

Uses of Artificial Intelligence in Criminal Investigation: An Analytical Study Between Criminal Sophistication and Naivety of Execution

Mebarkia takki^{1,*}, Mebarkia souad²

¹ Echahid Cheikh Larbi Tebessi university Tebessa, (Algeria)

takki.mebarkia@univ-tebessa.dz

² Larbi Ben M'hidi university, Oum El-Bouaghi, Algeria (Algeria)

Laboratory of Legal and Political Studies

mebarkia.souad@univ-oeb.dz

Received: 18 / 10 / 2025

Accepted: 21 / 05 / 2026

Published: 11 / 06 / 2026

Abstract:

Artificial intelligence is reshaping criminal justice, affecting both how crimes are committed and how they are investigated. This paper explores the dual role of AI from two interconnected perspectives. On one side, offenders exploit technologies such as deepfakes, algorithmic fraud, and chatbots to carry out crimes with growing sophistication. On the other, investigators employ the same tools—big data analytics, facial recognition, and voice identification—to enhance detection and expose offenders.

Findings reveal a widening gap: criminals increasingly use advanced systems that outpace traditional investigative methods, leaving justice mechanisms struggling to adapt. This imbalance highlights the urgent need for legislative updates, both to criminalize AI-driven offenses and to regulate the evidentiary value of AI-generated materials, while safeguarding defense rights and the principles of a fair trial.

Keywords: *Artificial Intelligence; Comparative Legislation; Criminal Investigation; Deepfake; Digital Evidence.*

المخلص:

يحدث الذكاء الاصطناعي تحولاً في منظومة العدالة الجنائية، بما يؤثر على كيفية ارتكاب الجرائم وأساليب التحقيق فيها. ويستعرض هذا البحث الدور المزدوج للذكاء الاصطناعي من منظورين مترابطين؛ فمن جهة، يستغل الجناة تقنيات مثل التزييف العميق، والاحتياال الخوارزمي، وروبوتات المحادثة لتنفيذ جرائم متزايدة التعقيد. ومن جهة أخرى، توظف جهات التحقيق الأدوات ذاتها — كتحليلات البيانات الضخمة، وتقنيات التعرف على الوجه، وتحديد هوية الصوت — لتعزيز قدرات الكشف عن الجرائم وفصح مرتكبيها.

وتكشف النتائج عن وجود فجوة آخذة في الاتساع؛ حيث يستخدم المجرمون بشكل متزايد أنظمة متقدمة تتفوق على أساليب التحقيق التقليدية، مما يجعل آليات العدالة تكافح من أجل التكيف. ويسلط هذا الاختلال الضوء على الحاجة الملحة لإجراء تحديثات تشريعية، سواء لتجريم الأفعال المعتمدة على الذكاء الاصطناعي، أو لتنظيم القيمة الإثباتية للمواد المستخرجة بواسطته، مع ضرورة حماية حقوق الدفاع ومبادئ المحاكمة العادلة. **الكلمات المفتاحية:** التحقيق الجنائي؛ التشريع المقارن؛ التزييف العميق؛ الدليل الرقمي؛ الذكاء الاصطناعي.

* Mebarkia takki

I. INTRODUCTION

Over the last two decades, artificial intelligence has evolved at an unprecedented pace, expanding across key sectors—including criminal justice. Investigative procedures have gradually moved away from traditional mechanisms and toward intelligent systems capable of automatic data processing, behavioral analysis, and predictive modeling of criminal behavior. This digital shift has not only enhanced law enforcement capabilities but has also been exploited by criminal actors to develop unconventional techniques that stretch the boundaries of what constitutes a crime, complicating both detection and response mechanisms (Casey, 2019, p. 45).

The significance of this topic lies in its exposure of one of the most pressing legal challenges of the modern era: the growing intersection between technological advancement and criminal practice on one hand, and the tension between modern investigative needs and traditional legal boundaries on the other. Analyzing the dual uses of artificial intelligence—by both offenders and investigators—helps reveal gaps and strengths in current legal frameworks (McGuire, 2020, p. 112).

This study aims to identify the most prominent AI-driven criminal behaviors and the technological means through which they are carried out, while also exploring the intelligent tools adopted by law enforcement agencies. It assesses the legal and operational effectiveness of these technologies, with special focus on the evidentiary and procedural issues they raise regarding criminal liability and basic rights (Wachter et al., 2017, p. 80).

The central question around which this paper revolves is:

To what extent can artificial intelligence tools enhance the process of criminal investigation without violating legal safeguards, particularly in light of the growing sophistication of AI-supported criminal conduct?

Sub-questions include:

- What are the primary forms of crime that exploit artificial intelligence?
- How are deepfake tools, voice manipulation, and chatbots used to commit offenses?
- What is the legal status of AI tools in criminal investigations?
- Are these tools compatible with procedural guarantees and the fundamental rights of the accused?
- Do existing legislative systems keep pace with these technological changes, or is urgent reform required to fill legal gaps?

This paper adopts a descriptive-analytical methodology. It describes the emerging criminal phenomena and analyzes them from a legal perspective, referencing comparative legislation, recent studies, and judicial precedents, with focused reference to the Algerian legal context where appropriate.

The article is structured into two main sections:

The first addresses criminal methods supported by artificial intelligence, including deepfake crimes, algorithmic fraud, and chatbot exploitation, with legal analysis of the issues raised by these methods.

The second explores AI-based investigative tools such as big data analytics, facial recognition, and behavioral analysis, and examines their legal validity and evidentiary strength.

1. Criminal Methods Supported by Artificial Intelligence

The emergence of artificial intelligence as a tool in criminal behavior has redefined the nature of crime itself. Today, offenses can be carried out using self-operating systems that do not require constant human interaction, making the perpetrator increasingly invisible. This shift has created what some scholars describe as a “post-human” criminal environment, where actions are automated, dynamic, and capable of evading traditional detection methods (McGuire, 2018, p.

103).

Unlike conventional crimes that rely on direct contact or physical presence, AI-driven crimes are executed through complex algorithms, neural networks, and generative models. These technologies allow offenders to commit fraud, manipulate identities, and breach secure systems in ways that are often difficult to trace or even define legally (Mittelstadt et al., 2016, p. 9). In many cases, the tools used for these crimes are the same ones developed to support security and efficiency—highlighting the dual-use nature of artificial intelligence.

This section will analyze the most critical manifestations of AI-supported criminality, focusing on methods that have already been observed in real-world legal contexts. Each type of offense will be discussed in terms of its technical mechanism, its legal classification (when available), and the challenges it poses for prosecutors and lawmakers alike (Floridi & Taddeo, 2014, p. 3).

1.1 The Use of Algorithms in Financial Fraud and System Intrusion

Algorithms—once perceived as neutral tools of automation—have increasingly become instruments of manipulation in the hands of criminal actors. Through machine learning and predictive models, offenders can now exploit digital infrastructures without ever setting foot inside a financial institution or protected system. The very architecture designed to optimize efficiency and security is being turned against itself, allowing for targeted attacks that are faster, more scalable, and harder to detect than traditional cybercrimes (Brennan-Marquez, 2018, p. 15).

This section will explore the use of algorithmic systems in facilitating financial fraud and unauthorized access to sensitive networks. These crimes are no longer speculative or emerging—they are now documented realities in jurisdictions around the world, prompting legal scholars and legislators to rethink how criminal liability and digital evidence are conceptualized in an age of autonomous decision-making (Wall, 2017, p. 880).

1.1.1 AI-Driven Financial Crimes

The rise of artificial intelligence in financial environments has significantly reshaped how crimes are committed, detected, and prosecuted. Criminal actors increasingly utilize intelligent systems capable of mimicking human behavior, analyzing security patterns, and executing unauthorized transactions—all while leaving minimal digital traces. These offenses are not only more sophisticated but also more autonomous, scalable, and resistant to conventional investigative techniques (McGuire, 2019, p. 78).

One of the most notable manifestations is electronic banking fraud, where machine learning models are trained to behave like legitimate customers. These bots simulate normal transaction behaviors, allowing them to bypass fraud detection systems that rely on behavioral anomalies. By deploying stolen credentials in combination with AI-driven pattern recognition, attackers can create nearly undetectable transaction flows (Levi & Soudijn, 2020, p. 390).

Another growing trend is unauthorized access to financial databases, where AI tools systematically scan institutional networks for vulnerabilities—such as outdated encryption, exposed APIs, or misconfigured cloud infrastructure. Once a weakness is detected, the system launches automated scripts that extract, reroute, or erase financial data in real-time. This minimizes both the exposure time and the likelihood of forensic recovery (Brenner, 2017, p. 67).

Equally concerning is the increasing use of artificial intelligence in money laundering.

Criminal networks employ algorithmic tools to divide large transactions into micro-payments, distribute them across decentralized platforms, and reassemble them later through anonymous wallets. The automation of these processes makes it difficult for financial monitoring authorities to detect suspicious activity in a timely manner (Unger & Ferwerda, 2022, p. 482).

AI-based financial crimes are no longer hypothetical—they are currently active and widespread across various jurisdictions. They pose significant challenges not only in terms of prevention but also with regard to legal qualification and evidentiary admissibility in court, especially in systems that lack updated legal provisions addressing autonomous digital misconduct (Broadhurst, 2020, p. 10).

1.1.2 Criminal Mechanisms Based on Artificial Intelligence

The reliance on artificial intelligence in executing crimes has evolved from passive use—such as evading surveillance or encrypting communication—to active involvement in designing and carrying out complex criminal schemes. What distinguishes these mechanisms is not just their technical sophistication, but their growing autonomy. In many cases, human oversight is minimal or even absent during the execution phase of the offense (Taddeo & Floridi, 2018, p. 751).

AI-driven systems are now used to identify legal loopholes, monitor judicial precedent databases, and suggest optimized criminal paths that minimize risk. Algorithms have been deployed to select the most vulnerable targets in phishing campaigns, determine optimal times to launch attacks based on digital traffic, or adjust the method of execution dynamically as a response to real-time feedback (Buchanan, 2020, p. 134).

A particularly concerning mechanism involves the use of generative adversarial networks (GANs) to produce synthetic identities or bypass biometric security. These models can create convincing digital fingerprints, facial data, or even voiceprints that allow unauthorized access to secure platforms or impersonation in legal and financial procedures (Kietzmann et al., 2018, p. 265).

Another dimension includes the automation of social engineering tactics, whereby AI chatbots and language models are programmed to build long-term deceptive relationships with victims, extract sensitive data, or guide them into compromising behaviors. The intelligence of these systems lies in their adaptability and emotional mimicry, allowing them to fine-tune responses based on the psychological profile of the target (Whittaker et al., 2018, p. 22).

What makes these mechanisms legally problematic is their partial or complete detachment from human intent. Traditional criminal law is built upon the principle of *mens rea*—the guilty mind—but in algorithmic crime, the intent may be coded into the system without real-time human decision-making. This raises fundamental questions about liability, attribution, and the threshold for criminal responsibility in AI-mediated acts (Caldwell & Reilly, 2021, p. 115).

1.1.3 Legal Challenges Related to the Use of Algorithms

The integration of algorithmic systems into criminal activity has raised a series of legal challenges that traditional frameworks struggle to address. Chief among these is the question of how to establish criminal intent when the act is carried out, not directly by a human, but through an automated or semi-autonomous system (Caldwell & Reilly, 2021, p. 110).

In conventional legal reasoning, criminal responsibility hinges on the presence of *mens rea*—the guilty mind—accompanied by a prohibited act. However, when an algorithm executes a crime based on pre-coded instructions or adaptive learning processes, the attribution of intent

becomes more complex. Should the liability fall upon the programmer, the operator, or the entity that deployed the system? These questions are currently the subject of active debate in legal scholarship (Sartor, 2020, p. 497).

Another pressing issue is the opacity of algorithmic systems, often referred to as the "black box" problem. Many AI models—especially deep learning systems—do not offer explainable outputs, making it difficult for investigators, judges, or even experts to understand how decisions were reached. This lack of transparency undermines the principles of fair trial and due process, particularly when such systems are used to produce evidence or guide prosecutorial decisions (Selbst & Barocas, 2018, p. 1089).

Furthermore, the cross-border nature of algorithmic crime complicates matters of jurisdiction, cooperation, and enforcement. A single algorithm can operate simultaneously in multiple countries, targeting victims and systems in diverse legal environments, all while being hosted in yet another jurisdiction. Existing legal frameworks are often inadequate to handle such decentralized and transnational operations (Clough, 2014, p. 700).

Finally, there is the problem of evidentiary admissibility. Digital evidence produced or processed by AI systems may face challenges in being accepted in court, especially if the system's functioning cannot be audited or verified. Courts may be reluctant to rely on outputs whose internal logic cannot be scrutinized or replicated by human experts (Kroll et al., 2017, p. 640).

1.2 Deepfake Technology in Blackmail and Defamation Crimes

Deepfake technology—based on artificial intelligence models capable of generating hyper-realistic synthetic audio-visual content—has emerged as one of the most controversial tools of digital manipulation. While originally developed for entertainment and creative applications, its malicious use has grown alarmingly widespread. Offenders are increasingly relying on this technique to fabricate compromising media involving public figures, professionals, or private individuals, often with the intent to defame, extort, or discredit (Chesney & Citron, 2019, p. 1760).

What makes deepfakes particularly dangerous from a legal perspective is their high level of realism and the difficulty of proving falsification, especially when the targeted individuals are unable to immediately access technical expertise. The boundary between fact and fabrication becomes increasingly blurry, challenging legal definitions of evidence, identity, and intentional harm (Paris & Donovan, 2019, p. 12).

This section will examine the nature of deepfake technology, its role in blackmail and defamation, and the legal frameworks—both comparative and national—that attempt to address these emerging risks.

1.2.1 The Nature of Deepfake Technology

Deepfake technology is grounded in machine learning systems—particularly Generative Adversarial Networks (GANs)—that are capable of producing highly realistic images, videos, and audio clips based on training data. These systems operate by having one neural network generate fake content while another evaluates its realism, creating an iterative loop that improves the authenticity of the output over time (Goodfellow et al., 2014, p. 2680).

Unlike traditional forms of editing or digital manipulation, deepfakes do not require manual frame-by-frame adjustments. Instead, they automate the process of facial swapping, voice cloning, and motion synthesis, allowing even non-experts to produce convincing forgeries using publicly available tools. This democratization of forgery represents a fundamental shift in

how misinformation and personal harm can be created and distributed (Westerlund, 2019, p. 42).

From a legal and evidentiary standpoint, the challenge with deepfakes lies in their plausibility. Courts, investigators, and even forensic experts may find it difficult to distinguish between authentic and synthetic content without advanced technical intervention. This not only jeopardizes the integrity of legal proceedings but also threatens individual rights such as reputation, privacy, and dignity (Maras & Alexandrou, 2019, p. 258).

The phenomenon of deepfake creation and dissemination has expanded beyond private disputes and now touches political discourse, judicial credibility, and corporate integrity. As such, understanding its technological underpinnings is essential for legal systems seeking to regulate its misuse and mitigate its harms (Citron & Chesney, 2020, p. 150).

1.2.2 Forms of Blackmail and Defamation Crimes Using AI Tools

Artificial intelligence has enabled the creation of new criminal tactics in the realm of defamation and extortion, most notably through the use of deepfake technology and synthetic media. These tools have allowed offenders to fabricate content that appears indistinguishably real, and then weaponize it against victims for financial gain, personal revenge, or reputational destruction (Chesney & Citron, 2019, p. 1765).

A common scenario involves the fabrication of sexually explicit videos featuring public figures or private individuals whose likenesses are digitally superimposed using deep learning. These synthetic videos are often used to extort victims under the threat of online publication or public exposure (Paris & Donovan, 2019, p. 15).

Other cases include fabricated audio recordings allegedly capturing incriminating statements—used in both political and corporate settings to destabilize opponents or extract concessions. In defamation contexts, such content is disseminated online with the intent to harm the social standing, credibility, or employment of the targeted individual (Westerlund, 2019, p. 50).

The speed of dissemination enabled by social media platforms amplifies the damage caused by these forgeries. Victims often suffer reputational harm before any forensic validation can occur. Moreover, even when content is proven to be false, the correction rarely receives the same attention or reach as the original material (Vaccari & Chadwick, 2020, p. 3).

The legal consequences of these acts are severe, but prosecution is complicated by the technical sophistication of the forgeries and the frequent use of anonymizing tools such as VPNs or offshore servers. As such, these crimes represent a hybrid threat: technologically complex, legally ambiguous, and socially destabilizing (King & Schindler, 2021, p. 95).

1.3 Exploitation of Chatbots to Entrap Victims

Conversational agents, commonly referred to as chatbots, have evolved from simple rule-based programs into highly sophisticated AI systems capable of simulating natural, context-aware dialogue. These systems are increasingly employed in commercial, administrative, and even therapeutic settings—but their misuse in criminal schemes has grown in tandem with their capabilities (Floridi & Cows, 2019, p. 15).

Malicious actors now exploit intelligent chatbots to extract sensitive information, manipulate human emotions, and construct deceptive relationships with victims. Unlike phishing emails or traditional scams, chatbots engage in interactive, real-time dialogue, creating a false sense of trust and legitimacy. This makes them particularly effective in grooming, psychological manipulation, and digital fraud (Neff & Nagy, 2016, p. 4920).

The criminal use of chatbot systems introduces a complex intersection between AI ethics, digital privacy, and criminal liability. This section explores how chatbots are used to facilitate criminal entrapment and the difficulties investigators face in detecting and prosecuting such activity.

1.3.1 Methods Used in AI-Based Victim Entrapment

The criminal use of chatbots involves a variety of techniques designed to manipulate or deceive individuals through automated conversations. These bots are often deployed on social media platforms, messaging apps, and dating websites, where they pose as real users and initiate seemingly genuine interactions (Neff & Nagy, 2016, p. 4927).

One common method is the gradual collection of personal and financial information. By simulating emotionally supportive dialogue or romantic interest, chatbots are able to extract bank details, login credentials, or identity documents over time. The victim may believe they are speaking with a trusted acquaintance or partner, unaware that the interaction is fully automated (Cresci et al., 2017, p. 965).

Another tactic involves posing as institutions or customer service agents, where chatbots mimic official tone and language to request account verifications, password resets, or sensitive identification data. This method is particularly effective when the bot is programmed to respond dynamically to user hesitation or suspicion (Lee & Kim, 2019, p. 190).

Some bots are designed to manipulate emotional states, using sentiment analysis to detect when a user is vulnerable, isolated, or distressed. They then steer the conversation toward emotional dependence, requests for financial help, or compromising disclosures—often leading to extortion or blackmail (Adams & Miles, 2020, p. 195).

The technological sophistication of these systems makes detection difficult. Many users do not realize they are interacting with a machine until the damage has already occurred. Moreover, the decentralized nature of deployment, often using proxy servers or anonymized infrastructures, complicates the identification and prosecution of perpetrators (Koshiyama et al., 2021, p. 355).

1.3.2 Legal Challenges in Proving the Crime

Proving criminal offenses committed through chatbot systems presents complex procedural and evidentiary challenges. Unlike traditional forms of fraud or extortion that involve human interaction, chatbot-driven crimes rely on automated dialogue engines that operate without direct, real-time human control. This disconnect raises immediate doubts about intentionality and accountability, which are central to criminal prosecution (Caldwell & Reilly, 2021, p. 118).

A core difficulty lies in demonstrating the fraudulent intent (*dolus malus*) behind the chatbot's operation. If the bot was pre-programmed with manipulative scripts, prosecutors must establish who authored, launched, and maintained the system. This task becomes particularly difficult when the code is hosted anonymously or sourced from public repositories without clear ownership (Christakis, 2022, p. 45).

Another issue involves the admissibility of chatbot-generated conversations as legal evidence. Courts must determine whether the dialogues—often stored in transient messaging platforms—are authentic, complete, and untampered. The lack of metadata, digital signatures, or verified timestamps can lead to disputes over reliability and chain of custody (Kroll et al., 2017, p. 650).

Additionally, some jurisdictions have yet to clearly regulate the legal status of automated

communications. Is a conversation with a chatbot equivalent to a conversation with a human in terms of legal effect? Can victims be considered deceived if no human ever interacted with them? These doctrinal uncertainties complicate both the prosecution and the protection of victims' rights (Sartor, 2020, p. 500).

Finally, chatbot interactions often cross jurisdictional boundaries, with servers, users, and victims located in different legal systems. This complicates both investigation and enforcement, as it requires international cooperation, mutual legal assistance treaties (MLATs), and compliance with privacy and data protection laws (Clough, 2020, p. 510).

2. The Role of Artificial Intelligence Tools in Solving Crimes

As criminal techniques have grown more sophisticated through the use of artificial intelligence, so too have investigative methods. Law enforcement agencies across the world are increasingly incorporating AI-based tools to enhance their ability to analyze evidence, detect patterns, and anticipate criminal behavior. These technologies range from big data analytics and facial recognition to voice analysis and behavioral assessment (Kroll et al., 2017, p. 670).

AI applications in criminal investigation are not limited to technical efficiency; they also raise fundamental questions about legality, procedural fairness, and the protection of human rights. The use of predictive algorithms and biometric tracking can significantly improve the accuracy and speed of investigations, but they must operate within strict legal boundaries to prevent abuses and ensure judicial integrity (Meijer & Wessels, 2019, p. 1035).

This section explores the major categories of AI tools currently used in criminal investigations, evaluating their technical capacity and legal validity. It focuses on how these systems contribute to identifying suspects, establishing evidence, and clarifying the circumstances of complex crimes.

2.1 Big Data Analysis and Criminal Network Mapping

The use of big data analytics in criminal investigations represents one of the most transformative shifts in modern law enforcement. By aggregating vast volumes of structured and unstructured data—from financial records and social media activity to geolocation signals and communication metadata—AI systems can identify hidden patterns and reconstruct complex criminal networks with unprecedented precision (Meijer & Wessels, 2019, p. 1038).

These technologies allow investigators not only to analyze past events but also to anticipate future risks and establish links between suspects, events, and digital evidence. This form of network intelligence has become particularly useful in tackling organized crime, cybercrime, and terrorism, where individual actors are often part of broader, decentralized structures (Helbing & Pournaras, 2015, p. 33).

Despite its effectiveness, big data-driven investigation raises important legal and ethical concerns. Chief among them is the tension between surveillance efficiency and privacy rights, especially in jurisdictions where data protection laws are either weak or inconsistently enforced (Tzanou, 2017, p. 75).

This section will examine how big data technologies are used in law enforcement settings, their legal basis, and the judicial limits that must govern their deployment.

2.1.1 Investigative Techniques in Criminal Justice Using Big Data

Artificial intelligence has reshaped traditional investigative techniques by enabling the analysis of large-scale datasets in real time. One of the most prominent applications is the tracking of suspicious financial transactions, where algorithms scan cross-border transfers,

cryptocurrency exchanges, and shell company activity to detect anomalies that may indicate money laundering or illicit funding (Levi & Soudijn, 2020, p. 395).

In the context of cybercrime and organized criminal activity, AI-powered platforms can map relationships between suspects, digital identifiers, and physical movements. These systems use graph-based models to visualize connections across various data points—such as shared IP addresses, common transaction patterns, or synchronized communications—thereby uncovering entire criminal networks from minimal initial evidence (Vandeppeer & Broadhurst, 2019, p. 100).

Another valuable technique involves temporal analysis, which enables investigators to reconstruct a timeline of events leading up to or following a crime. By analyzing timestamps from surveillance footage, login records, and mobile device pings, authorities can create high-resolution chronologies that help establish presence, complicity, or intent (Ferguson, 2017, p. 110).

Moreover, predictive analytics allows for behavioral forecasting, particularly in cases involving repeat offenders or criminal groups operating in patterns. AI models trained on historical data can highlight potential future offenses or targets, thus informing surveillance strategies and preemptive measures (Perry et al., 2013, p. 45).

While these methods enhance efficiency and accuracy, their legality hinges on adherence to evidentiary standards, judicial oversight, and respect for constitutional protections. Without these safeguards, the use of big data may shift from an investigative tool to a mechanism of unlawful surveillance (Tzanou, 2017, p. 120).

2.1.2 The Legal Framework Governing Investigative Methods

The integration of artificial intelligence and big data into criminal investigations must operate within a defined legal framework to ensure that constitutional rights—particularly the right to privacy and due process—are not compromised. Most legal systems require that data collection and analysis be justified by law, necessary for a legitimate aim, and proportionate to that aim (Kuner et al., 2019, p. 70).

In the European context, the General Data Protection Regulation (GDPR) establishes strict rules for data processing, including safeguards for profiling and automated decision-making. Law enforcement agencies must demonstrate that their use of big data tools is both necessary and subject to independent oversight. Violations may result in the exclusion of evidence or civil liability (European Parliament & Council, 2016, p. 1).

Several jurisdictions have adopted specific legislation governing surveillance and digital forensics, such as the UK's Investigatory Powers Act (2016) or Germany's Federal Data Protection Act (BDSG), both of which impose requirements for authorization, transparency, and data minimization when employing automated systems in investigations (UK Parliament, 2016, p. 5).

However, in Algeria, while Law No. 18-07 on the protection of individuals with regard to personal data processing (2018) introduces some basic safeguards, it lacks clear mechanisms regulating AI-based surveillance or big data analytics in criminal justice. The Penal Procedure Code remains largely silent on algorithmic evidence and the procedural rules governing its use (Djefflat, 2021, p. 210).

Judicial interpretation also plays a crucial role. Courts must assess whether AI-derived evidence meets admissibility standards, including authenticity, integrity, and relevance. Where the internal workings of an algorithm are opaque or unexplainable, the principle of equality of arms may be undermined, potentially violating the defendant's right to a fair trial (Kroll et al., 2017, p. 660).

2.2 Facial Recognition and Motion Analysis Technologies

Facial recognition and motion analysis technologies have become integral tools in modern criminal investigations. By leveraging biometric data and video analytics, law enforcement agencies can identify suspects, track movements, and verify the authenticity of surveillance footage. These technologies are increasingly used in public security settings such as airports, border crossings, and urban monitoring systems (Garvie et al., 2016, p. 25).

The application of these tools is not without controversy. Critics have raised concerns about accuracy, racial or gender bias, and the potential for mass surveillance. Additionally, legal systems are still grappling with questions regarding the legality of biometric evidence, particularly in the absence of informed consent or judicial authorization (Babuta & Oswald, 2020, p. 12).

This section will explore how facial recognition and motion tracking are employed in criminal proceedings, and examine the legal conditions under which such evidence can be used, challenged, or excluded.

2.2.1 Areas of Application for Facial Recognition and Motion Tracking

Facial recognition and motion analysis technologies are employed across a range of investigative contexts, primarily aimed at identifying suspects, verifying presence at crime scenes, and monitoring public spaces for security threats. These tools allow law enforcement to automatically match facial images captured from surveillance footage with databases of known individuals or wanted persons (Garvie et al., 2016, p. 40).

In high-traffic environments—such as airports, train stations, or political events—facial recognition systems serve as an early warning mechanism, flagging individuals of interest in real time. Motion tracking tools complement this by analyzing gait, speed, and spatial movement, enabling investigators to reconstruct suspect behavior over time (Introna & Wood, 2004, p. 180).

Another critical use involves the validation of alibis or claims of presence/absence. Investigators can compare timestamps from surveillance cameras with facial data to confirm or refute a suspect's narrative. This has proven particularly useful in urban settings where multiple surveillance points can be cross-referenced (Ferguson, 2017, p. 88).

Furthermore, facial recognition is now being used for digital forensics, helping to identify individuals in illicit online content, such as child exploitation materials or extremist propaganda. Here, AI tools scan millions of frames and detect recurring faces or body patterns across platforms (Babuta & Oswald, 2020, p. 20).

Despite their efficiency, these technologies are vulnerable to false positives, especially in diverse populations where algorithmic bias may distort accuracy. Legal challenges also arise when such tools are used without proper judicial oversight, potentially infringing on privacy and data protection rights (Buolamwini & Gebru, 2018, p. 5).

2.2.2 Legal Foundation of Facial Recognition and Motion Tracking

The legal use of facial recognition and motion analysis technologies hinges on a delicate balance between public safety and the protection of fundamental rights. While these tools can significantly enhance criminal investigations, their deployment must comply with legal norms governing privacy, data protection, and due process (Tzanou, 2017, p. 90).

In European law, the use of biometric technologies by law enforcement is governed by the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED).

These frameworks impose strict conditions on the collection and processing of biometric data, including the necessity of a legal basis, proportionality, and the requirement for independent oversight (European Parliament & Council, 2016, p. 5).

The European Court of Human Rights (ECtHR) has also ruled on the issue of surveillance and facial recognition, emphasizing the need for safeguards against arbitrary interference. In *S. and Marper v. United Kingdom*, the Court held that the retention of biometric data without justification violates Article 8 of the European Convention on Human Rights (European Court of Human Rights, 2008, p. 12).

National laws vary in their approach. For example, Germany's Federal Constitutional Court has ruled that the deployment of facial recognition technologies must be clearly authorized by statute and subject to judicial supervision, particularly when used in public spaces (German Federal Constitutional Court, 2020, p. 3). In contrast, France has allowed limited pilot use of such tools in educational and transportation contexts, though always under the scrutiny of the CNIL (Commission nationale de l'informatique et des libertés) (CNIL, 2020, p. 2).

In Algeria, the legal framework governing biometric surveillance is still underdeveloped. Although Law No. 18-07 (2018) provides general provisions on data protection, it does not specifically address facial recognition or AI-powered motion tracking. This legislative gap creates uncertainty regarding the admissibility of such evidence and the legal responsibility of authorities using it (Djefflat, 2021, p. 215).

Ultimately, the admissibility of biometric evidence depends not only on its technical accuracy but also on compliance with procedural safeguards, such as prior authorization, notice to the defense, and the right to challenge its reliability in court (Kroll et al., 2017, p. 640).

2.3 Voice and Body Language Analysis

The integration of artificial intelligence into the analysis of voice and body language has opened new frontiers in criminal investigation. These tools aim to detect verbal and non-verbal cues associated with deception, stress, or concealment, providing law enforcement with an additional layer of behavioral insight during interrogations or witness interviews (Vrij et al., 2017, p. 5).

Voice analysis systems rely on acoustic features such as pitch, tone, hesitation, and rhythm to assess emotional states or identify inconsistencies in speech patterns. In parallel, body language recognition software analyzes facial expressions, gestures, and micro-movements to infer intent or detect signs of psychological discomfort (De Paoli & Kerr, 2020, p. 8).

While these technologies offer promising investigative support, they raise significant concerns about scientific validity, reliability, and ethical admissibility. Questions persist about the accuracy of AI-based behavioral inference and the risk of bias, especially when used as evidence in criminal proceedings (Wagner, 2019, p. 80).

This section will explore the technical foundations of these systems, their role in modern interrogation practices, and the legal standards that govern their admissibility and use in court.

2.3.1 Detecting Stress and Deception During Interrogation

Artificial intelligence technologies are increasingly being deployed in the context of criminal interrogations to detect signs of deception or psychological stress. These systems are designed to analyze both vocal characteristics and physical behaviors in order to identify inconsistencies, emotional tension, or attempts at concealment. The premise is that lying produces measurable physiological and behavioral changes, which AI can be trained to recognize (Vrij et al., 2017, p. 10).

In practice, such tools assess acoustic features—such as voice pitch, speech latency, and intonation shifts—as potential indicators of dishonesty. For instance, a sudden change in tone or hesitation when responding to a specific question may be flagged by the system as suggestive of stress or evasion (Sénéchal & Geoffroy, 2020, p. 5).

Simultaneously, computer vision algorithms track facial expressions, pupil dilation, micro-expressions, and hand gestures to detect non-verbal indicators of deception. These tools rely on extensive databases of recorded behaviors to establish predictive models, which are then applied in real time during questioning (De Paoli & Kerr, 2020, p. 9).

Despite their growing popularity, these systems face serious scientific and legal challenges. Critics point out that emotional responses vary widely among individuals, making generalized models unreliable. Cultural differences, trauma histories, or even medical conditions may produce physiological signals that mimic deception, leading to false positives (LoPalo & Gruber, 2021, p. 250).

Moreover, the use of such technologies raises procedural fairness issues, particularly when suspects are unaware they are being analyzed by AI or when the output is used as substantive evidence without human review. Courts have begun to scrutinize the admissibility of behavior-detection algorithms, emphasizing the need for transparency, explainability, and expert interpretation (Wagner, 2019, p. 87).

2.3.2 Voice Comparison with Stored Samples

Voice comparison has become an essential forensic technique in criminal investigations, particularly in cases involving anonymous threats, ransom calls, or covert recordings. With advancements in artificial intelligence, law enforcement agencies now rely on automated speaker recognition systems to match unknown voice recordings with stored samples from suspects or criminal databases (Drygajlo, 2015, p. 2).

These systems analyze a range of vocal features—including frequency, tone, speech rhythm, and vocal tract characteristics—to create a voiceprint, a unique acoustic profile akin to a fingerprint. Once generated, this voiceprint is compared with existing recordings to determine the likelihood of a match (Morrison & Enzinger, 2019, p. 630).

AI-based voice comparison tools have several advantages over manual analysis. They can process thousands of samples in minutes, detect subtle variations undetectable to human ears, and account for differences caused by stress, environment, or audio quality. As a result, they are increasingly used in complex investigations such as terrorism, organized crime, and cross-border fraud (Zhang & Hansen, 2020, p. 285).

However, the admissibility of voice recognition evidence remains a contested issue in many legal systems. Concerns persist regarding the margin of error, especially in noisy recordings or when the speaker attempts to disguise their voice. Moreover, differences in hardware, recording conditions, or the absence of standardization across systems may affect reliability (French, 2020, p. 3).

Legal standards generally require that such evidence be supported by expert testimony, and that the underlying methodology meets the Daubert or Frye criteria (in the U.S.) or equivalent admissibility rules elsewhere. In some jurisdictions, courts have excluded AI-generated voice matches when the algorithm's internal workings were considered a “black box,” preventing meaningful scrutiny by the defense (Kroll et al., 2017, p. 675).

2.3.3 Evidentiary Value of AI-Based Voice and Behavior Analysis

The use of artificial intelligence in analyzing voice and body language has sparked an ongoing debate regarding the evidentiary weight of such tools in criminal proceedings. While

these technologies can support investigations by generating behavioral insights or identifying suspects, their reliability as primary evidence remains subject to legal scrutiny (LoPalo & Gruber, 2021, p. 255).

Courts generally assess the admissibility of AI-generated outputs based on criteria such as scientific validity, methodological transparency, and compliance with procedural safeguards. In some jurisdictions, particularly within the European Union and the United States, evidence derived from machine learning tools must be subject to expert interpretation and cross-examination to ensure the rights of the defense (Schindler, 2021, p. 60).

A key challenge is the "black box" nature of many AI systems, especially those using deep learning algorithms. These models may produce highly accurate results, but without clear explanations of how decisions are made, judges and juries may struggle to evaluate their probative value. This lack of explainability raises concerns under the principle of a fair trial, particularly the right to challenge evidence effectively (Kroll et al., 2017, p. 665).

Another issue relates to the standardization and accreditation of these tools. Unlike DNA testing or fingerprint analysis, which follow internationally recognized protocols, voice and behavior recognition systems vary widely in quality, calibration, and methodological consistency. This disparity undermines the possibility of uniform evidentiary standards across courts (Morrison, 2018, p. 270).

Ultimately, most legal systems treat AI-based behavior analysis as supporting evidence—useful when corroborated by additional proof, but insufficient on its own to sustain conviction. Without legislative or judicial guidelines to ensure its appropriate use, overreliance on these tools could compromise both the presumption of innocence and the integrity of the judicial process (Wagner, 2019, p. 85).

II. Conclusion:

This study has demonstrated that the growing integration of artificial intelligence into both the perpetration and investigation of crimes has profoundly transformed the dynamics of criminal justice. On the one hand, AI enables increasingly sophisticated and difficult-to-detect criminal behaviors, such as algorithmic fraud, deepfakes, and chatbot-based entrapment. On the other hand, the same technologies are proving to be powerful investigative tools, capable of analyzing large-scale data, identifying suspects through biometric analysis, and providing behavioral insights during interrogations.

Key Results

- AI-driven crimes are characterized by their complexity and speed, making them difficult to address using traditional legal tools.
- Deepfake, voice cloning, and behavioral manipulation technologies have created new categories of digital harm not clearly addressed by existing laws.
- Law enforcement agencies in technologically advanced countries are already using AI for predictive policing, network analysis, and automated interrogation—raising questions about procedural legality and the rights of the accused.
- The legal admissibility of evidence generated through AI remains a source of doctrinal and practical ambiguity, particularly where algorithms lack transparency or standardization.
- Algerian legislation lags behind in regulating AI-related crimes and investigations, lacking precise provisions to address the legal nature of synthetic media, algorithmic

fraud, or automated interrogation.

Recommendations

- Legislative reforms are necessary to define and criminalize emerging AI-based offenses such as deepfake extortion, voice forgery, and behavioral entrapment.
- Clear procedural frameworks must be established for the use of AI tools in investigations, including safeguards for privacy, data protection, and the right to silence.
- Courts must adopt evidentiary standards tailored to algorithmic outputs, ensuring that their scientific validity, traceability, and susceptibility to cross-examination are properly assessed.
- Awareness and training should be provided to judges, prosecutors, and law enforcement officers on the risks and limits of using AI in criminal justice.

Algerian authorities should initiate comparative studies and international cooperation to harmonize their legal framework with best practices from jurisdictions that have already begun to regulate AI in criminal matters.

Referrals and references:

Legislation & Case Law

1. Assemblée Nationale (France). (2018). Loi sur la sécurité numérique n°2018-493.
2. California Legislature. (2018). California Bot Disclosure Law (SB-1001).
3. CNIL. (2020). Facial recognition: The CNIL's position on experiments in schools.
4. European Commission. (2021). Proposal for a Regulation on Artificial Intelligence (Artificial Intelligence Act), COM (2021) 206 final.
5. European Court of Human Rights. (1996). Saunders v. United Kingdom, App. No. 19187/91.
6. European Court of Human Rights. (2008). S. and Marper v. United Kingdom, App. Nos. 30562/04 and 30566/04.
7. European Parliament & Council. (2016). General Data Protection Regulation (EU) 2016/679 and Directive (EU) 2016/680. Official Journal of the European Union.
8. German Bundestag. (2017). Network Enforcement Act (NetzDG). Federal Law Gazette I, 3352.
9. German Federal Constitutional Court. (2020). Facial recognition ruling, BVerfG 1 BvR 321/19.
10. Government of Canada. (2015). Cybercrime Act (S.C. 2015, c. 31).
11. UK Government. (2022). Draft Online Safety Bill.
12. UK Parliament. (2016). Investigatory Powers Act 2016.

An introduction that presents the specific problem under study and describes the research strategy.

Books

1. Buchanan, B. (2020). The hacker and the state: Cyber attacks and the new normal of geopolitics. Harvard University Press.
2. Casey, E. (2019). Digital evidence and computer crime: Forensic science, computers and the internet. Academic Press.
3. Ferguson, A. G. (2017). The rise of big data policing: Surveillance, race, and the future of law enforcement. NYU Press.
4. McStay, A. (2020). Emotional AI: The rise of empathic media. SAGE Publications.
5. Tzanou, M. (2017). The fundamental right to data protection: Normative value in the context of counter-terrorism surveillance. Hart Publishing.

Journal articles

1. Adams, R., & Miles, S. (2020). Emotionally intelligent chatbots: Risks and vulnerabilities. *AI & Society*, 35(1), 189–200.
2. Brennan-Marquez, K. (2018). Automated suspicion: AI, policing, and the Fourth Amendment. *Harvard Journal of Law & Technology*, 31(1), 1–47.
3. Broadhurst, R. (2020). Artificial intelligence and crime: A review. *Crime, Law and Social Change*, 73(1), 5–22.
4. Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(6), 1753–1819.
5. Citron, D. K., & Chesney, R. (2020). Deepfakes and the new disinformation war. *Foreign Affairs*, 99(1), 147–155.
6. Citron, D. K., & Chesney, R. (2021). Deepfakes and the new disinformation threat. *Georgetown Law Journal*, 109(4), 1011–1058.
7. Clough, J. (2014). A world of difference: The Budapest Convention on Cybercrime and the challenge of harmonisation. *Monash University Law Review*, 40(3), 698–736.
8. Clough, J. (2020). International criminal jurisdiction in the age of AI. *International Criminal Law Review*, 20(3), 497–522.
9. Floridi, L., & Cows, J. (2019). A unified framework of five principles for AI in society. *Harvard Data Science Review*, 1(1). <https://doi.org/10.1162/99608f92.8cd550d1>
10. Floridi, L., & Taddeo, M. (2014). The ethics of information warfare. *Minds and Machines*, 24(1), 1–6.
11. Helbing, D., & Pournaras, E. (2015). Society: Build digital democracy. *Nature*, 527(7576), 33–34.
12. Kietzmann, J., Paschen, J., & Treen, E. (2018). Artificial intelligence in advertising: How GANs are reshaping the creative industry. *Journal of Advertising Research*, 58(3), 263–267.
13. Koene, A., & de Hert, P. (2018). The challenges of AI evidence in criminal courts. *European Journal of Law and Technology*, 9(2).
14. Koshiyama, A., Frosi, P., Treleaven, P., & Gharib, M. (2021). AI and financial crime: Emerging challenges. *Journal of Financial Regulation and Compliance*, 29(3), 350–367.
15. Kroll, J. A., Barocas, S., Hardt, M., Narayanan, A., Rieke, A., Robinson, D., & Yu, H. (2017). Accountable algorithms. *University of Pennsylvania Law Review*, 165(3), 633–706.
16. Levi, M., & Soudijn, M. (2020). Technology and financial crime: Challenges for criminal justice. *European Journal on Criminal Policy and Research*, 26(4), 385–404.
17. LoPalo, N., & Gruber, J. (2021). Deception detection: Between behavioral science and machine learning. *Annual Review of Law and Social Science*, 17, 243–264.
18. Maras, M. H., & Alexandrou, A. (2019). Determining authenticity of video evidence in the age of artificial intelligence and in the wake of deepfake videos. *The International Journal of Evidence & Proof*, 23(3), 255–262.
19. Meijer, A., & Wessels, M. (2019). Predictive policing: Review of benefits and drawbacks. *International Journal of Public Administration*, 42(12), 1031–1039.
20. Mirsky, Y., & Lee, W. (2021). The creation and detection of deepfakes: A survey. *ACM Computing Surveys*, 54(1), 1–41.
21. Morrison, G. S. (2018). Forensic voice comparison and the paradigm shift. *Science & Justice*, 58(4), 267–272.
22. Morrison, G. S., & Enzinger, E. (2019). Forensic voice comparison. In W. F. Katz & P. F. Assmann (Eds.), *The Routledge Handbook of Phonetics* (pp. 623–641). Routledge.
23. Neff, G., & Nagy, P. (2016). Talking to bots: Symbiotic agency and the case of Tay. *International Journal of Communication*, 10, 4915–4931.
24. Sartor, G. (2020). Artificial intelligence and criminal law: New challenges. *European Journal of Risk Regulation*, 11(3), 495–505.
25. Schindler, R. (2021). The reversal of the burden of proof in digital defamation: The deepfake dilemma. *Law, Technology and Society*, 13(1), 45–67.
26. Selbst, A. D., & Barocas, S. (2018). The intuitive appeal of explainable machines. *Fordham Law Review*, 87(3), 1085–1139.
27. Sénéchal, T., & Geoffroy, P. A. (2020). Automatic stress detection in speech: Current advances

- and future directions. *Speech Communication*, 122, 1–12.
28. Unger, B., & Ferwerda, J. (2022). Artificial intelligence and money laundering. *Journal of Financial Crime*, 29(2), 479–494.
 29. Vaccari, C., & Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact on democracy. *Social Media + Society*, 6(1), 1–7.
 30. Vrij, A., Fisher, R. P., & Blank, H. (2017). A cognitive approach to lie detection: A meta-analysis. *Legal and Criminological Psychology*, 22(1), 1–21.
 31. Wagner, B., & Eidenbenz, S. (2021). AI regulation and human rights: Balancing innovation and accountability. *Computer Law & Security Review*, 41, 105561.
 32. Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review*, 9(11), 40–53.
 33. Zhang, C., & Hansen, J. H. L. (2020). Advancements in forensic speaker recognition: Deep learning approaches. *IEEE Transactions on Audio, Speech, and Language Processing*, 28, 283–295.

Conference papers & book chapters

1. Cresci, S., Di Pietro, R., Petrocchi, M., Spognardi, A., & Tesconi, M. (2017). The paradigm-shift of social spambots: Evidence, theories, and tools for the arms race. In *Proceedings of the 26th International Conference on World Wide Web Companion* (pp. 963–972). International World Wide Web Conferences Steering Committee.
2. Drygajlo, A. (2015). Forensic automatic speaker recognition. In R. A. Myers (Ed.), *Wiley Encyclopedia of Forensic Science* (pp. 1–12).
3. Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... & Bengio, Y. (2014). Generative adversarial nets. In *Advances in Neural Information Processing Systems* (Vol. 27, pp. 2672–2680).
4. Luger, E., & Sellen, A. (2016). “Like having a really bad PA”: The gulf between user expectation and experience of conversational agents. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 5286–5297). ACM.
5. Perry, W. L., McInnis, B., Price, C. C., Smith, S. C., & Hollywood, J. S. (2013). Predictive policing: The role of crime forecasting in law enforcement operations. RAND Corporation.

Reports

1. Garvie, C., Bedoya, A., & Frankle, J. (2016). *The Perpetual Line-Up: Unregulated police face recognition in America*. Center on Privacy & Technology, Georgetown Law.
2. Paris, B., & Donovan, J. (2019). *Deepfakes and cheap fakes: The manipulation of audio and visual evidence*. Data & Society Research Institute.
3. Whittaker, M., Alper, M., Crawford, K., Dobbe, R., Fried, G., Kaziunas, E., ... & Schwartz, O. (2018). *AI Now Report 2018*. AI Now Institute.