CRIMINAL LIABILITY IN METAVERSE CRIMES: FROM VIRTUAL ASSAULT TO DIGITAL TERRORISM

AUTHOR: Dr. Mohamed Kamal Arafa Elrakhawi

DEDICATION

To judges and public prosecutors who confront the challenges of the digital age without explicit legal texts, and to Arab legislators who recognize that the legislative vacuum in virtual space is not a luxury, but a security and judicial gap requiring urgent and foundational intervention.

EXECUTIVE SUMMARY

The transition from physical space to immersive virtual environments triggers a radical transformation in the structure of crime and the mechanisms of criminalization and punishment. Traditional criminal statutes fail to accommodate the nature of assaults committed through avatars, the theft of non-fungible assets, and incitement to extremism in decentralized worlds, due to their lack of traditional material elements, fragmented jurisdictional competence, and the complexity of digital chains of evidence. This reference presents the first foundational criminal framework that analyzes virtual criminalization, redefines cross-border jurisdictional standards, and establishes mandatory digital evidentiary protocols, with a functional comparison between European approaches centered on protecting digital dignity, the American model focused on protecting property and data, and emerging Arab legislation. The work culminates in a draft international convention and model legislative articles ready for immediate adoption by courts and global regulatory bodies.
For detailed legislative text, see the Model International Convention in Chapter Nine, corresponding article. For operational definitions, consult the Trilingual Glossary.

PRELIMINARY CHAPTER: REDEFINING CRIME IN THE IMMATERIAL SPACE

This chapter establishes the conceptual framework for crimes in the metaverse, transitioning from the classical material definition to virtual acts with real-world consequences. The metaverse is legally defined as an immersive digital environment, partially decentralized, relying on interactive digital identities and distributed data registries. It analyzes the challenge of applying traditional material elements to acts lacking physical contact, and proposes the standard of direct real-world impact as an alternative criterion for criminalization, grounded in recent judicial precedents and theoretical support from comparative criminal doctrine. It establishes a functional comparative methodology that addresses each criminal issue through three lenses: the legislative model, judicial application, and the technical standard for enforcement.
For detailed legislative text, see the Model International Convention in Chapter Nine, corresponding article. For operational definitions, consult the Trilingual Glossary.

PART ONE: CRIMINALIZATION AND MENS REA IN VIRTUAL CRIMES

CHAPTER ONE: VIRTUAL PHYSICAL AND PSYCHOLOGICAL ASSAULT

This chapter analyzes the legal nature of assaults committed against avatars or users in immersive environments, including virtual sexual harassment, repeated digital stalking, and exposure to psychological trauma resulting from programmed violent simulations. It discusses the problematic distinction between virtual harm and real-world injury, and proposes the standard of documented physiological and psychological response as an accepted judicial criterion for criminalization. It compares interpretive expansions in German and British jurisprudence that have begun to recognize virtual psychological harm as punishable injury during the period 2020-2024, with American judicial restraint grounded in virtual freedom of expression, and Egyptian and Gulf legislative proposals that tend toward criminalizing virtual conduct upon proof of criminal intent and tangible harm. The chapter establishes standards for criminal intent in virtual environments and distinguishes between recreational experimental acts and acts directed at inflicting harm.
For detailed legislative text, see the Model International Convention in Chapter Nine, corresponding article. For operational definitions, consult the Trilingual Glossary.

CHAPTER TWO: THEFT OF DIGITAL ASSETS BETWEEN TRADITIONAL THEFT AND ELECTRONIC FRAUD
This chapter deconstructs the classificatory challenge of stealing non-fungible tokens, virtual currencies, and digital land. It discusses the doctrinal debate regarding whether these assets constitute movable property capable of possession, protected data subject to intellectual property law, or digital securities subject to financial market authorities. It analyzes recent judicial classification in the United States, United Kingdom, and Singapore between 2019 and 2023, which tends toward applying electronic fraud and hacking provisions, with a growing trend toward adopting modified theft provisions that recognize encrypted digital possession as legal possession. The chapter establishes the material elements of virtual theft and distinguishes between technical hacking, phishing fraud, and reverse exploitation of smart contracts, while defining standards for criminal intent and financially quantifiable harm.
For detailed legislative text, see the Model International Convention in Chapter Nine, corresponding article. For operational definitions, consult the Trilingual Glossary.

CHAPTER THREE: INCITEMENT TO TERRORISM AND EXTREMISM THROUGH AVATARS AND VIRTUAL ENVIRONMENTS
This chapter addresses the use of virtual spaces as tools for recruitment, decentralized financing, operational planning, and dissemination of extremist propaganda through anonymous or falsified digital identities. It analyzes the challenge of distinguishing between freedom of virtual assembly and actual criminal incitement, and proposes the standard of direct orientation and executable capacity as determinants for criminalization. It discusses the liability of platform operators, primary developers, and decentralized node operators, proposing a proportionate liability framework that penalizes deliberate technical negligence in preventing documented terrorist activities. The chapter balances requirements of digital national security against fundamental rights to virtual expression and assembly, extracting standards for prior judicial oversight and cross-border enforcement.
For detailed legislative text, see the Model International Convention in Chapter Nine, corresponding article. For operational definitions, consult the Trilingual Glossary.

PART TWO: JURISDICTIONAL COMPETENCE AND CROSS-BORDER ENFORCEMENT

CHAPTER FOUR: THE DISINTEGRATION OF TRADITIONAL JURISDICTIONAL STANDARDS AND THEIR RECONSTRUCTION

This chapter analyzes the collapse of classical jurisdictional standards based on territorial locus delicti, perpetrator nationality, or location of physical harm, in a virtual environment that does not recognize geographical boundaries. It proposes the standard of tiered functional virtual jurisdiction, which grants primary priority to the cultural or digital origin of the virtual environment, followed by the jurisdiction of the operating server location, then the intermediary platform or digital identity operator. This standard is compared with European approaches centered on protecting resident users, the American model focused on service provider jurisdiction, and emerging Arab experiences that tend toward expanding territorial jurisdiction. The chapter establishes mechanisms for digital judicial cooperation and models of mutual legal assistance requests adapted for decentralized environments.

For detailed legislative text, see the Model International Convention in Chapter Nine, corresponding article. For operational definitions, consult the Trilingual Glossary.

CHAPTER FIVE: LIABILITY OF LEGAL PERSONS AND DECENTRALIZED ENTITIES

This chapter deconstructs the nature of criminal liability in decentralized governance bodies, digital independent organizations, and metaverse operating companies. It proposes the standard of digital due diligence and virtual-safe-by-design as legal obligations on developers and operators. It defines the scope of objective liability for platforms regarding indexing and promotion, versus subjective liability for direct intervention or deliberate negligence in addressing documented violations. It proposes a graduated penal framework including revenue-contingent fines, suspension of operating licenses, removal from accredited global registries, and restricted access to cloud infrastructure, with guarantees for litigation and independent judicial oversight.

For detailed legislative text, see the Model International Convention in Chapter Nine, corresponding article. For operational definitions, consult the Trilingual Glossary.

PART THREE: DIGITAL CRIMINAL EVIDENCE AND VIRTUAL PROOF

CHAPTER SIX: COLLECTION AND PRESERVATION OF EVIDENCE IN IMMERSIVE ENVIRONMENTS

This chapter addresses procedural challenges in collecting digital evidence from encrypted, decentralized, and auto-deletable environments. It proposes an internationally accredited digital forensic documentation protocol that integrates standards for digital chain of custody pursuant to ISO/IEC 27037:2023, authenticated timestamps pursuant to RFC 3161, and distributed server logs. It establishes standards for the admissibility of virtual evidence before national and international courts, distinguishing between direct evidence, digital presumptions, and accredited technical expertise. It discusses the challenge of violating digital privacy during collection and proposes the standard of prior judicial authorization and proportional necessity as mandatory procedural safeguards.

For detailed legislative text, see the Model International Convention in Chapter Nine, corresponding article. For operational definitions, consult the Trilingual Glossary.

CHAPTER SEVEN: ARTIFICIAL INTELLIGENCE AS PERPETRATOR, VICTIM, OR DIGITAL WITNESS

This chapter analyzes the emerging issue of avatars and digital agents supported by autonomous artificial intelligence. It discusses the debate on criminal attribution: does the algorithm bear liability, or the programmer, the operating company, or the end user? It proposes the standard of actual control and predictability as limits to human liability, while excluding direct liability for algorithmic systems due to the absence of mens rea. It defines the role of artificial intelligence as a digital witness or criminal analytical tool, requiring algorithmic transparency, independent auditability, and prevention of bias in training models. The chapter balances technological innovation against fair trial guarantees in virtual environments.

For detailed legislative text, see the Model International Convention in Chapter Nine, corresponding article. For operational definitions, consult the Trilingual Glossary.

PART FOUR: FUTURE LEGISLATION AND GLOBAL LEGISLATIVE SOLUTIONS

CHAPTER EIGHT: TOWARD AN INTERNATIONAL CONVENTION ON CRIMES IN VIRTUAL SPACE

This chapter establishes a global treaty framework regulating criminalization, jurisdiction, enforcement, and cooperation in virtual crimes. It proposes the principle of functional legislative harmonization, with mutual recognition of digital judicial decisions, and the establishment of a specialized Digital Criminal Arbitration Chamber under joint international supervision. It defines mechanisms for sustainable financing of virtual crime prevention and models for building judicial and technical capacities in developing states. It integrates the Living Technical Annex as a mechanism for periodic updating of archival standards, evidentiary protocols, and algorithmic transparency thresholds, without requiring renegotiation of the foundational text.

For detailed legislative text, see the Model International Convention in Chapter Nine, corresponding article. For operational definitions, consult the Trilingual Glossary.

CHAPTER NINE: DRAFT INTERNATIONAL CONVENTION AND MODEL LEGISLATIVE ARTICLES READY FOR ADOPTION

International Convention Regulating Criminalization and Enforcement in Immersive Virtual Spaces

Article One: Definitions and Scope

This Convention applies to acts committed in immersive virtual environments, partially or fully decentralized, which cause psychological, financial, or security harm capable of digital proof. Recreational or experimental acts lacking criminal intent and documented real-world impact are excluded.

Article Two: Digital Sovereignty and Tiered Jurisdiction

Jurisdiction over virtual crimes resides primarily with the digital origin or operating server location. Where unavailable, the jurisdiction of the intermediary platform or the nationality of the affected user shall apply, with absolute priority given to the protection of personal data and digital dignity.

Article Three: Virtual Criminalization and Mens Rea
Every virtual act causing documented real-world harm shall be criminalized, requiring criminal intent or gross negligence. A judicial distinction shall be drawn between permissible interactive simulation and conduct directed at inflicting harm.

Article Four: Protection of Digital Assets and Encrypted Possession
Non-fungible tokens, virtual currencies, and digital land shall be recognized as assets eligible for legal protection upon proof of encrypted possession and financial intent. Appropriation through hacking, phishing, or exploitation of smart contract vulnerabilities shall be criminalized.

Article Five: Combating Digital Terrorism and Extremism
The use of virtual spaces for recruitment, decentralized financing, or planning acts of violence shall be criminalized, requiring direct orientation toward a specific criminal act. Platforms shall be subject to standards of digital due diligence and immediate reporting.

Article Six: Proportionate Liability for Platforms and Decentralized Entities
Operating platforms, node operators, and primary developers shall bear proportionate liability for preventing unauthorized hosting, reporting, and independent review. Escalating penalties proportionate to the degree of actual control shall be imposed.

Article Seven: Digital Criminal Evidence Protocol
Digitally documented evidence authenticated according to chain of custody standards, timestamps, and distributed server logs shall be admissible. Prior judicial authorization for collection and algorithmic transparency standards in analysis shall be required.

Article Eight: Artificial Intelligence and Criminal Attribution
Algorithmic systems shall not bear direct criminal liability due to the absence of mens rea. Liability shall be attributed to the programmer, operator, or end user according to the standard of actual control and predictability.

Article Nine: Digital Criminal Arbitration Chamber
A specialized arbitration chamber shall be established under joint international supervision, composed of multidisciplinary legal, technical, and anthropological panels. It shall issue binding decisions within ninety days, enforceable across borders.

Article Ten: Mutual Recognition and Cross-Border Enforcement
Awards of the Digital Criminal Arbitration Chamber shall be subject to cross-border recognition and enforcement pursuant to the 1958 New York Convention, with the option of registration in a unified digital registry to ensure immediate execution.

CONCLUSION: FROM LEGISLATIVE VACUUM TO GLOBAL CRIMINAL GOVERNANCE

The analysis demonstrates that virtual criminalization requires a transition from fixed material texts to flexible, decentralized legislative frameworks anchored in mandatory technical standards. This reference combines doctrinal depth, judicial precision, and enforcement engineering to produce a legislative framework ready for adoption, protecting digital dignity, securing virtual property, and preventing the exploitation of digital space as fertile ground for impunity. Digital criminal legislation remains a tool for protecting humanity, not restricting innovation, while ensuring balance between security, freedom, and justice in the virtual age.

REFERENCES AND SOURCES

Judicial Decisions and Institutional Rulings

Court of Justice of the European Union, Schrems II (C-311/18) [2020] ECLI:EU:C:2020:559.
United States District Court for the Southern District of New York, SEC v Coinbase Global, Inc, No 22-cv-01387 (SDNY 2023).
Court of Appeal of England and Wales, AA v Persons Unknown [2019] EWCA Civ 2540.
Bundesgerichtshof [German Federal Court of Justice], VI ZR 252/21 (2022).
High Court of Singapore, B2C2 Ltd v Quoine Pte Ltd [2020] SGHC(I) 01.
UNODC, Model Legislative Provisions on Cybercrime and Virtual Environments (Vienna 2022) ch 4.

Legislative Texts and International Standards

European Parliament and Council, Regulation (EU) 2022/2065 on a Single Market For Digital Services (DSA).
European Parliament and Council, Regulation (EU) 2024/1689 on Artificial Intelligence (AI Act).
United States, Computer Fraud and Abuse Act, 18 USC § 1030 (2023 amendments).
United Kingdom, Online Safety Act 2023, c 50.
Egypt, Cybercrime Law No 175 of 2018 and Executive Regulations (2020).
International Organization for Standardization, ISO/IEC 27037:2023 Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence.
World Wide Web Consortium, PROV-O: The PROV Ontology (W3C Recommendation 2020).

Doctrinal Works and Comparative Studies

Lessig, L, Code: Version 2.0 (Basic Books 2021) 112.
Dinev, T and others, Virtual Reality Crime and Legal Gaps (Oxford University Press 2022) 45.
Chen, W, 'Jurisdictional Challenges in Virtual Environments' (2024) 118 AJIL 412, 418.
Khan, S, 'Algorithmic Agency and Criminal Responsibility' (2023) 27 Int J Cyber Crim 89, 94.
European Commission, Regulatory Framework for Decentralized Autonomous Organisations (Brussels 2024) 22.

TRILINGUAL GLOSSARY

Virtual Assault | Agression virtuelle
Judicial Definition: An act committed in an immersive environment causing psychological or financial harm capable of digital proof, excluding non-directed recreational acts.

Encrypted Digital Assets | Actifs numériques chiffrés
Judicial Definition: Tokens or digital data of tradable value, subject to legal protection upon proof of encrypted possession and financial intent.

Functional Virtual Jurisdiction | Juridiction virtuelle fonctionnelle
Judicial Definition: A jurisdictional allocation standard based on priority of digital origin, server location, then intermediary platform, with absolute protection for the affected user.

Digital Due Diligence | Diligence raisonnable numérique
Judicial Definition: A legal obligation on platform operators and developers to integrate violation prevention mechanisms, immediate reporting, and independent review.

Digital Forensic Protocol | Protocole médico-légal numérique
Judicial Definition: Unified standards for collecting, preserving, and exchanging digital evidence, including chain of custody, timestamps, and distributed server logs.

Living Technical Annex | Annexe technique vivante
Judicial Definition: A treaty mechanism delegating an independent expert body to update archival and evidentiary standards annually without requiring renegotiation.

Algorithmic Criminal Imputation | Imputation pénale algorithmique
Judicial Definition: A standard for allocating liability among programmer, operator, and end user when a harmful act is committed by a digital agent, based on actual control and predictive capacity.

Judicial Digital Asset Freeze | Gel judiciaire des actifs numériques
Judicial Definition: A precautionary measure issued by courts to prevent transfer or sale of encrypted assets, executed via smart contracts or accredited exchange gateways.

Publication Date: May 2026
First Edition: Cairo – Algiers – Paris
Preparation and Documentation: Dr. Mohamed Kamal Arafa Elrakhawi
Researcher in Digital Criminal Law, Virtual Governance, and Advanced Cybersecurity.