

EL-RAKHAWI DOCTRINE

THE GLOBAL ENCYCLOPEDIA OF CYBERCRIMES AND

COMPARATIVE DIGITAL LAW

A COMPREHENSIVE JURISPRUDENTIAL FRAMEWORK ACROSS THE AMERICAS, EUROPE, ASIA, AFRICA, AND THE GULF

DR. MOHAMED KAMAL ARAFA ELRAKHAWI

DOI: 10.5281/zenodo.22908154

Date: September 2026

FOREWORD AND PREFACE

This encyclopedia represents a paradigm shift in the understanding and application of digital law. It is founded upon the "Elrakhawi Doctrine," a pioneering jurisprudential framework that asserts three core principles: First, Digital Sovereignty must be balanced with Global Interoperability, meaning nations must protect their digital borders without fracturing the global internet. Second, the Harmonization of Legal Traditions is essential; the strict liability of Gulf and Asian systems must be dialogued with the intent-based requirements of European civil law and the procedural pragmatism of American common law. Third, Proactive Algorithmic Accountability dictates that the deployment of autonomous AI agents in cyberspace requires a shift from reactive punishment to preventive, mathematically verifiable compliance.

This work is designed to serve as the definitive global reference for prosecutors, defense counsel, compliance officers, and academics navigating the complex, borderless landscape of modern cybercrime.

ABOUT THE AUTHOR

Dr. Mohamed Kamal Arafa Elrakhawi is an independent international researcher specializing in Jurisprudence, Philosophy of Law, Biophysics, Neuroengineering, and Cosmic Justice. Based in Ismailia, Arab Republic of Egypt, Dr. Elrakhawi's work bridges the gap between advanced technological systems and robust legal frameworks. His research focuses on creating actionable, globally harmonized legal standards for emerging technologies, ensuring that innovation serves human dignity, security, and equitable access to justice.

TABLE OF CONTENTS

VOLUME ONE: GENERAL PRINCIPLES AND DIGITAL LIABILITY

Chapter 1: The Principle of Legality in Cybercrime and the Elrakhawi Doctrine

Chapter 2: Material and Moral Elements in Digital Crimes: The Role of AI

Chapter 3: Cross-Border Judicial Jurisdiction: Long-Arm Statutes and Digital Sovereignty

Chapter 4: Digital Evidence and Its Probative Value: Global Admissibility Standards

VOLUME TWO: CRIMES AGAINST SYSTEMS AND DATA

- Chapter 1: Unauthorized Access and Persistence in Information Systems
- Chapter 2: Interception, Alteration, and Destruction of Data
- Chapter 3: Creation and Distribution of Malicious Software: The Ransomware Epidemic
- Chapter 4: AI Crimes and the EU AI Act: Autonomous Agents in Hacking

VOLUME THREE: CONTENT AND DIGITAL IDENTITY CRIMES

- Chapter 1: Electronic Fraud and Identity Theft
- Chapter 2: Electronic Defamation and Extortion
- Chapter 3: Digital Sexual Crimes: Deepfakes and Revenge Porn
- Chapter 4: Personal Data Protection: GDPR, LGPD, and Global Frameworks

VOLUME FOUR: ECONOMIC AND FINANCIAL CYBERCRIMES

- Chapter 1: Money Laundering via Cryptocurrencies and Central Bank Digital Currencies (CBDCs)
- Chapter 2: Fraud in Cryptocurrencies and NFTs
- Chapter 3: Attacks on Critical Infrastructure
- Chapter 4: Criminal Liability of Corporations and Executives: Statute of Limitations and Compliance

VOLUME FIVE: PROCEDURES AND INTERNATIONAL COOPERATION

- Chapter 1: Digital Investigation and Evidence Seizure
- Chapter 2: International Judicial Cooperation: MLATs and Joint Investigation Teams (JITs)
- Chapter 3: Extradition of Offenders in Cybercrimes
- Chapter 4: Practical Templates and Cross-Border Legal Gap Analysis

LIST OF ABBREVIATIONS

- AI: Artificial Intelligence
- AMLD6: Sixth Anti-Money Laundering Directive (EU)
- CBDC: Central Bank Digital Currency
- CFAA: Computer Fraud and Abuse Act (US)
- CNIL: Commission Nationale de l'Informatique et des Libertés (France)
- ECPA: Electronic Communications Privacy Act (US)
- GDPR: General Data Protection Regulation (EU)
- JIT: Joint Investigation Team
- LGPD: Lei Geral de Proteção de Dados (Brazil)
- MLAT: Mutual Legal Assistance Treaty
- NIS2: Network and Information Security 2 Directive (EU)
- OFAC: Office of Foreign Assets Control (US)
- POPIA: Protection of Personal Information Act (South Africa)
- StGB: Strafgesetzbuch (German Criminal Code)
- VASP: Virtual Asset Service Provider

TABLE OF LEGISLATION (SELECTED)

United States: Computer Fraud and Abuse Act (18 USC 1030); Electronic Communications Privacy Act; Cyber Incident Reporting for Critical Infrastructure Act (2025).
European Union: General Data Protection Regulation (2016); NIS2 Directive (2024); Markets in Crypto-Assets Regulation (2023); EU AI Act (2024).
France: Penal Code Articles 323-1 to 323-7; Data Protection Act.
Germany: Criminal Code (StGB) Sections 202a, 202c, 303a.
Brazil: Marco Civil da Internet (Law 12.965/2014); Penal Code Article 154-A; LGPD.
Saudi Arabia: Royal Decree M/17 on Combatting Cybercrimes (2007, updated); Royal Decree M/19 on Personal Data Protection (2021).
United Arab Emirates: Federal Law 34/2021 on Combatting Rumours and Cybercrimes.
Egypt: Law 175/2018 on Combatting Information Technology Crimes.
Morocco: Law 07-03 on the Protection of Personal Data; Penal Code amendments.
Algeria: Penal Code provisions on cybercrimes.
Tunisia: Organic Law 2022-54 on Combatting Cybercrimes.

TABLE OF CASES (SELECTED)

United States: *Van Buren v. United States*, 141 S. Ct. 1648 (2021).
France: Cour de cassation, Criminal Chamber, 17 October 2018 (Unauthorized access via found credentials); Cour de cassation, 22 March 2023 (AI-generated exploit code).
Germany: Federal Court of Justice (BGH), rulings on effective security measures under StGB 202a.
Italy: Corte di Cassazione, rulings on Article 635-ter (Data alteration).

VOLUME ONE: GENERAL PRINCIPLES AND DIGITAL LIABILITY

CHAPTER ONE: THE PRINCIPLE OF LEGALITY IN CYBERCRIME AND THE ELRAKHAWI DOCTRINE

The principle of legality, *nullum crimen sine lege*, requires that criminal offenses be clearly defined by statute. The Elrakhawi Doctrine posits that in the digital realm, this principle must evolve to address "technological ambiguity," ensuring that laws are drafted with sufficient technical precision to avoid overcriminalizing legitimate security research while maintaining broad enough scope to cover novel attack vectors.

In the United States, the Computer Fraud and Abuse Act (CFAA) criminalizes unauthorized access. The US Supreme Court's 2021 decision in *Van Buren v. United States* narrowed the scope of "exceeds authorized access," holding that it applies only to those who obtain information from areas of a computer they have no legitimate right to access, rejecting broader "purpose-based" interpretations. This contrasts with France's Penal Code Article 323-1, which requires proof of fraudulent intent but interprets "automated system" broadly.

In Saudi Arabia, Royal Decree M/17 on Combatting Cybercrimes (distinct from M/19, which governs Personal Data Protection) criminalizes unauthorized access, requiring proof that the access was "without legitimate justification," permitting affirmative defenses like authorized security testing. Egypt's Law 175/2018 imposes severe penalties for accessing state infrastructure, reflecting a strong deterrence model.

CHAPTER TWO: MATERIAL AND MORAL ELEMENTS IN DIGITAL CRIMES

The attribution of criminal liability for acts facilitated by artificial intelligence challenges traditional mens rea doctrines. The 2024 EU AI Act establishes a risk-based framework, classifying certain AI systems used in law enforcement or critical infrastructure as "high-risk," mandating strict human oversight and logging to establish a clear chain of accountability.

In the US, the 2026 Executive Order on AI Cybersecurity suggests that developers deploying autonomous agents with known, unmitigated vulnerabilities may face liability under the CFAA if recklessness is proven. French jurisprudence (Cour de cassation, 2023) holds that using AI to overcome technical barriers constitutes evidence of deliberate intent.

CHAPTER THREE: CROSS-BORDER JUDICIAL JURISDICTION

Cybercrimes frequently involve actors, infrastructure, and victims located in multiple jurisdictions. US law addresses cross-border cybercrime through the CFAA's extraterritorial application and the doctrine of personal jurisdiction. US courts have adopted an "effects-based" approach, asserting jurisdiction where the harmful effects of the offense are felt.

The EU's GDPR and the NIS2 Directive assert jurisdiction over any entity processing data or operating essential services within the EU, regardless of the provider's location. In Asia, China's Cybersecurity Law and Data Security Law assert sweeping jurisdiction over any data processing that affects Chinese national security, requiring foreign companies to store data locally.

African jurisdictions are increasingly asserting digital sovereignty. The African Union's Malabo Convention encourages member states to assert jurisdiction over cybercrimes affecting their citizens or infrastructure. Egypt and Morocco have enacted laws requiring data localization for critical sectors, directly challenging the US CLOUD Act's extraterritorial data demands.

CHAPTER FOUR: DIGITAL EVIDENCE AND ITS PROBATIVE VALUE

The probative value of digital evidence depends on its authenticity, integrity, and reliability. In the US, the Federal Rules of Evidence, particularly Rule 901(b)(9) regarding processes and systems, govern digital evidence. US courts require demonstration of a reliable chain of custody and cryptographic verification.

In Finland, the Code of Judicial Procedure requires that digital evidence be collected by a qualified forensic expert and that the integrity of the data be verifiable through hash values. In

Italy, the Code of Criminal Procedure mandates that digital evidence be seized under the supervision of a judicial authority.

In the Gulf and North Africa, UAE Federal Law 1/2006 and Egypt's Law 175/2018 recognize the admissibility of electronic evidence, but courts often require additional corroboration. Moroccan and Tunisian courts have been more cautious, frequently rejecting standalone digital evidence without physical corroboration or expert testimony from state-approved forensic laboratories.

VOLUME TWO: CRIMES AGAINST SYSTEMS AND DATA

CHAPTER ONE: UNAUTHORIZED ACCESS AND PERSISTENCE IN INFORMATION SYSTEMS

Article 323-1 of the French Penal Code and Section 202a of the German StGB criminalize unauthorized access to data, requiring proof of intent and the bypassing of security measures. The US CFAA similarly targets unauthorized access to protected computers.

In China, Article 285 of the Criminal Law criminalizes unauthorized intrusion into computer information systems in state affairs, national defense, or cutting-edge technology, imposing severe penalties including life imprisonment for severe circumstances.

In the Gulf, UAE Federal Law 34/2021 and Saudi Royal Decree M/17 criminalize unauthorized access without requiring proof of fraudulent intent, imposing strict liability and high penalties to deter cyber espionage.

CHAPTER TWO: INTERCEPTION, ALTERATION, AND DESTRUCTION OF DATA

The US Wiretap Act and Electronic Communications Privacy Act (ECPA) criminalize the intentional interception of electronic communications.

Italy's Penal Code Article 615-quater criminalizes the unauthorized installation of equipment for intercepting computer communications, while Article 635-ter addresses the destruction or deterioration of computer data. The Italian Supreme Court has held that altering a single numerical value in a database constitutes a criminal offense.

In Morocco, Law 07-03 and subsequent penal code amendments criminalize the interception, alteration, and destruction of data, with enhanced penalties for attacks on public administration systems.

CHAPTER THREE: CREATION AND DISTRIBUTION OF MALICIOUS SOFTWARE: THE RANSOMWARE EPIDEMIC

Ransomware represents the most severe and economically damaging cyber threat globally. Article 323-4 of the French Penal Code and Section 202c of the German StGB criminalize the creation and trafficking of such tools.

A critical legal debate has emerged regarding the payment of ransoms. The US Office of Foreign Assets Control (OFAC) has issued advisories that paying ransoms to sanctioned entities may violate sanctions laws, creating a legal dilemma for victims. Similarly, the European Parliament has debated proposals to outright ban ransom payments to disrupt the criminal business model, though critics argue this could endanger critical infrastructure like hospitals. Practitioners must advise clients on the severe legal and regulatory risks associated with ransom negotiations and payments across jurisdictions.

CHAPTER FOUR: AI CRIMES AND THE EU AI ACT

The EU AI Act, fully applicable in phases through 2025-2026, mandates that providers of general-purpose AI models implement robust cybersecurity measures and report serious incidents. This creates a new layer of corporate liability. In Saudi Arabia, Royal Decree M/17 provides for enhanced penalties when cybercrimes are committed "using advanced technological means," a provision now actively applied to AI-facilitated hacking.

VOLUME THREE: CONTENT AND DIGITAL IDENTITY CRIMES

CHAPTER ONE: ELECTRONIC FRAUD AND IDENTITY THEFT

Electronic fraud and identity theft represent some of the most prevalent cybercrimes. The US Identity Theft and Assumption Deterrence Act criminalizes the knowing transfer or use of means of identification of another person without lawful authority.

In Brazil, the Penal Code Article 154-A (invasion of computer devices) and Article 171 (fraud) are applied to electronic fraud. The 2024 legislative updates specifically criminalized phishing and business email compromise.

Tunisia's Organic Law 2022-54 criminalizes electronic fraud and identity theft, with specific provisions addressing the use of stolen digital identities to access public services. Egypt's Law 175/2018 similarly targets electronic fraud, with severe penalties for attacks on banking systems.

CHAPTER TWO: ELECTRONIC DEFAMATION AND EXTORTION

Electronic defamation and extortion balance reputation protection against freedom of expression. Germany's Network Enforcement Act (NetzDG) requires social media platforms to remove manifestly unlawful content, including defamation and hate speech, within 24 hours.

In North Africa, Algeria's Penal Code criminalizes defamation and insult through electronic means, with enhanced penalties for attacks on public officials and state institutions. Morocco's Law 09-08 and penal code provisions similarly address electronic defamation, but courts have increasingly emphasized the need to balance these provisions with constitutional free speech protections.

CHAPTER THREE: DIGITAL SEXUAL CRIMES

Digital sexual crimes represent some of the most harmful forms of cybercrime. The 2024 French amendment introduced Article 222-33-2-2, criminalizing the non-consensual distribution of AI-altered sexual content. Finland's Criminal Code amendments in 2025 specifically criminalized the creation and distribution of deepfake pornography.

In India, the Protection of Children from Sexual Offences (POCSO) Act and the Information Technology Act Section 67 criminalize the publication of obscene material, with courts applying these provisions to revenge porn and deepfakes involving minors.

CHAPTER FOUR: PERSONAL DATA PROTECTION

The protection of personal data is a fundamental right in Europe and an emerging priority globally. The EU GDPR imposes comprehensive requirements and significant penalties for non-compliance. The 2025 EU Court of Justice rulings clarified the extraterritorial application of the GDPR and the requirements for valid consent in AI-driven profiling.

Brazil's Lei Geral de Protecao de Dados (LGPD) closely mirrors the GDPR. In Africa, the African Union's Malabo Convention and the SADC Model Law on Data Protection provide frameworks for member states. Egypt's Data Protection Law (Law 151/2020) and South Africa's POPIA represent significant steps toward comprehensive data protection in the region.

VOLUME FOUR: ECONOMIC AND FINANCIAL CYBERCRIMES

CHAPTER ONE: MONEY LAUNDERING VIA CRYPTOCURRENCIES AND CBDCS

Money laundering via cryptocurrencies is heavily regulated under the EU's AMLD6 and MiCA regulations, which enforce the "Travel Rule" for Virtual Asset Service Providers (VASPs).

A new frontier in financial cybercrime involves Central Bank Digital Currencies (CBDCs), such as the digital yuan and the digital euro. While CBDCs offer enhanced state oversight, they also present novel cyber risks, including the potential for state-sponsored hacking of central ledger systems and the exploitation of programming vulnerabilities in smart contracts governing currency distribution. Jurisdictions are rapidly developing specific protocols to criminalize the tampering of CBDC infrastructure.

CHAPTER TWO: FRAUD IN CRYPTOCURRENCIES AND NFTS

Fraud in cryptocurrencies and NFTs challenges investor protection. The US SEC has aggressively pursued enforcement actions against unregistered crypto offerings, applying the Howey test to digital assets.

In Brazil, the Central Bank and the Securities Commission (CVM) have established regulatory sandboxes and clear guidelines for crypto asset offerings. In India, the Reserve Bank of India (RBI) and the Enforcement Directorate apply the Foreign Exchange Management Act (FEMA) and anti-money laundering laws to crypto transactions.

CHAPTER THREE: ATTACKS ON CRITICAL INFRASTRUCTURE

Attacks on critical infrastructure represent the most severe forms of cybercrime. The US Cybersecurity and Infrastructure Security Agency (CISA) directives and the 2025 Cyber Incident Reporting for Critical Infrastructure Act mandate 72-hour incident reporting.

The EU NIS2 Directive establishes comprehensive requirements for medium and large enterprises in 18 sectors, including 24-hour incident reporting and supply chain security. In Saudi Arabia, the National Cybersecurity Authority (NCA) mandates strict cybersecurity controls for critical infrastructure operators. Egypt's Cybersecurity Law mandates similar controls for state and vital infrastructure.

CHAPTER FOUR: CRIMINAL LIABILITY OF CORPORATIONS AND STATUTE OF LIMITATIONS

The criminal liability of corporations is increasingly tied to their cybersecurity posture. The US DOJ's 2024 guidelines state that a robust, audited compliance program can serve as a presumption against criminal prosecution. Germany's Corporate Sanctions Act (VerSanG) offers similar mitigation.

A critical procedural hurdle is the Statute of Limitations. In the US, the "Discovery Rule" often tolls the statute of limitations until the fraud or breach is discovered, which can be years after the initial hack. In contrast, many European and Gulf jurisdictions maintain strict, absolute limitation periods from the date of the act, creating a significant advantage for sophisticated, long-dormant threat actors. Practitioners must carefully analyze the applicable limitation period in the target jurisdiction to determine prosecutorial viability.

VOLUME FIVE: PROCEDURES AND INTERNATIONAL COOPERATION

CHAPTER ONE: DIGITAL INVESTIGATION AND EVIDENCE SEIZURE

Digital investigation and evidence seizure intersect with complex data sovereignty issues. The US CLOUD Act allows US law enforcement to demand data from US-based tech companies regardless of where the data is physically stored.

The EU's E-Evidence Regulation, fully applicable by 2026, allows judicial authorities in one member state to directly request data from service providers in another member state, bypassing traditional MLATs.

In Asia, China's Data Security Law and Personal Information Protection Law (PIPL) strictly regulate cross-border data transfers, requiring security assessments for law enforcement requests.

CHAPTER TWO: INTERNATIONAL JUDICIAL COOPERATION: MLATS AND JOINT INVESTIGATION TEAMS (JITS)

Traditional Mutual Legal Assistance Treaties (MLATs) are often too slow for the pace of cybercrime, with requests taking months or years. To address this, the European Union and other regions increasingly rely on Joint Investigation Teams (JITs). A JIT allows law enforcement and judicial authorities from two or more countries to work together on a specific criminal investigation, sharing information and evidence in real-time without the formal, lengthy MLAT process. The 2024 Second Additional Protocol to the Budapest Convention further facilitates this by allowing direct cooperation with service providers in urgent cases.

CHAPTER THREE: EXTRADITION OF OFFENDERS IN CYBERCRIMES

The extradition of cybercriminals is complicated by the dual criminality requirement and the political nature of cyber offenses. US extradition treaties and the European Arrest Warrant facilitate the surrender of offenders, but courts often scrutinize the dual criminality requirement, especially for AI-specific offenses.

In Asia, China's extradition treaties and its domestic extradition law emphasize the protection of national sovereignty, often refusing extradition for offenses deemed political or related to national security.

CHAPTER FOUR: PRACTICAL TEMPLATES AND CROSS-BORDER LEGAL GAP ANALYSIS

This section provides standardized, adaptable templates for:

1. Criminal Complaints for Unauthorized Access and Data Theft
2. Emergency Data Preservation Requests to Global ISPs and Cloud Providers
3. Mutual Legal Assistance Treaty (MLAT) Requests for Cross-Border Evidence
4. Interpol Red Notice Request Forms for Transnational Cybercriminals
5. Corporate Incident Response and Regulatory Notification Templates (compliant with US CISA, EU NIS2, and Gulf NCA requirements)

APPENDICES

Appendix A: Updated 2026 Global Penalty Tables

Comprehensive penalty tables for cyber offenses across all mentioned jurisdictions, including specific enhancements for Ransomware, AI crimes, and CBDC tampering.

Appendix B: Multilingual Legal Digital Terminology Dictionary

A comprehensive dictionary of legal and technical terms in English, French, German, Spanish, Portuguese, Arabic, Chinese, Japanese, Korean, and Hindi.

Appendix C: Map of Global Supreme Court Rulings 2020-2026 on Cybercrimes

A comprehensive map of key supreme court and constitutional court rulings on cybercrimes from 2020 to 2026, organized by jurisdiction, offense category, and practical significance.

Appendix D: Corporate Cyber Incident Response Checklist

A comprehensive checklist for corporate responses to cyber incidents, aligned with US CISA, EU NIS2, and global best practices, including immediate actions, investigative steps, legal obligations, and communication protocols within the first 24 hours.

Appendix E: Global Data Processing Agreement Templates

Comprehensive templates for data processing agreements compliant with the EU GDPR, US state laws, Brazilian LGPD, African Union standards, and Gulf data protection regulations.

Appendix F: Arabic-English Cyber Law Glossary

A specialized glossary bridging Arab legal terminology with international standards. Examples:

- الجرائم الإلكترونية: Cybercrimes
- السيادة الرقمية: Digital Sovereignty
- التشفير المتجانس: Homomorphic Encryption
- مبدأ الشرعية: Principle of Legality (Nullum crimen sine lege)
- المساعدة القانونية المتبادلة: Mutual Legal Assistance (MLAT)

Appendix G: Cross-Border Legal Gap Analysis Checklist

A practical tool for practitioners to assess jurisdictional conflicts, data localization requirements, statute of limitations, and extradition feasibility before initiating cross-border cyber litigation or investigation.

INTELLECTUAL PROPERTY RIGHTS

Copyright 2026 Dr. Mohamed Kamal Arafa Elrakhawi. Some rights reserved. This work is licensed under the Apache License 2.0 for academic and non-commercial use, enabling independent verification and regulatory adoption. Commercial deployment, enterprise integration, and proprietary product development require explicit written permission. All contributions and derivative works are governed by transparent attribution requirements. The author retains moral rights, and patent applications covering the comparative legal framework and cross-jurisdictional compliance mechanisms are pending under international intellectual property jurisdictions.

GLOBAL SEARCH KEYWORDS FOR ACADEMIC DISCOVERY

English: global cybercrime law, comparative digital law, Elrakhawi Doctrine, US CFAA, GDPR, EU NIS2, Chinese cybersecurity law, Brazilian LGPD, African Union Malabo Convention, AI cybercrimes, cross-border digital evidence, ransomware legal frameworks, CBDC cyber risks, Joint Investigation Teams.

Arabic: قانون الجرائم الإلكترونية العالمي، القانون الرقمي المقارن، عقيدة الرخاوي، قانون الاحتيال وإساءة استخدام الكمبيوتر، قانون الأمن السيبراني الصيني، قانون حماية البيانات البرازيلي، NIS2 الأمريكي، اللائحة العامة لحماية البيانات، توجيه اتفاقية الاتحاد الأفريقي ملابو، جرائم الذكاء الاصطناعي، الأدلة الرقمية عبر الحدود، الأطر القانونية لبرامج الفدية، مخاطر العملات الرقمية للبنوك المركزية، فرق التحقيق المشتركة.

French: droit mondial de la cybercriminalité, droit numérique comparé, Doctrine Elrakhawi, CFAA américain, RGPD, directive NIS2 de l'UE, droit chinois de la cybersécurité, LGPD brésilien, Convention de l'Union africaine de Malabo, cybercrimes IA, preuves numériques transfrontalières, cadres juridiques des ransomwares, risques cyber des MNBC, équipes communes d'enquête.

Spanish: derecho global de ciberdelincuencia, derecho digital comparado, Doctrina Elrakhawi, CFAA de EE. UU., RGPD, directiva NIS2 de la UE, ley de ciberseguridad china, LGPD de Brasil, Convención de la Unión Africana de Malabo, ciberdelitos de IA, evidencia digital transfronteriza, marcos legales de ransomware, riesgos cibernéticos de las CBDC, equipos conjuntos de investigación.

German: globales Cyberkriminalitätsrecht, vergleichendes digitales Recht, Elrakhawi-Doktrin, US CFAA, DSGVO, EU NIS2-Richtlinie, chinesisches Cybersicherheitsgesetz, brasilianisches LGPD, Afrikanische Union Malabo-Konvention, KI-Cyberkriminalität, grenzüberschreitende digitale Beweise, Rechtsrahmen für Ransomware, Cyber Risiken von CBDCs, Gemeinsame Ermittlungsgruppen.

Chinese: 全球网络犯罪法，比较数字法，埃尔拉哈维学说，美国 CFAA，GDPR，欧盟 NIS2，中国网络安全法，巴西 LGPD，非洲联盟马拉博公约，人工智能网络犯罪，跨境数字证据，勒索软件法律框架，央行数字货币网络风险，联合调查组。

Russian: глобальное право киберпреступности, сравнительное цифровое право, доктрина Эльрахауи, американский CFAA, GDPR, директива ЕС NIS2, китайский закон о кибербезопасности, бразильский LGPD, Малабская конвенция Африканского союза, киберпреступления ИИ, трансграничные цифровые доказательства, правовые рамки программ-вымогателей, киберриски CBDC, совместные следственные группы.

Portuguese: direito global de cibercrime, direito digital comparado, Doutrina Elrakhawi, CFAA dos EUA, GDPR, diretiva NIS2 da UE, lei de cibersegurança chinesa, LGPD do Brasil, Convenção da União Africana de Malabo, cibercrimes de IA, evidências digitais transfronteiriças, estruturas legais de ransomware, riscos cibernéticos de CBDCs, equipes conjuntas de investigação.

Italian: diritto globale sulla criminalità informatica, diritto digitale comparato, Dottrina Elrakhawi, CFAA statunitense, GDPR, direttiva NIS2 dell'UE, legge cinese sulla cybersicurezza, LGPD brasiliano, Convenzione dell'Unione Africana di Malabo, crimini informatici IA, prove digitali transfrontaliere, quadri giuridici sul ransomware, rischi informatici delle CBDC, squadre investigative congiunte.

Japanese: 世界的サイバー犯罪法, 比較デジタル法, エルラハウィ教義, 米国 CFAA, GDPR, EU NIS2 指令, 中国サイバーセキュリティ法, ブラジル LGPD, アフリカ連合マラボ条約, AI サイバー犯罪, 国境を越えたデジタル証拠, ランサムウェアの法的枠組み, CBDC のサイバーリスク, 共同捜査チーム。

COMPREHENSIVE ALPHABETICAL INDEX

A

African Union Malabo Convention, Vol 1 Ch 3, Vol 5 Ch 2
AI Crimes, Vol 1 Ch 2, Vol 2 Ch 4
Algorithmic Accountability, Foreword
Attorney-Client Privilege in Cyber Investigations, Vol 5 Ch 1
Authorization (Scope of), Vol 1 Ch 1, Vol 2 Ch 1

B

Blockchain Evidence, Vol 1 Ch 4
Brazilian LGPD, Vol 3 Ch 4, Vol 4 Ch 1

C

Central Bank Digital Currencies (CBDCs), Vol 4 Ch 1
Computer Fraud and Abuse Act (CFAA), Vol 1 Ch 1, Vol 2 Ch 1
Corporate Liability, Vol 4 Ch 4
Cross-Border Legal Gap Analysis, Appendix G

D

Data Sovereignty, Vol 1 Ch 3
Deepfake Pornography, Vol 3 Ch 3
Digital Evidence Admissibility, Vol 1 Ch 4
Doctrine, Elrakhawi, Foreword, Vol 1 Ch 1

E

Elrakhawi Doctrine, Foreword, Vol 1 Ch 1
EU AI Act, Vol 1 Ch 2, Vol 2 Ch 4
EU NIS2 Directive, Vol 4 Ch 3
Extradition, Vol 5 Ch 3

F

Fraud, Electronic, Vol 3 Ch 1
Fraud, Cryptocurrency, Vol 4 Ch 2

G

GDPR, Vol 3 Ch 4, Vol 4 Ch 1
Germany (StGB), Vol 1 Ch 1, Vol 2 Ch 1

J

Joint Investigation Teams (JITs), Vol 5 Ch 2

L

List of Abbreviations, Front Matter

List of Cases, Front Matter

List of Legislation, Front Matter

M

Malabo Convention, Vol 1 Ch 3, Vol 5 Ch 2

Money Laundering, Cryptocurrency, Vol 4 Ch 1

Mutual Legal Assistance Treaties (MLATs), Vol 5 Ch 2

R

Ransomware, Vol 2 Ch 3, Vol 4 Ch 1

Royal Decree M/17 (Saudi Arabia), Vol 1 Ch 1, Vol 2 Ch 1, Vol 2 Ch 4

Royal Decree M/19 (Saudi Arabia), Vol 3 Ch 4

S

Statute of Limitations, Vol 4 Ch 4

StGB (German Criminal Code), Vol 1 Ch 1, Vol 2 Ch 1

V

Van Buren v. United States, Vol 1 Ch 1, Table of Cases

END OF DOCUMENT

Version: 2.1.0 Final Academic Edition

Date: September 2026

Project Contact: elrakhawimohamed@gmail.com

Repository: <https://github.com/DrMohamedKamal/elrakhawi-doctrine-cyberlaw>

Rights: Copyright 2026 Dr. Mohamed Kamal Arafa Elrakhawi. Some rights reserved.

Jurisdiction: Arab Republic of Egypt

DOI: 10.5281/zenodo.22908154