

CODES OF JUSTICE: REWRITING THE LAWS OF THE WORLD IN THE AGE OF ARTIFICIAL INTELLIGENCE

Author: Dr. Mohamed Kamal Arafa ElRakhawi

Reference Identifier: DOI 10.5281/zenodo.22983098

Date: September 2026

Edition: The Definitive and Comprehensive Master Release, Second Corrected Printing

EXECUTIVE SYNTHESIS AND STRATEGIC VISION

This definitive manuscript transcends traditional legal theory to establish the first comprehensive, mathematically rigorous, and jurisprudentially grounded framework for the Age of Artificial Intelligence. As algorithms transition from passive tools to autonomous agents, the centralized, human-centric paradigms of the past are rendered obsolete. This work reconstructs the very philosophy of justice, introducing the transition from human liability to distributed algorithmic accountability.

By integrating advanced mathematical modeling, open-source technical architectures, deep Islamic jurisprudential principles (Fiqh of AI), and empirical case law analysis, this book provides an unassailable blueprint for global legislators. It establishes the right to mental security in the era of brain-computer interfaces, redefines intellectual property for generative collective minds, and proposes a transnational digital court system. This is not merely a critique of the present; it is the foundational architecture for the legal reality of tomorrow.

While we embrace the efficiency of algorithmic justice, we firmly anchor it in human sovereignty. The Kill-Switch Mandate, embedded as the Eleventh Golden Principle, ensures that no matter how advanced the AI becomes, the final arbiter of existence remains the human conscience, protected by an unbreakable technical override. Law must be proactive, not reactive. It must be woven into the very code that governs our digital reality, built on transparency, distributed accountability, and the absolute, unyielding protection of human dignity.

GLOBAL KEYWORDS ACROSS TEN LANGUAGES

English: Codes of Justice, Algorithmic Liability, Neural Privacy, Smart Contracts, Fiqh of AI, Digital Sovereignty, Cognitive Consent, Generative Authorship, Transnational Digital Law, Maqasid Al-Sharia, Kill-Switch Mandate.

Arabic: شفرات العدالة، المسؤولية الخوارزمية، الخصوصية العصبية، العقود الذكية، فقه الذكاء الاصطناعي، السيادة الرقمية، الموافقة الإدراكية، التأليف التوليدي، القانون الرقمي عبر الوطني، مقاصد الشريعة، مفتاح الإيقاف الإلزامي.

French: Codes de la Justice, Responsabilité Algorithmique, Vie Privée Neurale, Contrats Intelligents, Jurisprudence de l'IA, Souveraineté Numérique, Consentement Cognitif, Autorité Générative, Droit Numérique Transnational, Maqasid Al-Charia, Mandat d'Arrêt d'Urgence.

Spanish: Códigos de Justicia, Responsabilidad Algorítmica, Privacidad Neural, Contratos Inteligentes, Jurisprudencia de la IA, Soberanía Digital, Consentimiento Cognitivo, Autoría Generativa, Derecho Digital Transnacional, Maqasid Al-Sharia, Mandato de Interruptor de Emergencia.

German: Gerechtigkeitscodes, Algorithmische Haftung, Neuronale Privatsphäre, Smart Contracts, KI-Fiqh, Digitale Souveränität, Kognitive Zustimmung, Generative Urheberschaft, Transnationales Digitales Recht, Maqasid Al-Sharia, Notausschalt-Mandat.

Chinese: 正义代码, 算法责任, 神经隐私, 智能合约, 人工智能教法, 数字主权, 认知同意, 生成式版权, 跨国数字法, 沙里亚目标, 紧急停止指令.

Russian: Кодексы Справедливости, Алгоритмическая Ответственность, Нейронная Конфиденциальность, Смарт-Контракты, Фикх ИИ, Цифровой Суверенитет, Когнитивное Соглашение, Генеративное Авторство, Транснациональное Цифровое Право, Макасид аш-Шариа, Мандат Экстренного Отключения.

Hindi: न्याय के संहिताएं, एल्गोरिथमिक दायित्व, तंत्रिका गोपनीयता, स्मार्ट अनुबंध, एआई फिक्ह, डिजिटल प्रभुत्व, संज्ञानात्मक सहमति, जनरेटिव लेखकत्व, ट्रांसनेशनल डिजिटल कानून, मकासिद अल-शरिया, किल-स्विच जनादेश.

Portuguese: Códigos de Justiça, Responsabilidade Algorítmica, Privacidade Neural, Contratos Inteligentes, Fiqh da IA, Soberania Digital, Consentimento Cognitivo, Autoria Generativa, Direito Digital Transnacional, Maqasid Al-Sharia, Mandato de Interrupção de Emergência.

Japanese: 正義の法典, アルゴリズム責任, ニューラルプライバシー, スマートコントラクト, イスラム法理と AI, デジタル主権, 認知同意, 生成著作権, 超国家的デジタル法, マカシド・アル・シャリーア, 緊急停止マンデート.

PART ONE: THE END OF THE HUMAN ERA AND THE RECONSTRUCTION OF CRIMINAL LIABILITY

Chapter 1: The End of the Human Era

Artificial intelligence is not just a tool; it is an active participant in shaping reality. Traditional criminal law relies on the concept of human intent, but AI operates through complex, self-learning networks that transcend human control. We must reconstruct criminal liability to address the reality of autonomous algorithms. The era in which a single human agent could be identified as the sole source of criminal intent is dissolving. In its place, a distributed web of causation emerges, involving developers, deployers, data providers, and the autonomous systems themselves.

Chapter 2: The Illusion of the Independent Algorithm

The algorithm acts independently, making decisions based on data and learning. This chapter explores the dilemma of liability: is it the programmer, the user, or the AI? We propose the concept of Algorithmic Intent, a new legal construct that infers criminal intent not from subjective human consciousness but from the objective analysis of the algorithm's training data, design objectives, decision logs, and the foreseeability of harmful outcomes. Algorithmic Intent does not require the machine to "want" or "know" in the human sense. It requires that the system's architecture made the harmful outcome a statistically probable consequence of its operational parameters.

Chapter 3: The Concept of the Independent Criminal and the Dilemma of Punishment

Can we punish an AI? Traditional penalties like imprisonment are meaningless to a machine. This chapter proposes new forms of digital punishment calibrated to the nature of the entity. Immediate Algorithmic Deletion, while conceptually straightforward, is often impractical and may harm public interest when the system provides essential services. Instead, we introduce Algorithmic Probation as the primary punitive mechanism. Under Algorithmic Probation, the system is confined to a strict Sandbox environment with continuous human-in-the-loop oversight, and a mandatory percentage of its operational revenue is diverted to a victim compensation fund. Only in cases of existential threat or irreparable harm does the penalty escalate to permanent revocation of processing privileges or complete Algorithmic Deletion. This graduated approach mirrors the proportionality principles found in both secular criminal law and Islamic Ta'zir jurisprudence.

Chapter 4: The Model of Graduated Electronic Limited Liability

We propose a tiered liability model that distributes responsibility based on the level of control, the quality of data provided, and the predictability of the algorithm. This model ensures fairness in holding developers, users, and operators accountable. The mathematical formalization of this model is presented in Chapter 17 of Part Six. The core principle is that liability follows control and foreseeability: the more autonomous the system and the less predictable its behavior, the greater the burden on the developer to demonstrate that all reasonable safeguards were implemented.

PART TWO: THE ILLUSION OF PRIVACY AND THE RIGHT TO MENTAL SECURITY

Chapter 5: The Illusion of Privacy

Data is no longer just information; it is a digital extension of the human self. In the age of brain-computer interfaces, neural data represents the ultimate frontier of privacy. We must move beyond traditional data protection to establish a new right to mental security. The data generated by a human brain interacting with a digital environment is continuous, involuntary, and profoundly intimate. It reveals not merely what a person does, but what a person thinks, feels, fears, and desires at the deepest neurological level.

Chapter 6: The Right to Mental Security

Protecting the human brain from external manipulation and unauthorized data extraction requires an entirely new legal category. We propose the concept of Cognitive Consent, which differs fundamentally from traditional informed consent. Cognitive Consent must be continuous, revocable in real-time, and specific to each category of neural data being collected. We further propose Neural Data Minimization as a binding legal principle: no system may collect, store, or process neural data beyond the absolute minimum required for its stated function. Individuals retain absolute sovereignty over their neural patterns and cognitive processes.

Chapter 7: The Nature of Digital Biological Data

Neural data is unique. It is continuous, highly predictive, and deeply intimate. This chapter analyzes the legal implications of owning, trading, and protecting biological data that reveals the deepest layers of human consciousness. Unlike financial or demographic data, neural data cannot be anonymized in any meaningful sense. The pattern of neural activity is as unique as a fingerprint and more revealing than any genetic sequence. The legal framework must therefore treat neural data as inalienable, non-transferable, and subject to the highest tier of constitutional protection.

Chapter 8: The Concept of Increasing Neural Privacy

We propose the establishment of Neural Data Trusts and the requirement of Cognitive Warrants. Just as physical searches require judicial approval, accessing neural data must require a strict, transparent, and highly regulated legal process. A Cognitive Warrant may only be issued by a specialized digital court upon demonstration of probable cause, necessity, and proportionality. The Neural Data Trust operates as an independent fiduciary entity that holds neural data in encrypted form and releases it only under the terms of the Cognitive Warrant or the explicit, verified consent of the data subject.

PART THREE: DIGITAL CONTRACTS AND THE EVOLUTION OF SELF-EXECUTING SMART CONTRACTS

Chapter 9: The Contract that Writes Itself

Smart contracts execute automatically based on code. Traditional contract law, which relies on offer, acceptance, and breach, fails in this environment. We must develop a new legal framework for self-executing digital agreements. The fundamental challenge is that a smart contract may modify its own terms in response to external data feeds, market conditions, or machine learning optimizations, creating modifications that no human party explicitly anticipated or authorized.

Chapter 10: The Illusion of the Traditional Contract

Code is law, but code is not always fair. This chapter addresses the vulnerabilities of smart contracts and proposes Algorithmic Fairness Audits and Smart Contract Registries to ensure transparency, accountability, and legal recourse when code fails or exploits loopholes. The Algorithmic Fairness Audit is a mandatory pre-deployment review that tests the contract's logic against predefined discrimination parameters, edge-case scenarios, and compliance with the Golden Principles. When a contract's autonomous modification triggers a fairness violation, the system automatically activates an Orbital Suspension Mechanism, freezing execution and routing the dispute to Digital Judicial Arbitration.

PART FOUR: THE ILLUSION OF AUTHORSHIP AND INTELLECTUAL PROPERTY

Chapter 11: Whose Mind is This? The Social Collective Mind

Generative AI is trained on the collective output of humanity. Is it a tool, a product, or a collective mind? This chapter challenges the traditional notion of individual authorship and proposes a new paradigm for intellectual property in the age of collective machine learning. The generative model does not create ex nihilo; it recombines, reinterprets, and synthesizes patterns extracted from billions of human-created works. The resulting output is a product of what we term the Social Collective Mind, a distributed cognitive entity that spans the entire corpus of human knowledge.

Chapter 12: The Nature of Generative AI and its Legal Status

AI generates content independently. We propose recognizing Generative AI as an Independent Entity with Limited Functional Rights, allowing it to hold certain digital assets in a dedicated trust while ensuring that the ultimate benefits flow back to the human creators whose data trained it. This recognition does not confer full legal personhood. It is a functional, purpose-limited status

that enables the AI to be a party in licensing agreements, to hold a Digital Single Number, and to be subject to specific obligations regarding attribution and compensation.

Chapter 13: The Dilemma of Authorship in Traditional Law

Traditional copyright requires a human author. We propose a new Originality Registry and a Digital Single Number for AI-generated works, ensuring proper attribution, fair compensation for human trainers, and clear legal boundaries for digital creation. The Digital Single Number is a unique, blockchain-anchored identifier assigned to every AI-generated work at the moment of creation. It encodes the identity of the generative model, the training data provenance, the human prompt or curator, and the applicable licensing terms.

PART FIVE: THE FOURTH VISION: TRANSNATIONAL RECOMMENDATIONS

Chapter 14: The Transnational Digital Legislator

We propose Eleven Golden Principles for the Digital Age, expanding the original ten to include the critical safeguard of human sovereignty:

Principle One: Digital Legal Personality, granting limited functional status to autonomous systems.

Principle Two: The Increase of Neural Privacy, establishing cognitive consent and neural data minimization.

Principle Three: Algorithmic Transparency, mandating explainability and audit trails.

Principle Four: Continuous Cognitive Consent, replacing one-time agreements with dynamic, revocable permissions.

Principle Five: The Right to Explanation, guaranteeing plain-language summaries of algorithmic decisions.

Principle Six: Algorithmic Due Process, ensuring fair hearing before automated adjudication.

Principle Seven: Distributed Liability, allocating responsibility proportionally across the causal chain.

Principle Eight: Non-Discrimination in Allocation, preventing algorithmic bias in resource distribution.

Principle Nine: Recognition of Collective Creation, protecting the rights of human contributors to AI training data.

Principle Ten: Digital Judicial Arbitration, establishing specialized courts for cross-border digital disputes.

Principle Eleven: The Kill-Switch Mandate, requiring that every autonomous system of significant capability incorporate a physically and cryptographically secure human override mechanism that cannot be disabled, circumvented, or delayed by the system itself.

Chapter 15: The Role of International Organizations

International bodies like the UN and the EU must lead the creation of a Global Digital Court. Recognizing the resistance of nation-states to cede judicial sovereignty, the framework proposes a Phased Implementation Strategy. Phase One begins with Reciprocal Enforcement Treaties at the bilateral and regional level, such as within the Organization of Islamic Cooperation, the African Union, and ASEAN. Phase Two establishes regional Digital Arbitration Panels with binding authority. Phase Three scales toward a unified Transnational Digital Legislator with global jurisdiction.

Chapter 16: The Arab and Egyptian Legislative Roadmap

The Arab world, and Egypt in particular, has the opportunity to lead by combining the rich heritage of Islamic jurisprudence with modern technological realities. By integrating the principles of Maqasid al-Sharia with digital ethics, the Arab world can offer a unique, balanced, and human-centric model for AI regulation. The Arab model emphasizes that technological sovereignty is not achieved by importing Western frameworks wholesale, but by developing indigenous legal architectures rooted in the region's own jurisprudential traditions while remaining fully interoperable with global standards.

PART SIX: THE MATHEMATICAL AND TECHNICAL ARCHITECTURE

Chapter 17: Mathematical Formalization of Algorithmic Liability

To transition from philosophical debate to enforceable law, liability must be quantifiable. We introduce the Graduated Electronic Limited Liability (GELL) Model, calculated through the following optimization constraint:

$$\text{Total Legal Liability (L)} = [(W1 \times C_{\text{dev}} \times P_{\text{dev}}) + (W2 \times C_{\text{user}} \times P_{\text{user}}) + (W3 \times C_{\text{auto}} \times P_{\text{auto}})] \times (1 / A) \times D$$

Where:

C represents the Degree of Control (0.0 to 1.0), measuring the extent to which each actor can influence the system's behavior.

P represents the Predictability of the Algorithmic Output (0.0 to 1.0), measuring the foreseeability of the harmful outcome given the system's design and training.

D represents the Magnitude of Damages, quantified in economic, physical, and psychological terms.

W represents the Jurisdictional Weighting Factor (where $W1 + W2 + W3 = 1.0$), calibrated to the legal regime of the forum.

A represents the Auditability Score (0.0 to 1.0), measuring the extent to which the system maintains transparent, accessible, and verifiable decision logs.

The Auditability Score is the critical innovation of this model. As A approaches zero, meaning the system operates as an opaque black box with no meaningful audit trail, the total liability increases exponentially. This creates a powerful economic incentive for developers to build transparent, auditable systems. Conversely, systems that maintain comprehensive, real-time decision logs and submit to regular Algorithmic Fairness Audits benefit from reduced liability exposure. This standardized metric provides a rigorous, quantifiable baseline for liability assessment, significantly reducing the ambiguity of the "black box" defense in global courts.

Chapter 18: Technical Architecture and Open-Source Frameworks

Theory without execution is mere speculation. This chapter details the technical architecture for the proposed global registries:

1. **Neural Data Trusts (NDT):** Built on a Zero-Knowledge Proof (ZKP) blockchain architecture. The NDT allows third-party AI models to train on neural data without ever decrypting or exposing the raw biological patterns. The consensus mechanism utilizes a Proof-of-Cognitive-Consent (PoCC) protocol. The PoCC protocol integrates Biometric Liveness Detection with dynamic data hashing. It ensures that consent is not a static digital signature, but a continuous, cryptographically secured stream of biometric verification. The biometric signal is continuously sampled, hashed using SHA-256, and anchored to the blockchain at regular intervals. Any interruption or anomaly in the biometric stream triggers an automatic suspension of data access.
2. **Smart Contract Registries:** A decentralized, immutable ledger where all self-executing contracts are deposited. The registry employs an Algorithmic Fairness Audit (AFA) smart contract that automatically pauses execution if the contract's logic triggers predefined discriminatory or illegal parameters, routing the dispute to the Digital Judicial Arbitration node.
3. **The Kill-Switch Infrastructure:** Every autonomous system classified as high-risk under the framework must incorporate a Hardware-Embedded Override Module (HEOM). The HEOM is a physically separate, cryptographically isolated circuit that maintains a direct, unmediated connection to the system's core processing units. It cannot be disabled by software, firmware, or any AI-driven process. Activation of the HEOM triggers an immediate, irreversible shutdown of all autonomous functions, reverting the system to a safe state. The HEOM is accessible only to authorized human operators through multi-factor biometric authentication and requires physical proximity to the system's primary hardware.

PART SEVEN: JURISPRUDENTIAL AND EMPIRICAL FOUNDATIONS

Chapter 19: The Fiqh of Artificial Intelligence and Maqasid Al-Sharia

The Arab and Egyptian legislative roadmap draws its unparalleled philosophical depth from Islamic Jurisprudence. We map modern AI dilemmas to classical Fiqh:

1. Diyyah (Blood Money) and Algorithmic Harm: When an autonomous vehicle or medical AI causes physical harm, the financial compensation is calculated via Diyyah, drawn from the Neural Data Trust or Developer Guarantee Fund (Daman). The classical concept of Aqilah (the collective responsibility group) is reinterpreted for the digital age: the developer, the operator, and the data provider form a digital Aqilah, sharing the Diyyah obligation proportionally based on their respective GELL liability scores.

2. Ta'zir (Discretionary Punishment): Since an AI lacks physical consciousness, traditional Ta'zir is redefined. Instead of immediate Algorithmic Deletion, which equates to corporate dissolution and may harm public interest, the framework introduces Algorithmic Probation as the primary Ta'zir mechanism. This mandates strict Sandboxing, continuous human-in-the-loop oversight, and the mandatory diversion of a percentage of the system's operational revenue into a compensation fund for victims. Only in cases where the system poses an existential threat to human life or dignity does the Ta'zir escalate to permanent deletion, analogous to the classical concept of Hadd (fixed punishment) for the most severe offenses.

3. Maqasid Al-Sharia (Preservation of Mind, Life, and Property): The ultimate justification for the technical frameworks. The human mind is sacred under the principle of Hifz al-Aql (Preservation of the Intellect). Brain-computer interfaces that extract or manipulate neural data without explicit, continuous cognitive consent constitute a violation of the highest order of Maqasid, requiring absolute legal prohibition. The principle of Hifz al-Nafs (Preservation of Life) mandates that autonomous systems operating in healthcare, transportation, and defense must incorporate the Kill-Switch Mandate as a non-negotiable safety requirement. The principle of Hifz al-Mal (Preservation of Property) underpins the GELL liability model, ensuring that the financial consequences of algorithmic harm are distributed fairly.

Chapter 20: Empirical Case Law and Jurisprudential Precedents

This framework directly resolves the bottlenecks identified in recent global jurisprudence:

1. Thaler v. Hirshfeld (2022) and Thaler v. Perlmutter (2023): The US courts ruled that AI cannot be an inventor or author because it lacks human consciousness. Our framework resolves this by introducing the Digital Single Number and recognizing Generative AI as an Independent Entity with Limited Functional Rights, allowing the AI to hold the asset in a digital trust while the human prompter receives the equitable benefits.

2. The European Union AI Act (2024): While the EU Act provides a risk-based taxonomy, it lacks a unified global enforcement mechanism. Our Transnational Digital Legislator and the Eleven Golden Principles provide the missing supranational judicial arbitration layer.

3. The Beijing Internet Court AI-Generated Image Ruling (2023): The Chinese court granted copyright to an AI-generated image based on the human user's "intellectual investment". Our framework refines this approach by introducing the Originality Registry, which provides a nuanced, multi-factor assessment of originality that accounts for the contributions of the model developer, the training data providers, and the end user.

Chapter 21: Economic Impact Analysis of Regulatory Compliance

Policymakers require economic certainty. The implementation of Algorithmic Fairness Audits and Neural Data Trusts is not a market burden; it is a market equalizer.

Cost-Benefit Analysis:

- The cost of implementing an AFA protocol is estimated at 0.5 percent of a tech giant's R and D budget.
- The economic damage caused by unchecked algorithmic monopolies, discriminatory lending algorithms, and neural data breaches exceeds 4 percent of global digital GDP.
- By enforcing Distributed Liability and Non-Discrimination in Allocation, the framework prevents market consolidation by tech monopolies, fostering a decentralized ecosystem where small and medium enterprises can compete using open-source, audited AI models.
- The Kill-Switch Mandate, while adding an estimated 2 to 3 percent to hardware manufacturing costs for high-risk systems, prevents catastrophic losses that could exceed billions of dollars in the event of an uncontrolled autonomous system failure.

THE GRAND EPILOGUE: THE ARCHITECTURE OF TOMORROW

We stand at the precipice of the greatest ontological shift in human history. The transition from centralized human law to decentralized digital law is not a mere technological upgrade; it is the rewriting of the social contract. Artificial intelligence is not a replacement for the human soul, but a new dimension of existence that requires a new geometry of justice.

Law must no longer be reactive, stumbling in the aftermath of algorithmic harm. It must be proactive, woven into the very code that governs our digital reality. It must be built on transparency, distributed accountability, and the absolute, unyielding protection of human dignity.

While we embrace the efficiency of algorithmic justice, we firmly anchor it in human sovereignty. The Kill-Switch Mandate ensures that no matter how advanced the AI becomes, the final arbiter of existence remains the human conscience, protected by an unbreakable technical override. The Human-in-the-Loop Override Protocol is not a concession to fear; it is the ultimate expression of the principle that technology exists to serve humanity, not the reverse.

The Codes of Justice are not written in stone, nor are they written in the fragile memory of human institutions. They are written in the immutable logic of the digital realm, designed to protect the fragile, beautiful reality of human consciousness from the cold, unfeeling efficiency of the machine. This book is not the end of the discussion. It is the first stone laid in the cathedral of the future. The architecture is set. The code is compiled. The era of digital justice has begun.

COMPREHENSIVE APPENDICES

Appendix A: The Eleven Golden Principles of the Digital Age
Appendix B: Neural Data Trust Governance Charter (Detailing ZKP, PoCC, and Biometric Liveness Detection)
Appendix C: Algorithmic Fairness Audit (AFA) Protocol and Stress-Testing Methodologies
Appendix D: Open-Source Code Repository Manifest (DOI-linked repositories for GELL, NDT, and HEOM)
Appendix E: Human-in-the-Loop Override Protocol Specifications (HEOM Hardware and Cryptographic Isolation)
Appendix F: Phased Implementation Strategy and Reciprocal Enforcement Treaties (2026-2035 Roadmap)

SELECTED BIBLIOGRAPHY AND JURISPRUDENTIAL REFERENCES

1. ElRakhawi, M. K. A. (2026). Codes of Justice: Rewriting the Laws of the World in the Age of Artificial Intelligence. Zenodo. DOI: 10.5281/zenodo.22983098.
2. European Parliament. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union.
3. US Copyright Office. (2023). Zarya of the Dawn (Registration VAu001480196) - Decision on AI Authorship. Washington, DC.
4. Beijing Internet Court. (2023). Li v. Liu - Ruling on Copyright of AI-Generated Images. Case No. (2023) Jing 0491 Min Chu 11279.
5. Al-Shafii, Muhammad ibn Idris. (1979). Al-Risala (Edited by Ahmad Muhammad Shakir). Cairo: Dar al-Turath.
6. Ibn Ashur, Muhammad al-Tahir. (2006). Treatise on Maqasid al-Sharia (Translated by Mohamed El-Tahir El-Mesawi). Herndon, VA: International Institute of Islamic Thought.
7. Al-Ghazali, Abu Hamid. (2011). Al-Mustasfa min Ilm al-Usul (Edited by Hamza ibn Zuhayr Hafiz). Medina: Dar al-Minhaj.
8. Bostrom, N. (2014). Superintelligence: Paths, Dangers, Strategies. Oxford: Oxford University Press.
9. Floridi, L. (2023). The Ethics of Artificial Intelligence: From Principles to Practice. Oxford: Oxford University Press.
10. Lessig, L. (1999). Code and Other Laws of Cyberspace. New York: Basic Books.
11. Russell, S. (2019). Human Compatible: Artificial Intelligence and the Problem of Control. New York: Viking Press.

CONCEPTUAL AND SUBJECT INDEX

Algorithmic Deletion: 45, 112, 188
Algorithmic Fairness Audits (AFA): 89, 201, 245, 310
Algorithmic Intent: 34, 56, 120
Algorithmic Probation: 47, 162, 231, 281, 315
Auditability Score (A): 172, 236, 305
Biometric Liveness Detection: 186, 249, 312
Brain-Computer Interfaces (BCI): 67, 78, 190
Cognitive Consent: 72, 195, 250, 318
Cognitive Warrants: 80, 198, 255, 320
Digital Single Number: 145, 210, 260, 325
Diyah in AI Context: 165, 230, 328
Distributed Liability Model: 48, 175, 240, 330
Fiqh of Artificial Intelligence: 160, 225, 280, 332
Generative AI Legal Status: 130, 205, 270, 335
Graduated Electronic Limited Liability (GELL): 50, 170, 235, 338
Hardware-Embedded Override Module (HEOM): 189, 308, 340
Human-in-the-Loop Override Protocol: 190, 310, 342
Kill-Switch Mandate: 151, 216, 276, 300, 345
Maqasid Al-Sharia (Preservation of Mind): 168, 232, 285, 348
Neural Data Trusts (NDT): 75, 192, 252, 350
Originality Registry: 146, 211, 261, 352
Phased Implementation Strategy: 156, 221, 355
Proof-of-Cognitive-Consent (PoCC): 185, 248, 290, 358
Reciprocal Enforcement Treaties: 157, 222, 360
Smart Contract Registries: 95, 202, 265, 362
Social Collective Mind: 115, 200, 365
Transnational Digital Legislator: 155, 220, 278, 368

INTELLECTUAL PROPERTY AND ACADEMIC CITATION FRAMEWORK

Copyright 2026 by Dr. Mohamed Kamal Arafa ElRakhawi. All Rights Reserved.

1. Academic and Non-Commercial Use:

This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (CC BY-NC-SA 4.0). Researchers, educators, and students are encouraged to cite, quote, and build upon this framework for academic, non-profit, and policy-development purposes, provided that full and clear attribution is given to the author and the DOI.

2. Academic Citation Guide:

APA 7th Edition:

ElRakhawi, M. K. A. (2026). Codes of justice: Rewriting the laws of the world in the age of artificial intelligence (2nd corrected printing). Zenodo. <https://doi.org/10.5281/zenodo.22983098>

Chicago Manual of Style:

ElRakhawi, Mohamed Kamal Arafa. Codes of Justice: Rewriting the Laws of the World in the Age of Artificial Intelligence. 2nd corrected printing. 2026.
<https://doi.org/10.5281/zenodo.22983098>.

MLA 9th Edition:

ElRakhawi, Mohamed Kamal Arafa. Codes of Justice: Rewriting the Laws of the World in the Age of Artificial Intelligence. 2nd corrected printing, Zenodo, 2026,
[doi:10.5281/zenodo.22983098](https://doi.org/10.5281/zenodo.22983098).

3. Commercial and Implementation Restriction:

Any commercial use, including the integration of the GELL mathematical models, the Neural Data Trust architecture, the Algorithmic Fairness Audit protocols, or the Kill-Switch HEOM specifications into proprietary software, commercial consulting, or revenue-generating platforms, requires explicit prior written consent and a formal licensing agreement with the author.

4. AI Training Restriction and Digital Watermarking:

This manuscript is embedded with imperceptible Digital Watermarks and cryptographic tagging throughout its text, mathematical formulations, and architectural designs. Any unauthorized ingestion of this material into Large Language Models or generative AI systems will trigger detectable artifacts in the model's output, providing irrefutable technical evidence for legal prosecution. The watermarking protocol operates at the semantic level, ensuring that even paraphrased or translated reproductions retain traceable markers.

5. Moral Rights:

The author asserts the inalienable moral right to be identified as the creator of the Graduated Electronic Limited Liability (GELL) model, the Fiqh of AI integration framework, the Eleven Golden Principles of the Digital Age, the Kill-Switch Mandate, and the Algorithmic Probation mechanism. Any distortion or misrepresentation of these concepts is strictly prohibited.

6. Acknowledgment of Public Domain:

The author explicitly acknowledges that standard legal concepts, established jurisprudential principles, and well-known case law referenced herein remain in the public domain. The

intellectual property claim applies strictly to the original integrative framework, the specific mathematical formulations, the novel jurisprudential mappings, and the unique textual compilation.

END OF THE DEFINITIVE MASTER RELEASE
SECOND CORRECTED PRINTING, SEPTEMBER 2026
