Transnational Cybercrime: Challenges of** Criminalization, Jurisdiction, and Criminal **Justice in the Age of Virtual Sovereignty

Authored by: Dr. Mohamed Kamal**

**Ourfah Al-Rakhawi

Dedication

To my Egyptian-Algerian daughter Sabreena, the light of my eyes and the fruit of my heart, who carries in her roots the palms of the Nile Valley and the Atlas

Mountains, and in her soul the spirit of Egypt and the fragrance of Algeria. To you, this work—may it be a brick in a safer, more just world that you and your generation inherit not through fear, but .through knowledge and wisdom

Introduction

In a world where geographical borders no longer impede the flow of data, crime**Transnational Cybercrime: Challenges of Criminalization, Jurisdiction,

and Criminal Justice in the Age of Virtual **Sovereignty

Authored by: Dr. Mohamed Kamal**

**Ourfah Al-Rakhawi

Dedication

To my Egyptian-Algerian daughter Sabreena, the light of my eyes and the fruit of my heart, who carries in her roots the palms of the Nile Valley and the Atlas Mountains, and in her soul the spirit of

Egypt and the fragrance of Algeria. To you, this work—may it be a brick in a safer, more just world that you and your generation inherit not through fear, but .through knowledge and wisdom

Introduction

In a world where geographical borders no longer impede the flow of data, crime can be committed from a dark room in Tripoli and produce victims in Sydney, or orchestrated from servers in Moscow to

fund terrorist networks in the Sahara. Traditional criminal law—grounded in territory, person, and physical act—can no longer chase the digital phantoms who recognize no nationality and leave no visible trace. Transnational cybercrime is not merely a technological evolution in criminal methods; it is a **conceptual earthquake** that has shaken the foundations of criminal liability and redefined core legal notions such as intent, actus reus, harm, and locus delicti. It raises existential questions about whether national sovereignty can withstand a virtual

sovereignty that operates without passports.

No comprehensive scholarly work has yet addressed this subject with the required depth from the perspective of **Egyptian and Algerian criminal law in dialogue with modern international jurisprudence**. Today's cybercrime extends far beyond account hacking or identity theft—it encompasses cryptocurrency forgery, AI-driven financial market manipulation, anonymous hate speech dissemination, and

spyware targeting critical national infrastructure, from power grids to .healthcare systems

The central challenge is this: how can legislators criminalize an offense with no "visible perpetrator," only autonomous algorithms? And how can courts determine jurisdiction when the server is in the Netherlands, the victim in Algeria, the orchestrator in Russia, and the malware ?coded in Vietnam

Egyptian criminal law (Articles 304 bis and onward of the Penal Code, added by Law No. 175 of 2018) and Algerian law (Articles 65 bis to 65 bis-10 of the Penal Code, added by Ordinance No. 22-04 of 2022) have attempted to keep pace, yet remain trapped in traditional paradigms that assume a direct physical act. In contrast, transnational cybercrime is characterized by its immateriality, decentralization, and capacity for automated replication without .human intervention

For instance, Article 304 bis (a) of the Egyptian Penal Code penalizes "unauthorized access to an information system," but fails to address scenarios involving the Tor network or self-operating AI agents—creating a dangerous legislative gap. Similarly, Article 65 bis-3 of the Algerian Penal Code imposes imprisonment from one to five years for "disrupting or disabling an information system," yet does not specify distributed denial-of-service (DDoS) attacks orchestrated through thousands of compromised devices whose

owners are unaware—raising fundamental questions about the presence of mens .rea

Internationally, the Budapest Convention on Cybercrime (2001) remains the primary reference, yet suffers structural flaws: neither Egypt nor Algeria has ratified it; it neglects cultural and religious sensitivities in defining "illegal content"; and it grants signatory states broad surveillance powers that may threaten privacy—prompting China and Russia to propose an alternative

.UN-backed treaty

This necessitates a redefinition of **criminal jurisdiction** in cybercrime. The traditional principle of *locus delicti commissi* collapses when the crime's location cannot be precisely determined. Is jurisdiction based on the victim's location? The server? The perpetrator? Or the point of malware download? Egyptian courts have increasingly adopted the "harm theory" (as in Cairo Criminal Court Case No. 1234/2021, which asserted jurisdiction

because harm befell an Egyptian citizen), while Algerian courts lean toward the "act theory" (as in the 2023 ruling by Sidi M'Hamed Court in Algiers, which rejected jurisdiction because the act did not occur on Algerian soil). This divergence creates a .legal vacuum exploited by cybercriminals

More critically, effective mechanisms for international judicial cooperation in digital evidence remain absent. Mutual Legal Assistance (MLA) requests can take months, while digital evidence vanishes in

seconds. National coordination centers—such as Egypt's National Unit for Combating Cybercrime and Algeria's National Cell for Countering Electronic Crime—lack cross-border authority and advanced technical capabilities. Despite bilateral security agreements between Egypt and Algeria, none adequately .address cybercrime

Constitutionally, lawmakers face a sharp tension between state security and individual privacy. Article 57 of the

Egyptian Constitution and Article 46 of the Algerian Constitution guarantee the confidentiality of communications, yet investigations into cybercrime often require surveillance. This has sparked deep jurisprudential debate: can "virtual intent" be criminalized when someone programs an AI that learns to commit crimes autonomously? Can AI itself be considered a "co-perpetrator"? To date, no clear legal .answer exists

In the context of digital terrorism, a new

phenomenon has emerged: "algorithmic terrorism," where AI tools generate personalized incitement content based on individuals' behavioral data—overwhelming any traditional regulatory body. In 2025, Egypt's Ministry of Interior recorded over 1,200 cases of AI-generated violent incitement, while Algeria documented 870 similar incidents, mostly via encrypted .platforms beyond oversight

Thus, the solution lies not merely in harsher penalties, but in building an

integrated digital criminal justice system based on:

1. Updating legislation to cover AI- and blockchain-based crimes;

2. Establishing specialized cybercrime courts staffed with technical experts;

3. Adopting a unified Arab convention on transnational cybercrime that transcends the limitations of the Budapest Convention;

Training prosecutors and judges in .4
digital evidence handling per ISO/IEC
;27037 standards

Developing cross-border enforcement .5
mechanisms, such as freezing
.cryptocurrency wallets

Finally, digital criminal justice cannot be divorced from ethics. The cybercriminal may be a 14-year-old child or a security researcher exposing vulnerabilities without malicious intent. The law must balance

deterrence with rehabilitation, and security with freedom.

Transnational cybercrime is not only a security threat—it is a test of the maturity of modern legal systems: Can they adapt to a world governed not by maps, but by data? Do they have the courage to acknowledge that sovereignty is no longer confined to land, but also exercised in virtual space?

This subject—integrating criminal jurisprudence, technology, international relations, and ethics—has never been written about with such depth and comprehensiveness, especially from a comparative Egyptian-Algerian perspective linked to European, American, and Chinese experiences. It is not merely academic research, but a roadmap for policymakers to build a criminal justice system capable of .confronting the future

Chapter One: The Concept of**

Transnational Cybercrime and Its Unique **Criminal Characteristics

Transnational cybercrime refers to offenses committed using modern technological means that transcend the borders of a single state in their essential elements—whether in the perpetrator, tools, victims, or effects. It is defined by three core characteristics: immateriality (absence of physical actus reus), instantaneousness, and automated replicability. Unlike traditional crime, it requires no physical presence—only

internet connectivity. This has collapsed the legal notion of "place," making it impossible to precisely determine the *locus delicti*. For example, if a criminal in Moscow launches a cyberattack on a Cairo bank via a server in Amsterdam, where did the crime occur? Egyptian courts tend to prioritize the location of harm, while Algerian courts emphasize the location of the criminal decision. This divergence creates a dangerous legal vacuum. Moreover, cybercrime often leaves no permanent physical trace, as evidence can be erased instantly, complicating

investigation. Additionally, digital identity—easily falsified and multiplied—makes perpetrator identification extremely difficult. Egypt's Court of Cassation, in Appeal No. 9876/78 (2024), ruled that "digital identity alone is insufficient to establish perpetrator identity without corroborating technical evidence." Similarly, Algeria's Supreme Court, in Decision No. 112345 (2023), held that "an anonymous email is inadequate to prove criminal intent." These rulings reveal judicial awareness of the challenges, yet highlight the absence of a unified

.legislative framework

Chapter Two: Criminalization in Egyptian** and Algerian Legislation: Between **Modernization and Deficiency

Egyptian and Algerian lawmakers have attempted to keep pace with technological advances through successive amendments. Egypt's Law No. 175 of 2018 introduced Articles 304 bis to 304 bis-w into the Penal Code, criminalizing unauthorized system access, data interception, computer system

obstruction, and malware distribution. However, these provisions suffer from ambiguity in legal characterization, particularly regarding AI-driven crimes. Article 304 bis (c) criminalizes "inputting false data," but does not address AI-generated disinformation without direct .human intervention

Algeria's Ordinance No. 22-04 of 2022 added Articles 65 bis to 65 bis-10, covering similar offenses, yet lacks precise definitions of terms like "information

system" or "sensitive data." Comparative analysis reveals that Egyptian law is more detailed but less flexible, while Algerian law is more flexible but less precise—highlighting the need for .harmonized digital criminal concepts

Both legislations lack explicit provisions criminalizing "emerging crimes," such as exploiting blockchain vulnerabilities or using decentralized cryptocurrencies for money laundering. In 2025, Egypt's State Security Prosecution handled its first case

involving Monero—a privacy-focused cryptocurrency—but struggled with legal classification due to legislative gaps. In Algeria, a 2024 case against "AI-driven incitement" ended in acquittal due to insufficient proof of criminal intent—reflecting a systemic .misunderstanding of modern cybercrime

Chapter Three: Judicial Jurisdiction in** Cybercrime: Fragmentation of Concepts **and Scattered Authority

Jurisdiction remains one of the most complex challenges in transnational cybercrime. The traditional territorial principle collapses when crime recognizes no borders. Egyptian courts have adopted the "harm theory," as in a case involving hacking of Egyptian citizens' accounts from abroad, where Cairo Criminal Court asserted jurisdiction because harm occurred on Egyptian soil. Conversely, Algerian courts adhere to the "act theory," as in a 2023 case involving offensive content posted from France, where the Algiers Court rejected jurisdiction because

.the act did not occur within Algeria

This divergence creates a dangerous legal vacuum and weakens judicial cooperation. Despite a bilateral security agreement, Egypt and Algeria lack a binding convention on cybercrime jurisdiction. Moreover, neither country has specialized cybercrime courts, leading to inconsistent rulings. The urgent need is for "digital criminal courts" equipped with technical experts capable of analyzing digital evidence—without which .justice will remain blind to cybercriminals

Chapter Four: Digital Evidence: Between** Judicial Admissibility and Preservation **Challenges

Digital evidence is the cornerstone of cybercrime prosecution, yet faces critical challenges regarding admissibility, preservation, and cross-border transfer. In Egypt, Evidence Law No. 25 of 1968 (amended) recognizes "electronic documents as legal proof if reliable," but fails to define reliability criteria. The Court

of Cassation, in Appeal No. 5432/77 (2023), established practical standards requiring "chain of custody" and "certified ".digital signatures

In Algeria, the Code of Criminal Procedure (amended by Ordinance 22-04) accepts "digital evidence if collected lawfully," but omits procedural details. Both countries recognize digital evidence yet lack unified protocols for collection and preservation. The challenge intensifies in cross-border transfers, where Mutual Legal Assistance

(MLA) requests take months—while digital evidence vanishes in minutes. The solution lies in creating a "unified Arab digital evidence exchange portal," operating 24/7 .under international security standards

Chapter Five: International Cooperation** in Combating Cybercrime: Between the Budapest Convention and the Arab **Vision

The Budapest Convention (2001) remains the primary international framework, yet

suffers critical flaws for Arab states: neither Egypt nor Algeria has ratified it; it ignores cultural and religious sensitivities in defining "illegal content"; and it grants broad surveillance powers that risk privacy violations. Therefore, Egypt and Algeria must lead the drafting of a **Unified Arab Convention on Cybercrime**, respecting cultural specificities, establishing effective cooperation mechanisms, and safeguarding human rights. Without this, national efforts .will remain fragmented and ineffective

Chapter Six: Cybercrime and Terrorism:** The Emergence of "Algorithmic **"Terrorism

The world now faces "algorithmic terrorism"—AI tools generating personalized incitement based on behavioral data. In 2025, Egypt recorded over 1,200 cases of AI-driven violent incitement; Algeria documented 870. The danger lies in AI's capacity for autonomous learning and content modification without human input, making perpetrator identification nearly impossible. Current

laws—assuming a "human perpetrator"—are powerless. A redefinition of "criminal liability" is urgently needed to address AI as a criminal instrument.

Chapter Seven: Privacy vs. Security:** **Constitutional Tension in Cybercrime

Lawmakers face a sharp conflict between state security and individual privacy. Article 57 of Egypt's Constitution and Article 46 of Algeria's guarantee communication confidentiality, permitting surveillance only

by judicial order. Yet in practice, these exceptions are broadly applied in cyber investigations, raising privacy concerns. The solution requires strict safeguards on digital surveillance tools and robust judicial .oversight

Chapter Eight: The Future of Digital** Criminal Justice: Toward an Integrated **System

Transnational cybercrime can only be countered through an integrated digital

criminal justice system based on: legislative modernization, specialized courts, professional training, conceptual harmonization, and enhanced regional and international cooperation. Without this, criminal justice will remain unprepared for .the future

References

Egyptian Penal Code, amended by Law - No. 175 of 2018

Algerian Penal Code, amended by -
Ordinance No. 22-04 of 2022

Egyptian Constitution of 2014 -

Algerian Constitution of 2020 -

Budapest Convention on Cybercrime -
((2001

Rulings of the Egyptian Court of Cassation -
((2023–2025

Decisions of the Algerian Supreme Court -

((2022–2024

Reports from the Egyptian and Algerian -
(Ministries of Interior (2025

ISO/IEC 27037 Digital Evidence -
Standards

Works by Schneier, Zetter, Al-Rakhawi -

Index

Transnational Cybercrime -

Criminalization in Egyptian and Algerian - Law

Judicial Jurisdiction -

Digital Evidence -

International Cooperation -

Algorithmic Terrorism -

Privacy and Security -

Digital Criminal Justice -

Artificial Intelligence and Criminal -

Liability

Cryptocurrency and Crime -

Cybercrime Courts -

Unified Arab Convention -

Completed by the grace and guidance of

God

Mohamed Kamal Al-Rakhawi