vulnerabilities, does the element of "fraud" exist in its classical sense? According to traditional criminal jurisprudence, the answer is negative, as fraud necessitates directed human will.
- **The Problem of Behavioral Attribution:** Even if we concede the possibility of fraud existing within the user or developer, proving this element remains problematic. The generative and learning nature of the algorithm makes it exceedingly difficult to prove that the specific behavior was originally intended by the human actor (Saadaoui, 2021, p. 227).

Evaluating Law No. 09-04 on ICT-Related Crimes: This law established a specialized institutional and procedural framework for combating cybercrime. However, a critical reading reveals several shortcomings:

- **Terminology:** The law relies on terms such as "surveillance", "interception", and "digital search"—terms crafted for human-originated criminal behaviors that fail to capture the nature of autonomous algorithmic behavior.
- **Actors:** The law focuses on "Internet Service Providers" (Articles 10 and 11) as pivotal actors. However, a significant portion of AI applications operates outside this scope, utilizing open-source platforms or peer-to-peer decentralized networks, creating a genuine regulatory vacuum (Ben Ahmed, 2022).
- **Proactive Dimension:** The law lacks any regulatory framework for the proactive security use of AI technologies, such as Predictive Policing systems, which are currently regulated in several European countries (Council of Europe, 2018).

3.2 Protecting Personal Data vs. Algorithmic Data Mining

AI systems rely on processing massive amounts of data (Big Data) to train their models, raising fundamental issues concerning the right to privacy. The Algerian legislator enacted Law No. 18-07 on the protection of individuals regarding the processing of personal data, establishing the National Authority for the Protection of Personal Data (ANPDP) (Bouchenak, 2022).

The Problem of Explicit Consent vs. Algorithmic Feeding: Article 7 of Law 18-07 requires the explicit consent of the data subject prior to processing, under penalty of criminal sanctions. Applying this condition to AI systems encounters an insurmountable technical reality: deep learning models are trained on billions of data points automatically extracted from the internet (web scraping), making it practically impossible to obtain explicit consent from every data subject (Chesterman, 2021). Comparative legal scholars, notably Danielle Citron, argue that the traditional concept of consent has lost its efficacy in the face of "Surveillance Capitalism" imposed by major AI corporations (Citron & Chesney, 2019).

The Impossibility of the "Right to be Forgotten" in Neural Networks: Article 39 of Law 18-07 grants data subjects the right to request the correction or erasure of their personal data. However, this right faces a core technical challenge in the context of AI. When a neural network is trained on specific data, it does not store this data in its original form; rather, it integrates the data into its neural weights in a manner that makes selective separation or retrieval impossible (Pagallo, 2013). This creates a fundamental gap between the legal text and its practical applicability.

The Challenge of Algorithmic Bias: AI systems raise an additional issue not explicitly addressed by the Algerian legislator: algorithmic bias. Studies have proven that facial recognition algorithms, for instance, produce disproportionately high error rates when applied to specific racial or gender groups (Solaiman, 2017). Using these algorithms in criminal contexts (e.g., identifying suspects via CCTV) could lead to wrongful convictions, yet Algerian legislation lacks any framework regulating liability for utilizing these technologies in criminal investigations.

4. THE CRISIS OF CRIMINAL ATTRIBUTION AND PROCEDURAL CHALLENGES

Two fundamental issues form the core of the legal challenges in confronting AI-enhanced cybercrimes: determining the actor deserving punishment (the problem of criminal attribution), and proving the crime (the problem of digital evidence).

4.1 The Crisis of Attribution and Criminal Liability

Criminal liability in Algerian legislation is based on the duality of material attribution (*actus reus*) and mental attribution (*mens rea*), presupposing criminal capacity based on sanity, discernment, and will. The scope of the criminal actor is restricted to natural persons and legal entities (Article 51 *bis*, Penal Code).

The Theory of Electronic Personhood and its Limits in Algeria: Some Western literature—notably the European Parliament Resolution of February 2017 on Civil Law Rules on Robotics—proposed granting advanced AI systems an "Electronic Personhood", allowing for independent civil and criminal liability (European Parliament, 2017). While scholars like Ugo Pagallo (2013) viewed this as an opportunity to build a suitable legal

framework, the European Commission's High-Level Expert Group rejected it in 2019, arguing it empties criminal liability of its philosophical content (HLEG, 2019).

In the Algerian context, this theory faces fundamental obstacles:

- **Philosophically**, the general theory of crime is based on moral responsibility grounded in freedom and will—concepts lacking in smart systems (Bousquiea, 2023, pp. 220-225).
- **Practically**, it is impossible to apply traditional criminal penalties (like imprisonment) to an algorithmic entity.
- **Constitutionally**, recognizing the criminal liability of smart systems conflicts with the principle of personal penalty enshrined in Article 46 of the 2020 Constitution.

Attributing Liability to Human Actors: A Gradual Approach: Ruling out direct liability for the machine necessitates searching for the human actor behind it. Contemporary criminal jurisprudence distinguishes between four types of liability (Garland, 2021):

- **End-User Liability:** Triggered when an individual consciously uses an AI system to execute a criminal act (e.g., creating extortive deepfakes). This falls under principal perpetration in Article 41 of the Algerian Penal Code.
- **Developer Liability:** Triggered when a developer designs an algorithm to commit crimes, or intentionally omits necessary safety mechanisms. The issue arises when a developer acts in good faith, but the algorithm self-evolves to commit unplanned acts.
- **Operator/Deployer Liability:** The liability of the entity operating the AI system professionally. The EU AI Act explicitly adopted this distinction in Article 3 (Regulation (EU) 2024/1689).
- **Data Provider Liability:** An emerging liability when harm results from the quality of training data rather than the algorithm itself.

The "Responsibility Gap" and Proposed Solutions: German philosopher Andreas Matthias (2004) coined the "Responsibility Gap" to denote situations where it is impossible to attribute criminal liability to any human actor despite harm occurring. Contemporary jurisprudence proposes several approaches to bridge this gap:

- **Strict Liability:** Holding the developer/operator liable upon the occurrence of harm without proving fault. While adopted in civil liability, its application in criminal law faces strong resistance as it breaches the principle of legality (Boullain, 2021).
- **Design-Based Liability:** Holding the developer liable for failing to incorporate "Safety-by-Design" mechanisms, aligning with the philosophy of the EU AI Act.
- **Distributed Liability:** Distributing liability across various actors in the algorithmic chain based on their contribution to the harm (Chesterman, 2021).

4.2 Procedural Challenges in Proving AI Cybercrimes

Procedural challenges are equally, if not more, impactful than substantive challenges, as they dictate the efficacy of applying criminal texts.

The "Black Box" Problem and Criminal Evidence: The aforementioned Black Box phenomenon constitutes the greatest challenge for the criminal judge and forensic expert. When it is impossible to explain how an algorithm reached a specific decision, proving the causal link between human fault and the criminal outcome becomes virtually impossible (Le Guyader, 2022). In Algerian courts, judges rely on forensic reports from the Central Service for Combating ICT Crimes. If experts cannot provide a definitive scientific explanation for the algorithmic behavior, the principle of *In dubio pro reo* (doubt benefits the accused, Article 3, Code of Criminal Procedure) must apply, leading to impunity.

Search and Seizure of Cloud Data: The Algerian legislator regulated electronic search and seizure in Law No. 09-04 and the amended Code of Criminal Procedure. However, these procedures were largely designed for "static data" stored on specific media under national jurisdiction. In the context of AI, data is often "fluid" and distributed instantaneously across multiple cloud servers outside the national territory (Zouda, 2021). This raises two issues:

- **Territorial Jurisdiction:** The Penal Code relies on the principle of territoriality, assuming the crime scene can be precisely located. Algorithmic crimes may occur simultaneously on servers in different countries.
- **International Judicial Cooperation:** Investigating cloud data requires international cooperation, which, despite the 2001 Budapest Convention, remains slow and complex. (Algeria is not a party to the Budapest Convention, though it has joined the 2010 Arab Convention on Combating Information Technology Offences).

Admissibility of AI-Extracted Evidence: Digital evidence extracted via AI (e.g., facial recognition, predictive analysis) raises issues regarding admissibility:

- **Scientific Reliability:** Criminal evidence must rely on verifiable scientific methodology. The U.S. Supreme Court's *Daubert* standard (1993) requires testability, known error rates, and general scientific acceptance (Le Guyader, 2022).
- **Rights of the Defense:** The right to a fair trial requires the accused to be able to challenge evidence. The Black Box phenomenon makes challenging algorithmic evidence nearly impossible, violating the core of defense rights (Chesterman, 2021).

5. TOWARD A COMPREHENSIVE ALGERIAN LEGISLATIVE STRATEGY

The multiple challenges revealed by this analysis demonstrate that the Algerian legislative response requires structural development, not merely piecemeal patching of existing texts.

5.1 Substantive Amendments to Criminal Law

Contemporary criminal policy requires a comprehensive review of substantive texts, maintaining a delicate balance between effective deterrence and the guarantee of rights and freedoms:

First - Expanding Criminalization to Accommodate Synthetic Generation: It is proposed to amend Article 303 *bis* of the Penal Code to explicitly include acts of "synthetic generation," "algorithmic generation", and "digital blending" alongside "capturing" and "recording". This ensures the complete criminalization of deepfakes without resorting to expansive interpretations that clash with the principle of legality. The French approach in the SREN Law of 2024, which explicitly criminalized the unconsented publication of artificially generated visual or audio content, serves as a valuable model.

Second - Introducing AI Use as a Specific Aggravating Circumstance: A general aggravating circumstance should be introduced in the Penal Code for all crimes—not just cybercrimes—committed using AI systems. This is justified by the exceptional danger, rapid dissemination, and difficulty of detection associated with these systems. The French legislature adopted a similar approach in the 2023 Justice Law (Garland, 2021).

Third - Establishing Criminal Liability for Design Flaws: A specific provision should be introduced to establish the criminal liability of developers for damages resulting from their failure to include basic "Safety-by-Design" mechanisms. This would mirror the crime of failing to take necessary precautions (Article 288, Penal Code), but tailored to the technical specificity of smart systems.

Fourth - Drafting a Specific Provision for Criminal Use of Biometric Systems: Given the risks facial and voice recognition systems pose to privacy, a specific penal provision should criminalize their unauthorized use, akin to Article 5 of the EU AI Act, which bans biometric recognition in public spaces save for strictly defined exceptions.

5.2 Procedural and Institutional Development

The deterrent framework is incomplete without advanced procedural tools and technologically qualified institutions:

First - Updating the Code of Criminal Procedure for Cloud Data: Amendments to the Code should include:

- Introducing "Expedited Data Preservation", allowing judicial authorities to order cloud providers to retain data for a specified period (as per Article 16 of the Budapest Convention).
- Regulating "Transborder Access" to cloud data stored abroad under parameters respecting judicial sovereignty.
- Establishing a system akin to the "European Production Order" adapted to the Algerian context to accelerate cross-border digital evidence acquisition.

Second - Establishing a Legal Framework for Algorithmic Reverse Engineering: A specific legal framework for "Algorithmic Reverse Engineering" should be created, defining the conditions of its practice, methodology, and evidentiary value. This includes forming a core of forensic experts specialized in reverse engineering within the Central Service for Combating ICT Crimes, and compelling developers of high-risk AI to provide "Explainability Data."

Third - Enhancing the Regulatory Role of the ANPDP: The powers of the National Authority for the Protection of Personal Data should be expanded to include proactive oversight of AI systems processing personal data, mandating "Data Protection Impact Assessments" prior to deployment, and establishing an "Ethical Certification" mechanism for sensitive sectors.

Fourth - Qualifying Judicial and Security Personnel: Specialized training in digital law and AI should be integrated into the Higher School of Magistracy and the National Institute of Criminalistics.

6. CONCLUSION

This study reveals that the accelerated evolution of AI technologies has produced a novel criminal typology that challenges the philosophical and legal foundations of traditional criminal policy. AI-enhanced cybercrimes are not merely a quantitative extension of classical cybercrimes; they represent a qualitative leap requiring a radical rethinking of the concepts of the criminal actor, *mens rea*, and rules of attribution.

Meticulous analysis of the Algerian legislative framework proves it suffers from a dual deficit: a substantive deficit manifested in the rigidity of legislative terminology regarding synthetic generation, and a procedural deficit linked to the inability of investigative mechanisms to address the complexities of algorithmic evidence. This gap cannot be filled merely by expansive interpretation of existing texts—which would violate the principle of legality—but requires decisive legislative intervention to rewrite the system in light of technological advancements.

Key Findings:

1. **Deficiency in Criminal Definitions:** The terminology in the Penal Code and Law 09-04 suffers from conceptual rigidity, unable to accommodate AI-enhanced behaviors, particularly full synthetic generation (deepfakes).
2. **A Vacuum in Criminal Liability:** The decisional autonomy of smart systems produces a "Responsibility Gap" that traditional criminal jurisprudence cannot address, necessitating a new theory of liability based on "Design-Based Liability."
3. **The Crisis of Criminal Evidence:** The "Black Box" phenomenon is the greatest challenge to criminal evidence rules, rendering the establishment of a causal link nearly impossible and threatening the principle of *In dubio pro reo*.
4. **Inadequacy of Data Protection Mechanisms:** Law 18-07 lacks the legal tools to confront algorithmic Big Data mining, particularly regarding explicit consent and the right to be forgotten.

Recommendations:

- **Substantive Level:** Rewrite Section 7 *bis* of the Penal Code and update Law 09-04 to explicitly address AI. Introduce an aggravating circumstance for AI use and establish developer liability for design flaws.
- **Procedural Level:** Amend the Code of Criminal Procedure to accommodate transborder cloud data challenges and establish a legal framework for algorithmic reverse engineering.
- **Institutional Level:** Enhance the regulatory role of the ANPDP and qualify judicial/security personnel through specialized training.
- **International Level:** Actively accede to international conventions related to combating cybercrime and participate in ongoing UN negotiations regulating AI uses.

Ultimately, national criminal policy must transition from a reactive approach to a proactive one that anticipates technological developments before they materialize into

actual threats. Balancing the imperatives of digital security with the protection of fundamental rights and freedoms will remain the greatest challenge for the Algerian legislator and criminal judge in the coming decades—a challenge that can only be successfully met through a multidisciplinary approach combining legal expertise, technical acumen, and ethical awareness.

REFERENCES

- Ayache, S. (2023). The legal characterization of crimes committed via deepfake technology in Algerian legislation [In Arabic]. *Journal of Judicial Jurisprudence*, 15(1), 45-63.
- Balkin, J. M. (2017). The three laws of robotics in the age of big data. *Ohio State Law Journal*, 78(5), 1217-1241.
- Belaïd, B. (2020). *Cybercrime in Algerian legislation* [In Arabic]. Dar Wael for Publishing and Distribution.
- Ben Ahmed, A. (2022). The problem of electronic search in cybercrimes across the cloud environment [In Arabic]. *Journal of Legal and Economic Thought*, 5(2), 177-195.
- Bouchenak, F. (2022). Criminal protection of personal data in light of artificial intelligence technologies: A reading of Law No. 18-07 [In Arabic]. *Journal of the Researcher for Academic Studies*, 9(1), 310-328.
- Boullain, P.-J. (2021). *L'Intelligence artificielle et le droit pénal: Vers une nouvelle théorie de l'imputation* [Artificial intelligence and criminal law: Towards a new theory of imputation]. Dalloz.
- Bousquiea, A. (2023). *Al-Wajeez in general criminal law* (20th ed.) [In Arabic]. Dar Houma for Printing, Publishing and Distribution.
- Chesterman, S. (2021). *We, the robots? Regulating artificial intelligence and the limits of the law*. Cambridge University Press.
- Citron, D. K., & Chesney, R. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(6), 1753-1820.
- Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)*. ETS No. 185.
- Council of Europe. (2018). *Study on the human rights dimensions of automated data processing techniques and possible regulatory implications*. Committee of Experts on Human Rights Dimensions of Automated Data Processing and Different Forms of Artificial Intelligence (MSI-AUT).
- European Parliament. (2017, February 16). *Resolution with recommendations to the Commission on Civil Law Rules on Robotics* (2015/2103(INL)). Official Journal of the European Union, C 252.
- Garland, R. (2021). L'imputation pénale à l'ère des systèmes autonomes [Criminal imputation in the era of autonomous systems]. *Revue Internationale de Droit Pénal*, 92(1), 89-115.
- High-Level Expert Group on Artificial Intelligence (HLEG). (2019). *Ethics guidelines for trustworthy AI*. European Commission.
- Khedri, H. (2021). *Criminal protection of information systems in Algerian legislation* [In Arabic]. Dar Belqis Publications.
- League of Arab States. (2010). *Arab convention on combating information technology offences*. Cairo.
- Le Guyader, D. (2022). Le juge pénal face à l'intelligence artificielle : entre certitude scientifique et doute raisonnable [The criminal judge facing artificial intelligence:

- Between scientific certainty and reasonable doubt]. *Revue de Science Criminelle et de Droit Pénal Comparé*, 3, 567-589.
- Matthias, A. (2004). The responsibility gap: Ascribing responsibility for the actions of learning automata. *Ethics and Information Technology*, 6(3), 175-183.
- Merrouk, N. E. (2019). *Lectures on criminal evidence* [In Arabic]. Dar Houma for Printing, Publishing and Distribution.
- Pagallo, U. (2013). *The laws of robots: Crimes, contracts, and torts of artificial intelligence agents*. Springer.
- Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings. (2023). *Official Journal of the European Union*, L 191.
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). (2024). *Official Journal of the European Union*, L 1689.
- Saadaoui, M. L. (2021). Criminal liability for crimes committed via artificial intelligence in Algerian legislation [In Arabic]. *Journal of Comparative Legal Studies*, 7(1), 220-245.
- Solaiman, S. M. (2017). Legal personality of robots, corporations, idols and chimpanzees: A quest for legitimacy. *Artificial Intelligence and Law*, 25(2), 155-179.
- Tahri, H. (2020). Criminal liability for acts of artificial intelligence: An analytical reading of the concepts of criminal attribution [In Arabic]. *Journal of Rights and Freedoms*, 8(2), 142-161.
- Youssef, M. (2022). Artificial intelligence and cybercrime challenges in North African legal systems. *Journal of Cyber Policy and Law*, 11(2), 54-71.
- Zouaoui, A. (2020). *Cybercrimes in Algerian legislation and comparative law* (2nd ed.) [In Arabic]. Dar Houma for Printing, Publishing and Distribution.
- Zouda, O. (2021). Digital criminal evidence and the challenges of artificial intelligence before the criminal judge [In Arabic]. *Journal of Legal and Political Sciences*, 12(3), 88-107.