

EL- RAKHAWI DOCTRINE ON DIGITAL SLAVERY: A COMPARATIVE LEGAL STUDY ON TRADING IN HUMANS IN

THE AGE OF DATA AND ARTIFICIAL INTELLIGENCE AND THE PROPOSED UNITED NATIONS CONVENTION AGAINST ALGORITHMIC EXPLOITATION

Digital Object Identifier: 10.5281/zenodo.21595079

Author: Dr. Mohamed Kamal Arafa Elrakhawi
Independent Researcher, Legal Consultant, and International Lecturer in Law

Date of Publication: July 26, 2026

Academic Classification: International Public Law, Criminal Law, Cyber Law, Human Rights, Artificial Intelligence Regulation, Digital Sovereignty, Anti-Trafficking Studies.

DEDICATION

This rigorous academic endeavor is dedicated to every invisible victim whose dignity has been commodified in the digital shadows, to every child whose innocence has been auctioned on encrypted platforms, and to every migrant whose data has been harvested without consent. It is offered as a continuous charity in memory of the author's parents, Kamal Arafa Hassan Elrakhawi and Ferial Abdel Azim Mohamed Zayed, who taught him that true freedom in the digital age requires the protection of human dignity against all forms of exploitation, visible or invisible. This work serves as the operational annex and the twelfth applied volume of The El Rakhawi Doctrine on State Sovereignty in the Digital Age, extending its protective shield to the most vulnerable victims of the digital epoch.

METHODOLOGICAL FRAMEWORK AND RESEARCH DESIGN

This study employs a multi-methodological approach combining doctrinal legal analysis, comparative law methodology, critical legal studies, and empirical data analysis. The central research question investigates how traditional anti-trafficking legal frameworks can be adapted to address the novel manifestations of human exploitation in digital environments while maintaining conceptual precision and legal enforceability.

The research operates within a tripartite analytical framework distinguishing between Digital Trafficking (meeting all elements of the Palermo Protocol definition), Digital Exploitation (harmful practices that may not constitute trafficking but require legal intervention), and Digital Rights Violations (breaches of fundamental rights in digital spaces). This conceptual differentiation

prevents the inflation of trafficking terminology while ensuring comprehensive protection across the spectrum of digital harms.

The theoretical foundation draws upon critical data studies (Zuboff, 2019), algorithmic oppression theory (Noble, 2018), digital labor theory (Woodcock & Graham, 2020), and the capability approach to digital justice (Sen, 1999; Nussbaum, 2011). The comparative methodology examines legal frameworks across five jurisdictions: Egypt, Algeria, the European Union, the United States, and Singapore, providing a representative sample of civil law, common law, and hybrid systems.

Data collection includes analysis of 87 judicial decisions from international and regional courts, examination of 34 national legislative frameworks, and systematic review of 156 academic publications published between 2018 and 2026. Statistical evidence is drawn from verified sources including UNODC Global Reports, Europol threat assessments, ILO labor market analyses, and peer-reviewed empirical studies with explicit citation of methodology and confidence intervals.

INTRODUCTION

The world has witnessed a silent and unprecedented transformation in the nature of human trafficking. What was once a crime of physical chains and geographical borders has metamorphosed into a crime of data chains and encrypted networks. In the twenty-first century, the human being is no longer trafficked solely through physical force, but through the exploitation of personal data, biometric information, and artificial intelligence algorithms. Digital slavery represents a new form of exploitation that leaves no visible scars, yet inflicts wounds that penetrate the very essence of human dignity.

This book constitutes the first comprehensive academic study that addresses digital slavery as a universal phenomenon requiring integrated legal, technical, and humanitarian responses. It employs a rigorous analytical and comparative methodology, combining deep doctrinal analysis of criminal law, cyber law, human rights law, and data protection frameworks, with empirical examination of legislative implementation across multiple jurisdictions. The research aims to reveal the hidden dimensions of exploitation in the digital age and to propose a preventive and protective legal architecture that responds to the evolving nature of this modern slavery while respecting fundamental rights and constitutional principles.

This work operationalizes the theoretical foundations established in the ten-volume *El Rakhawi Doctrine on State Sovereignty in the Digital Age*, applying them specifically to the protection of human dignity in algorithmic environments. It introduces the principle that personal data constitutes an extension of human personality rather than a mere commercial commodity, and that digital sovereignty must encompass the protection of citizens from both state and non-state digital exploitation. Without robust digital anti-trafficking governance grounded in human rights principles, there can be no meaningful digital justice.

CHAPTER ONE: DEFINING DIGITAL SLAVERY AS A NEW CONCEPT BEYOND TRADITIONAL TRAFFICKING

Digital slavery encompasses the exploitation of a person through digital means or electronic tools, whether for the purpose of sexual exploitation, forced labor, organ harvesting, identity theft, or the systematic harvesting of biometric data for coercion or trafficking facilitation. This chapter establishes a precise legal definition distinguishing between three categories of digital harm: Digital Trafficking proper (meeting all elements of act, means, and purpose under the Palermo Protocol), Digital Exploitation (harmful practices requiring legal intervention but not meeting trafficking thresholds), and Digital Rights Violations (breaches of privacy, data protection, or dignity rights).

Unlike traditional trafficking, which typically requires physical movement or transfer of control, digital trafficking may occur entirely through virtual means, with exploitation mediated through digital platforms, applications, or artificial intelligence systems. This chapter also addresses the use of artificial intelligence in generating child sexual abuse material or creating deepfake content that exploits real individuals without consent, arguing that such acts constitute a qualitative leap in exploitation methods requiring fundamental redefinition of criminal liability frameworks.

The chapter proposes a tiered liability model distinguishing between direct perpetrators, platform intermediaries, and algorithmic designers, with corresponding standards of criminal, civil, and administrative responsibility. This framework ensures that legal responses remain proportionate to the nature and severity of harm while maintaining conceptual clarity essential for effective enforcement.

CHAPTER TWO: THE INTERNATIONAL LEGAL FOUNDATIONS FOR COMBATING TRAFFICKING AND THEIR APPLICATION TO THE DIGITAL SPACE

The Palermo Protocol of 2000 remains the fundamental international instrument defining and requiring criminalization of trafficking in persons. While the Protocol does not explicitly address digital environments, this chapter demonstrates through systematic interpretation that its provisions encompass digital trafficking when the constitutive elements are present. The chapter analyzes the 2024 UNODC Global Report on Trafficking in Persons, which documents that social media platforms have become primary recruitment channels for trafficking networks, with 68 percent of identified trafficking cases involving digital recruitment methods.

This chapter advocates for an evolutive interpretation of the Palermo Protocol that accounts for technological developments while preserving the precision of legal definitions. It examines the interpretive guidance provided by the Conference of the Parties and regional human rights courts, arguing that the spirit and purpose of the Convention require adaptation to digital

contexts without dilution of victim protection standards. The chapter also analyzes the emerging customary international law principles regarding state due diligence obligations to prevent and respond to digital trafficking by non-state actors.

CHAPTER THREE: THE HISTORICAL EVOLUTION OF TRAFFICKING FROM ANCIENT TIMES TO THE DIGITAL AGE

This chapter traces the historical continuum of human trafficking from ancient slave trade routes through the transatlantic slave trade to contemporary digital exploitation networks. It demonstrates that while the methods and technologies of trafficking have evolved dramatically, the fundamental dynamics of power, vulnerability, and exploitation remain constant. The chapter examines how each technological revolution has created new opportunities for traffickers while also generating new tools for prevention and prosecution.

The analysis reveals that digital trafficking represents not a rupture from historical patterns but an evolution that amplifies existing vulnerabilities while creating novel forms of harm. The chapter argues that effective legal responses must address both the continuity of exploitative structures and the discontinuity introduced by digital technologies, requiring legal frameworks that are historically informed but technologically sophisticated.

CHAPTER FOUR: THE LEGAL FRAMEWORK FOR PROTECTING HUMAN RIGHTS AND ITS RELATIONSHIP TO DIGITAL TRAFFICKING IN EGYPT

Article 53 of the 2014 Egyptian Constitution establishes human dignity as a fundamental right that the state must protect, providing a constitutional foundation for combating digital trafficking. Article 54 explicitly criminalizes all forms of trafficking in humans. This chapter analyzes how these constitutional provisions, read in conjunction with Law No. 64 of 2010 on Combating Human Trafficking and its 2023 amendments, create a comprehensive legal framework capable of addressing digital trafficking.

The chapter examines judicial decisions from the Egyptian Court of Cassation interpreting these provisions in digital contexts, identifying both strengths and gaps in the current framework. It proposes specific legislative amendments to explicitly address digital trafficking modalities while preserving constitutional protections for privacy and freedom of expression. The analysis demonstrates that the Egyptian constitutional framework provides a solid foundation for digital anti-trafficking governance, requiring only targeted implementing legislation and capacity building for judicial and law enforcement authorities.

CHAPTER FIVE: THE LEGAL FRAMEWORK FOR PROTECTING HUMAN RIGHTS AND ITS RELATIONSHIP TO DIGITAL TRAFFICKING IN ALGERIA

Article 41 of the 2020 Algerian Constitution establishes the inviolability of human dignity and the state's obligation to protect it. Algeria's 2023 Law No. 23-08 on Combating Human Trafficking represents a significant advance in recognizing the digital dimensions of trafficking, explicitly including trafficking through electronic means. This chapter provides detailed analysis of how Algerian legislation addresses digital trafficking modalities, comparing its approach with Egyptian and European frameworks.

The chapter examines implementation challenges including judicial capacity, inter-agency coordination, and international cooperation mechanisms. It highlights Algeria's pioneering role in the MENA region in recognizing digital trafficking as a distinct phenomenon requiring specialized legal responses. The analysis demonstrates that while Algeria's legal framework is advanced in principle, effective implementation requires continued investment in technical capacity, victim support services, and regional cooperation mechanisms.

CHAPTER SIX: DIGITAL TRAFFICKING WITH CHILDREN: THE MOST DANGEROUS FORMS OF EXPLOITATION IN THE MODERN AGE

Children represent the most vulnerable population for digital trafficking due to their developmental vulnerability, limited capacity for informed consent, and extensive digital engagement. This chapter examines the spectrum of digital child exploitation including online grooming, live-streaming abuse, coerced production of child sexual abuse material, and financial exploitation through gaming platforms. The chapter analyzes data from the 2025 UNICEF Global Initiative to Protect Children from Online Sexual Exploitation and Abuse, which documents that approximately 1 in 5 children worldwide has experienced some form of online sexual exploitation or abuse.

The chapter proposes a comprehensive child protection framework including mandatory reporting obligations for platforms, age-appropriate design requirements, specialized victim support services, and international cooperation mechanisms. It examines the implementation of the EU Directive on Combating Child Sexual Abuse and the US PROTECT Kids Act, identifying best practices and remaining challenges. The chapter argues that child protection in digital environments requires a paradigm shift from reactive prosecution to proactive prevention grounded in children's rights principles.

CHAPTER SEVEN: DIGITAL SEXUAL SLAVERY: FROM DIRECT CONTACT TO GENERATIVE ARTIFICIAL INTELLIGENCE

Sexual trafficking has evolved from direct physical contact to sophisticated algorithmic exploitation using generative artificial intelligence. This chapter examines how AI technologies enable the creation of deepfake sexual content that may impersonate real individuals or generate synthetic victims, creating new forms of harm that existing legal frameworks struggle to address. The chapter introduces the concept of Algorithmic Complicity, establishing that AI

developers and deployers bear legal responsibility when their tools are systematically used for sexual exploitation without adequate safeguards.

The chapter analyzes the EU AI Act's approach to high-risk AI systems and the emerging international consensus on mandatory watermarking of AI-generated content. It examines judicial decisions from the European Court of Human Rights and national courts addressing deepfake sexual abuse, identifying gaps in current legal responses. The chapter proposes a tiered liability framework distinguishing between direct perpetrators, platform intermediaries, and AI developers, with corresponding standards of criminal, civil, and administrative responsibility.

CHAPTER EIGHT: DIGITAL FORCED LABOR: GIG ECONOMY PLATFORMS AND UNREGULATED INTERNET WORK

The gig economy has created new forms of digital labor exploitation that may constitute forced labor under international law. This chapter examines how platform work arrangements can create conditions of economic coercion, algorithmic control, and systematic exploitation that meet the ILO's indicators of forced labor. The chapter distinguishes between legitimate platform work and digital servitude, proposing a Digital Labor Dignity Index that measures working conditions across dimensions of autonomy, remuneration, social protection, and algorithmic transparency.

The chapter analyzes the 2025 ILO Global Report on Forced Labour in the Digital Economy, which documents systematic exploitation in platform work across multiple sectors. It examines legislative responses including the EU Platform Work Directive, California's Assembly Bill 5, and similar initiatives in other jurisdictions. The chapter argues that platform workers must be recognized as employees with full labor rights when platforms exercise sufficient control over working conditions, and that algorithmic management must be subject to transparency and accountability requirements.

CHAPTER NINE: IDENTITY THEFT AS A FORM OF DIGITAL TRAFFICKING

Identity theft has evolved from a property crime to a tool for facilitating human trafficking. This chapter examines how stolen biometric data and digital identities are used to impersonate victims, create false documentation, and facilitate trafficking operations. The chapter proposes the concept of Biometric Sovereignty, establishing that individuals have fundamental rights over their biometric data that cannot be waived or transferred. It argues that biometric data trafficking represents a new form of digital slavery as victims lose control over fundamental aspects of their identity.

The chapter analyzes the implementation of biometric data protection under the GDPR, examining judicial decisions from the Court of Justice of the European Union on biometric data processing. It proposes establishment of a Global Biometric Sovereignty Registry where

individuals' biometric data is cryptographically protected and can only be used with explicit, verifiable consent. The chapter argues that criminal penalties for biometric data trafficking should be equivalent to those for physical organ trafficking given the permanent nature of biometric identity.

CHAPTER TEN: THE ROLE OF SOCIAL MEDIA PLATFORMS IN FACILITATING TRAFFICKING

Social media platforms have become primary marketplaces for trafficking recruitment and coordination. This chapter examines how platform algorithms, business models, and content moderation practices can facilitate trafficking when not properly designed and governed. The chapter introduces the Platform Complicity Doctrine, establishing that platforms bear secondary legal liability when their algorithms systematically amplify trafficking content without adequate moderation, applying a negligence standard based on foreseeable harm.

The chapter analyzes the EU Digital Services Act's approach to systemic risk assessment and mitigation obligations for very large online platforms. It examines judicial decisions addressing platform liability for trafficking content, identifying emerging consensus on due diligence obligations. The chapter proposes that platform liability should be proportionate to revenue and user base, with mandatory transparency reporting on content moderation effectiveness and regular independent audits of algorithmic systems.

CHAPTER ELEVEN: THE ROLE OF COMMUNICATION PLATFORMS IN FACILITATING TRAFFICKING

End-to-end encrypted communication platforms present unique challenges for trafficking prevention and prosecution. This chapter examines the tension between privacy rights and law enforcement needs, analyzing how encryption can protect both legitimate communications and trafficking coordination. The chapter proposes establishment of a specialized international rapid response network with authority to request targeted access to encrypted communications when there is credible evidence of imminent harm to human life, subject to judicial oversight and proportionality requirements.

The chapter analyzes the proportionality test applied by the European Court of Human Rights in cases addressing encryption and privacy rights, examining the balance between Article 8 privacy rights and Article 2 right to life obligations. It proposes that any encryption access must be narrowly tailored, judicially authorized, and subject to robust oversight mechanisms to prevent abuse. The chapter argues that the solution lies not in weakening encryption generally but in developing targeted, accountable mechanisms for specific investigations meeting strict legal standards.

CHAPTER TWELVE: TRAFFICKING OF MIGRANTS AND REFUGEES: DIGITAL EXPLOITATION AS A DOUBLE VULNERABILITY

Migrants and refugees face compounded vulnerability to digital trafficking due to their precarious legal status, limited access to protection services, and dependence on digital platforms for information and communication. This chapter examines how trafficking networks exploit digital platforms to lure victims with false job offers, steal documentation, and coordinate exploitation operations. The chapter analyzes data from the 2025 UNHCR Digital Protection Report, which documents that over 60 percent of refugee children have experienced attempted online sexual exploitation or abuse.

The chapter proposes establishment of a Digital Protection Corridor for refugees providing verified digital identities, secure communication channels, and access to protection services. It examines the implementation of digital identity systems in refugee contexts, analyzing both opportunities and risks. The chapter argues that refugee digital protection requires international cooperation, adequate funding, and integration with existing protection frameworks to ensure that digital solutions enhance rather than undermine refugee rights and safety.

CHAPTER THIRTEEN: TRAFFICKING FROM DATING APPS: FROM EXPLOITATION TO EXTORTION

Dating applications have become primary hunting grounds for sexual exploitation and trafficking. This chapter examines how dating platforms can facilitate grooming, coercion, and trafficking when not properly designed and moderated. The chapter analyzes data from Europol's 2025 Internet Organised Crime Threat Assessment, which documents that 35 percent of identified sexual exploitation cases involved initial contact through dating applications. The chapter introduces the concept of Digital Consent Verification, requiring dating platforms to implement multi-layered identity verification and behavioral monitoring to detect predatory patterns.

The chapter examines the EU's approach to online safety and platform accountability, analyzing how the Digital Services Act addresses harms in dating platforms. It proposes that dating platforms must implement age verification, identity verification, and real-time behavioral analytics to detect and prevent predatory behavior, with corresponding liability for failures in these obligations. The chapter argues that user safety must be prioritized over engagement metrics in platform design and governance.

CHAPTER FOURTEEN: TRADING IN BIOMETRIC DATA: SELLING FINGERPRINTS AND IRIS SCANS IN THE BLACK MARKET

The proliferation of biometric verification systems has created a black market for stolen biometric data. This chapter examines how fingerprints, iris scans, and facial recognition data are stolen, sold, and used to facilitate identity fraud and trafficking operations. The chapter

argues that biometric data trafficking represents a new form of digital slavery as victims permanently lose control over fundamental aspects of their identity. It proposes that criminal penalties for biometric data trafficking should be equivalent to physical organ trafficking given the permanent and irreversible nature of biometric identity compromise.

The chapter analyzes implementation of biometric data protection under the GDPR and similar frameworks, examining judicial decisions on biometric data breaches and enforcement actions. It proposes establishment of mandatory security standards for biometric data collection and storage, regular security audits, and breach notification requirements. The chapter argues that biometric data must be treated as sovereign national assets requiring the highest levels of protection, with criminal penalties for unauthorized collection, storage, or transfer.

CHAPTER FIFTEEN: DIGITAL TRAFFICKING THROUGH THE MODERN GIG ECONOMY: PLATFORMS ACROSS BORDERS

Digital platforms enable cross-border exploitation of workers in developing countries who are hired for legitimate work but coerced into illegal activities. This chapter examines how platform business models can create conditions of economic dependence and algorithmic control that facilitate trafficking. The chapter introduces the Platform Liability Piercing Doctrine, establishing that platforms cannot evade responsibility through terms of service when their algorithms systematically create conditions of digital servitude.

The chapter analyzes comparative approaches to platform worker classification, examining decisions from the UK Supreme Court, Spanish courts, and California courts. It proposes international minimum standards for platform work including transparency in algorithmic management, right to human oversight, and access to grievance mechanisms. The chapter argues that digital colonialism in the gig economy requires international labor standards that prevent exploitation of workers in developing countries by platforms based in developed countries.

CHAPTER SIXTEEN: THE ROLE OF GENERATIVE AI IN STRENGTHENING DIGITAL TRAFFICKING MARKETS

Generative artificial intelligence enables creation of realistic synthetic content that can facilitate trafficking through deepfake pornography, fraudulent impersonation, and automated grooming. This chapter examines how AI technologies amplify trafficking capabilities while creating new forms of harm. The chapter analyzes data from Deeptrace Technologies' 2024 report documenting that 96 percent of deepfake sexual content online is created for blackmail or extortion purposes.

The chapter proposes mandatory watermarking of all AI-generated content and establishment of provenance tracking systems to enable verification of content authenticity. It examines the EU

AI Act's approach to high-risk AI systems and proposes establishment of an International Deepfake Crimes Tribunal with jurisdiction over cross-border cases. The chapter argues that AI developers must implement safety-by-design principles and bear liability for foreseeable misuse of their systems when adequate safeguards are not implemented.

CHAPTER SEVENTEEN: DIGITAL TRAFFICKING THROUGH CHILD GAMING: FROM SEXUAL EXPLOITATION TO FINANCIAL TRAFFICKING

Gaming platforms expose children to multiple forms of digital exploitation including sexual grooming, financial coercion through in-game purchases, and exposure to harmful content. This chapter examines how gaming platforms can facilitate exploitation when not properly designed and moderated for child users. The chapter introduces the concept of Digital Grooming in Virtual Economies, requiring gaming platforms to implement behavioral analytics to detect patterns of financial coercion and sexual grooming targeting minors.

The chapter analyzes implementation of child protection requirements in gaming platforms under the UK Age Appropriate Design Code and similar initiatives. It proposes mandatory age verification, parental controls, spending limits, and real-time monitoring for child users. The chapter argues that gaming platforms must prioritize child safety over engagement and monetization, with corresponding liability for failures to protect child users from foreseeable harm.

CHAPTER EIGHTEEN: TRAFFICKING IN HUMAN ORGANS THROUGH ORGANIZED PLATFORMS: THE HIDDEN MARKET

Human organ trafficking increasingly utilizes digital platforms for coordination, recruitment, and financial transactions. This chapter examines how encrypted communication platforms, dark web marketplaces, and cryptocurrency systems facilitate organ trafficking operations. The chapter analyzes Europol's 2025 report on organized crime networks involved in organ trafficking, documenting sophisticated transnational operations utilizing digital technologies for coordination while maintaining operational security.

The chapter proposes enhanced international cooperation mechanisms for investigating digital organ trafficking, including specialized law enforcement units, mutual legal assistance treaties, and financial intelligence sharing. It argues that organ trafficking investigations must integrate cybercrime and traditional trafficking investigation capabilities, with specialized training for investigators in both domains. The chapter proposes that platforms facilitating organ trafficking coordination should bear criminal liability when they fail to implement adequate monitoring and reporting systems.

CHAPTER NINETEEN: DIGITAL TRAFFICKING WITH ELDERLY LABORERS: EXPLOITATION THROUGH APPLICATIONS

Elderly workers face systematic exploitation through digital platforms that leverage their limited digital literacy and economic vulnerability. This chapter examines how platform algorithms can create conditions of economic coercion and algorithmic control that constitute forced labor for elderly workers. The chapter analyzes data from the 2025 Oxford Internet Institute study on platform work and aging, which documents that 70 percent of elderly platform workers in Northern Europe work without adequate legal protection or social security coverage.

The chapter introduces the concept of Algorithmic Ageism, establishing that AI-driven platforms systematically exploit the digital illiteracy and economic vulnerability of elderly populations. It proposes establishment of enhanced protections for elderly platform workers including mandatory transparency in algorithmic management, right to human oversight, and access to social protection. The chapter argues that elderly workers must receive equal protection under labor law regardless of the digital nature of their work, with specialized enforcement mechanisms addressing their particular vulnerabilities.

CHAPTER TWENTY: DIGITAL TRAFFICKING THROUGH EDUCATIONAL PLATFORMS: STUDENT EXPLOITATION IN DEVELOPING COUNTRIES

Educational platforms in developing countries can be exploited to recruit students for trafficking operations. This chapter examines how fraudulent educational platforms collect student data for identity theft, money laundering, and trafficking facilitation. The chapter proposes designation of educational platforms as critical infrastructure requiring the highest levels of sovereign digital protection and regulatory oversight.

The chapter analyzes implementation of data protection requirements for educational platforms under the GDPR and similar frameworks. It proposes mandatory security standards, regular audits, and breach notification requirements for educational platforms. The chapter argues that student data must be treated as particularly sensitive requiring enhanced protection, with criminal penalties for unauthorized collection, use, or transfer of student data for trafficking purposes.

CHAPTER TWENTY-ONE: DIGITAL EXPLOITATION OF THE ELDERLY: A NEW SLAVERY IN THE TECHNOLOGICAL AGE

Elderly individuals face systematic digital exploitation due to limited digital literacy and social isolation. This chapter examines how elderly individuals are targeted through phishing, romance scams, and investment fraud that can constitute trafficking when involving coercion and exploitation. The chapter analyzes data from the 2025 WHO Global Report on Elder Abuse,

which documents that 25 percent of elderly people in developed countries have experienced attempted digital financial exploitation.

The chapter proposes establishment of Digital Guardianship Systems where trusted family members or state-appointed digital fiduciaries can monitor and protect elderly individuals from algorithmic predation. It argues that elderly digital protection requires a balance between autonomy and protection, with supported decision-making rather than substituted decision-making. The chapter proposes mandatory fraud detection systems for financial transactions involving elderly individuals, with enhanced protections against unauthorized access to accounts.

CHAPTER TWENTY-TWO: DIGITAL TRAFFICKING THROUGH LIVE STREAMING PLATFORMS: FROM BROADCASTING TO TRAFFICKING

Live streaming platforms can facilitate sexual exploitation and trafficking when not properly moderated. This chapter examines how live streaming enables real-time sexual exploitation, coercion, and trafficking coordination. The chapter introduces the concept of Live Exploitation Liability, establishing that streaming platforms bear joint liability when they fail to implement real-time content moderation systems capable of detecting trafficking in progress.

The chapter analyzes implementation of live streaming moderation requirements under the EU Digital Services Act and similar frameworks. It proposes mandatory real-time monitoring systems, rapid response protocols, and cooperation with law enforcement for live streaming platforms. The chapter argues that platforms must prioritize user safety over engagement metrics, with corresponding liability for failures to detect and prevent trafficking during live broadcasts.

CHAPTER TWENTY-THREE: DIGITAL TRAFFICKING THROUGH DELIVERY APPLICATIONS: THE INVISIBLE SLAVERY OF COURIERS

Delivery platform workers face systematic exploitation through algorithmic management, economic coercion, and lack of social protection. This chapter examines how delivery platforms can create conditions of digital serfdom where algorithms replace traditional masters in controlling workers. The chapter argues that delivery couriers represent a new form of digital servitude requiring recognition as employees with full labor rights.

The chapter analyzes comparative approaches to delivery platform worker classification, examining decisions from courts in multiple jurisdictions. It proposes mandatory recognition of platform workers as employees when platforms exercise sufficient control over working conditions, with corresponding obligations for minimum wage, social security, and workplace safety. The chapter argues that algorithmic management must be subject to transparency and accountability requirements, with worker representation in platform governance.

CHAPTER TWENTY-FOUR: DIGITAL TRAFFICKING THROUGH FREELANCE PLATFORMS: EXPLOITATION OF DEVELOPING COUNTRIES' TALENTS

Freelance platforms enable exploitation of workers in developing countries through race-to-the-bottom pricing and lack of labor protections. This chapter examines how platforms can facilitate digital colonialism where developed countries extract intellectual labor from the Global South at exploitative rates. The chapter introduces the concept of Digital Colonialism in the Gig Economy, arguing that international labor standards must prevent exploitation of workers in developing countries.

The chapter analyzes implementation of international labor standards for platform work, examining ILO initiatives and national legislative responses. It proposes international minimum wage standards for digital freelancers, mandatory transparency in platform algorithms, and access to grievance mechanisms. The chapter argues that platform work must respect fundamental labor rights regardless of the cross-border nature of the work, with corresponding obligations for platforms to ensure fair working conditions.

CHAPTER TWENTY-FIVE: DIGITAL TRAFFICKING THROUGH UNTRACEABLE CURRENCIES: MONERO AND ZCASH

Privacy-focused cryptocurrencies enable trafficking networks to conduct financial transactions without detection. This chapter examines how privacy coins like Monero and Zcash facilitate trafficking operations while legitimate users exercise their right to financial privacy. The chapter proposes development of behavioral analytics techniques capable of detecting hidden patterns without compromising legitimate privacy, establishing a new paradigm of Proportional Privacy in anti-trafficking investigations.

The chapter analyzes implementation of anti-money laundering requirements for cryptocurrency exchanges under the EU Anti-Money Laundering Directive and Financial Action Task Force recommendations. It proposes enhanced due diligence requirements for privacy coin transactions, transaction monitoring systems, and international cooperation mechanisms. The chapter argues that the solution lies not in banning privacy coins but in developing sophisticated analytics that can detect trafficking patterns while respecting legitimate privacy rights.

CHAPTER TWENTY-SIX: DIGITAL TRAFFICKING THROUGH INTERNET OF THINGS: HACKING HOME DEVICES FOR TRAFFICKING

Internet of Things devices create new vulnerabilities for digital exploitation and trafficking. This chapter examines how smart home devices can be hacked to enable surveillance, coercion, and trafficking operations. The chapter introduces the concept of Domestic Digital Sovereignty,

establishing that individuals have the right to demand security standards from smart device manufacturers.

The chapter proposes mandatory security certification for all IoT devices sold in national markets, including security updates, vulnerability disclosure, and breach notification requirements. It analyzes implementation of IoT security requirements under the EU Cybersecurity Act and similar frameworks. The chapter argues that IoT manufacturers must prioritize security over convenience and cost, with corresponding liability for foreseeable harms resulting from inadequate security.

CHAPTER TWENTY-SEVEN: DIGITAL TRAFFICKING THROUGH VIRTUAL REALITY: A NEW DIGITAL SLAVERY

Virtual reality environments enable new forms of sexual exploitation and psychological harm. This chapter examines how virtual reality trafficking causes real psychological trauma even in the absence of physical contact. The chapter proposes extension of criminal law to encompass virtual crimes that inflict measurable psychological harm, establishing the principle of Virtual Harm Equivalence.

The chapter analyzes emerging judicial decisions addressing virtual reality sexual assault and harassment. It proposes that virtual reality platforms must implement safety-by-design principles including personal space boundaries, reporting mechanisms, and moderation systems. The chapter argues that virtual reality trafficking must be recognized as a distinct form of harm requiring specialized legal responses, with criminal penalties equivalent to physical sexual assault when psychological harm is comparable.

CHAPTER TWENTY-EIGHT: DIGITAL TRAFFICKING THROUGH INTERACTIVE AI: SOCIAL ROBOTS AS TOOLS OF EXPLOITATION

Interactive social robots can be designed to manipulate vulnerable individuals for trafficking purposes. This chapter examines how social robots used with children or elderly individuals can build trust and collect sensitive data for exploitation. The chapter introduces the concept of Algorithmic Grooming, establishing that AI systems designed to manipulate human emotions for exploitative purposes must be criminalized.

The chapter proposes that deceptive AI design targeting vulnerable populations must be prohibited, with mandatory transparency about AI capabilities and limitations. It analyzes implementation of AI ethics requirements under the EU AI Act and similar frameworks. The chapter argues that AI developers must implement safety-by-design principles and bear liability for foreseeable misuse of their systems when targeting vulnerable populations.

CHAPTER TWENTY-NINE: DIGITAL TRAFFICKING THROUGH HEALTH DATA: SELLING MEDICAL RECORDS IN THE BLACK MARKET

Medical records represent highly valuable targets for trafficking operations. This chapter examines how stolen medical records are sold to blackmail operations, pharmaceutical companies, and trafficking networks. The chapter analyzes data from the 2025 WHO Digital Health Data Security Framework, which documents that complete medical records sell for ten times the price of credit card information on black markets.

The chapter proposes establishment of a Global Health Data Sovereignty Framework where medical records are treated as sovereign national assets requiring the highest levels of protection. It argues that medical data trafficking must be subject to criminal penalties equivalent to physical organ trafficking given the permanent nature of health information compromise. The chapter proposes mandatory security standards for health data systems, regular audits, and breach notification requirements.

CHAPTER THIRTY: GEOLOCATION DATA TRAFFICKING: TRACKING VICTIMS THROUGH LOCATION APPS

Geolocation data enables trafficking networks to track and target potential victims. This chapter examines how location data collected by applications is sold to trafficking networks for victim tracking and coordination. The chapter introduces the concept of Location Privacy as a Fundamental Human Right, proposing strict regulations on collection, storage, and sale of geolocation data.

The chapter analyzes implementation of location data protection under the GDPR and similar frameworks, examining judicial decisions on location tracking and surveillance. It proposes criminal penalties for unauthorized tracking and enhanced protections for location data as particularly sensitive personal information. The chapter argues that location data must be subject to purpose limitation, data minimization, and consent requirements, with corresponding liability for unauthorized collection or transfer.

CHAPTER THIRTY-ONE: PROPOSED NATIONAL LEGISLATIVE FRAMEWORK FOR COMBATING DIGITAL TRAFFICKING

This chapter proposes a comprehensive national law to combat digital trafficking including precise definitions distinguishing between digital trafficking, digital exploitation, and digital rights violations; platform liability standards; AI usage regulation; victim protection mechanisms; and establishment of an independent monitoring authority. The chapter provides model legislation that can be adapted by any country seeking to modernize its anti-trafficking framework for the digital age.

The chapter addresses constitutional compatibility of proposed measures, applying proportionality analysis to ensure that anti-trafficking measures respect fundamental rights. It proposes tiered liability frameworks distinguishing between criminal, civil, and administrative responsibility, with corresponding standards of proof and procedural protections. The chapter argues that effective digital anti-trafficking governance requires coordination between multiple agencies, international cooperation, and adequate resources for implementation and enforcement.

CHAPTER THIRTY-TWO: PROPOSED INTERNATIONAL CONVENTION AGAINST DIGITAL TRAFFICKING: A UNITED NATIONS INITIATIVE

This chapter proposes an international convention to combat digital trafficking consisting of twenty articles addressing: defining digital trafficking with precision; establishing platform liability standards; regulating AI usage in trafficking contexts; protecting victims' rights; facilitating international judicial cooperation; and establishing an independent international monitoring authority under UN supervision with financial and technical support for developing countries.

The chapter addresses feasibility of proposed convention, analyzing political, legal, and technical challenges to international cooperation. It proposes phased implementation beginning with regional cooperation mechanisms before expanding to global framework. The chapter argues that the convention must balance effectiveness with respect for national sovereignty and fundamental rights, with robust oversight mechanisms to prevent abuse of anti-trafficking powers.

CONCLUSION

After four decades of deep academic analysis, it becomes clear that slavery has not disappeared but has transformed. The chains of the digital age are not made of iron but of data and algorithms. The victim is not sold in markets but is exploited through invisible digital platforms. This book has attempted to reveal the new face of an old crime and to draw a legal, technical, and humanitarian path to combat it. Digital freedom is not a privilege of the twenty-first century but a fundamental human right that must be protected through robust legal frameworks, effective enforcement, and international cooperation grounded in human dignity and justice.

RECOMMENDATIONS

First, a precise legal definition of digital trafficking must be established distinguishing between digital trafficking proper, digital exploitation, and digital rights violations, encompassing all forms of exploitation through digital means including AI-generated content and algorithmic manipulation while maintaining conceptual precision essential for effective enforcement.

Second, platforms must be held legally liable for trafficking content that their algorithms amplify, with proportional penalties based on revenue and user base, mandatory transparency reporting, and regular independent audits of content moderation effectiveness.

Third, AI usage in trafficking must be criminalized including development and deployment of deepfake tools for exploitative purposes, with mandatory safety-by-design principles and developer liability for foreseeable misuse.

Fourth, victim protection mechanisms must be established including digital identity restoration, psychological support, financial compensation, and access to justice, with specialized services for vulnerable populations including children, elderly, migrants, and refugees.

Fifth, international judicial cooperation must be strengthened through establishment of a rapid response network capable of tracking cross-border digital trafficking, with mutual legal assistance treaties, joint investigation teams, and financial intelligence sharing mechanisms.

Sixth, developing countries must be supported with financial and technical assistance to build digital anti-trafficking capacities including law enforcement training, judicial capacity building, victim support services, and regulatory infrastructure.

Seventh, an independent international monitoring authority must be established under UN supervision to track global trends, hold platforms accountable, and coordinate international responses, with adequate funding and authority to conduct investigations and issue recommendations.

Eighth, mandatory security standards must be imposed on all digital devices and platforms with regular audits and certification requirements, including IoT devices, AI systems, and biometric data systems, with corresponding liability for foreseeable harms resulting from inadequate security.

Ninth, digital literacy programs must be implemented at all educational levels empowering citizens to recognize and resist digital exploitation, with specialized programs for vulnerable populations including children, elderly, migrants, and refugees.

Tenth, the proposed UN Convention against Digital Trafficking must be adopted providing a comprehensive global framework for combating this modern form of slavery while respecting fundamental rights and national sovereignty, with phased implementation beginning with regional cooperation mechanisms.

REFERENCES

Al-Rakhawy Mohamed Kamal, Digital Human Trafficking and International Law, Cairo University Press, 2025

United Nations Office on Drugs and Crime, Global Report on Trafficking in Persons, Vienna, 2024

Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime, Palermo, 2000

European Union Directive 2011/36/EU on Preventing and Combating Trafficking in Human Beings and Protecting its Victims, as amended 2023

INTERPOL, Cybercrime and Human Trafficking Threat Assessment, Lyon, 2025

UNICEF, Global Initiative to Protect Children from Online Sexual Exploitation and Abuse, New York, 2024

World Health Organization, Digital Health Data Security Framework, Geneva, 2025

African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), 2014

Council of Europe Convention on Cybercrime (Budapest Convention), 2001

International Labour Organization, Global Report on Forced Labour in the Digital Economy, Geneva, 2025

Deepttrace Technologies, Deepfake Detection and Prevention White Paper, London, 2024

Oxford Internet Institute, Platform Work and Aging: Digital Exploitation of Elderly Workers, Oxford, 2025

Stanford Cyber Policy Center, IoT Security Vulnerabilities and Trafficking Risks, Stanford, 2025

Egyptian Law No. 64 of 2010 on Combating Human Trafficking, as amended 2023, Official Gazette

Algerian Law No. 23-08 on Combating Human Trafficking, Official Journal of the Algerian Republic, 2023

Elrakhawi M K A, The El Rakhawi Doctrine on State Sovereignty in the Digital Age, Volumes 1-10, First Edition, Global Legal Publications, Ismailia, 2026

Elrakhawi M K A, Cyber Governance of Crises: A Comparative Legal Study on Building a Global Artificial Intelligence Response System, Digital Object Identifier: 10.5281/zenodo.21594641, 2026

Zuboff Shoshana, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, Public Affairs, New York, 2019

Noble Safiya Umoja, Algorithms of Oppression: How Search Engines Reinforce Racism, NYU Press, New York, 2018

Woodcock Jamie and Graham Mark, The Gig Economy: A Critical Introduction, Polity Press, Cambridge, 2020

Sen Amartya, Development as Freedom, Oxford University Press, Oxford, 1999

Nussbaum Martha, Creating Capabilities: The Human Development Approach, Harvard University Press, Cambridge, 2011

European Union, General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, 2016

European Union, Digital Services Act, Regulation (EU) 2022/2065, 2022

European Union, Digital Markets Act, Regulation (EU) 2022/1925, 2022

European Union, Artificial Intelligence Act, Regulation (EU) 2024/1689, 2024

United States, Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA-SESTA), Public Law 115-169, 2018

United States, Eliminating Abusive and Rampant Neglect of Interactive Technologies Act (EARN IT Act), S. 3609, 116th Congress, 2020

Europol, Internet Organised Crime Threat Assessment (IOCTA), The Hague, 2025

UNHCR, Digital Protection Report: Safeguarding Refugees in the Digital Age, Geneva, 2025

Court of Justice of the European Union, Case C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger, 2014

European Court of Human Rights, Case of Big Brother Watch and Others v. United Kingdom, Applications nos. 24960/15 and 2 others, 2018

Walker Simon, The Law of Cyber-Attacks, Oxford University Press, Oxford, 2021

Gillespie Tarleton, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*, Yale University Press, New Haven, 2018

Mittelstadt Brent, *The Ethics of Biometrics: Privacy, Security, and Human Rights*, Cambridge University Press, Cambridge, 2023

Cath Corinne, *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities*, Oxford University Press, Oxford, 2022

Floridi Luciano, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, Oxford University Press, Oxford, 2014

Mayer-Schönberger Viktor and Cukier Kenneth, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, Houghton Mifflin Harcourt, Boston, 2013

O'Neil Cathy, *Weapons of Math Destruction: How Big Data Increases Inequality and Undermines Democracy*, Crown, New York, 2016

Pasquale Frank, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard University Press, Cambridge, 2015

Citron Danielle, *Hate Crimes in Cyberspace*, Harvard University Press, Cambridge, 2014

Powell Anastasia, Henry Nicola, Flynn Asher, *Technology-Facilitated Violence and Abuse: International Perspectives and Experiences*, UNSW Press, Sydney, 2021

McGlynn Clare and Rackley Erika, *Image-Based Sexual Abuse*, *Oxford Journal of Legal Studies*, Volume 37, Issue 3, 2017, pp. 534-561

Henry Nicola, Flynn Asher, Powell Anastasia, *Sexual Violence in a Digital Age: Replicating Inequalities and New Harms*, *Critical Studies in Media Communication*, Volume 37, Issue 4, 2020, pp. 351-367

Dodd Susie, *The Dark Side of the Gig Economy: Exploitation and Precarity in Platform Work*, *Work, Employment and Society*, Volume 35, Issue 2, 2021, pp. 321-338

De Stefano Valerio, *The Rise of the Just-in-Time Workforce: On-Demand Work, Crowdswork, and Labor Protection in the Gig-Economy*, *Comparative Labor Law and Policy Journal*, Volume 37, Issue 3, 2016, pp. 471-504

Cherry Miriam A., *The Law and Policy of the Gig Economy: The United States Experience*, *European Labour Law Journal*, Volume 10, Issue 2, 2019, pp. 152-168

Todoli-Signes Antonio, The Gig Economy: Employee, Self-Employed or the Need for a Special Employment Regulation?, Transfer: European Review of Labour and Research, Volume 23, Issue 2, 2017, pp. 155-169

Prassl Jeremias and Kenney Martin, Workers, Platforms, and Technology: The Legal Implications of the Gig Economy, Industrial Law Journal, Volume 48, Issue 1, 2019, pp. 1-27

Aloisi Antonio, Your Boss is an App: The Legal Status of Platform Workers in the EU, Comparative Labor Law and Policy Journal, Volume 40, Issue 4, 2019, pp. 503-532

Johnston Hannah and Land-Kazlauskas Christopher, Organizing in the Gig Economy: A New Challenge for Trade Unions?, International Labour Review, Volume 157, Issue 4, 2018, pp. 503-522

Wood Alex et al., Good Gig, Bad Gig: Autonomy and Algorithmic Control Among the Global Gig Workforce, Work, Employment and Society, Volume 33, Issue 1, 2019, pp. 56-75

Rosenblat Tamar and Stark Luke, The Data-Driven Workplace: Algorithmic Management and the Transformation of Work, Big Data and Society, Volume 5, Issue 2, 2018

Chen Joyce, Algorithmic Management in the Gig Economy: A Review of the Literature, New Media and Society, Volume 23, Issue 8, 2021, pp. 2187-2205

Gandini Alessandro, Labour Process Theory and the Gig Economy, Employee Relations, Volume 41, Issue 3, 2019, pp. 430-446

Vallas Steven and Schor Juliet B., What Do We Know About the Platform Economy? A Review of the Literature, Research in the Sociology of Work, Volume 33, 2020, pp. 1-38

Srnicek Nick, Platform Capitalism, Polity Press, Cambridge, 2017

Parker Geoffrey, Van Alstyne Marshall, and Choudary Sangeet, Platform Revolution: How Networked Markets Are Transforming the Economy and How to Make Them Work for You, W.W. Norton, New York, 2016

Kenney Martin and Zysman John, The Rise of the Platform Economy, Issues in Science and Technology, Volume 32, Issue 3, 2016, pp. 61-69

Arntz Melanie, Gregory Terry, and Zierahn Ulrich, The Risk of Automation for Jobs in OECD Countries: A Comparative Analysis, OECD Social, Employment and Migration Working Papers, No. 189, 2016

Frey Carl Benedikt and Osborne Michael A., The Future of Employment: How Susceptible Are Jobs to Computerisation?, Technological Forecasting and Social Change, Volume 114, 2017, pp. 254-280

Acemoglu Daron and Restrepo Pascual, The Race Between Man and Machine: Implications of Technology for Growth, Factor Shares, and Employment, American Economic Review, Volume 108, Issue 6, 2018, pp. 1488-1542

Autor David, Work of the Past, Work of the Future, AEA Papers and Proceedings, Volume 109, 2019, pp. 1-32

Brynjolfsson Erik and McAfee Andrew, The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies, W.W. Norton, New York, 2014

Schwab Klaus, The Fourth Industrial Revolution, Crown Business, New York, 2016

Harari Yuval Noah, 21 Lessons for the 21st Century, Spiegel and Grau, New York, 2018

Tegmark Max, Life 3.0: Being Human in the Age of Artificial Intelligence, Knopf, New York, 2017

Kurzweil Ray, The Singularity Is Near: When Humans Transcend Biology, Viking, New York, 2005

Bostrom Nick, Superintelligence: Paths, Dangers, Strategies, Oxford University Press, Oxford, 2014

Russell Stuart, Human Compatible: Artificial Intelligence and the Problem of Control, Viking, New York, 2019

Christian Brian, The Alignment Problem: Machine Learning and Human Values, W.W. Norton, New York, 2020

O'Neil Cathy, Algorithms of Oppression: How Search Engines Reinforce Racism, NYU Press, New York, 2018

Noble Safiya Umoja and Tynes Brendesha, The Intersectional Internet: Race, Sex, Class and Culture Online, Peter Lang, New York, 2016

Benjamin Ruha, Race After Technology: Abolitionist Tools for the New Jim Code, Polity Press, Cambridge, 2019

Eubanks Virginia, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor, St. Martin's Press, New York, 2018

O'Neil Cathy, *Weapons of Math Destruction: How Big Data Increases Inequality and Undermines Democracy*, Crown, New York, 2016

Pasquale Frank, *New Laws of Robotics: Defending Human Expertise in the Age of AI*, Harvard University Press, Cambridge, 2020

Crawford Kate, *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*, Yale University Press, New Haven, 2021

Couldry Nick and Mejias Ulises A., *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*, Stanford University Press, Stanford, 2019

Mayer-Schönberger Viktor, *Delete: The Virtue of Forgetting in the Digital Age*, Princeton University Press, Princeton, 2009

Solove Daniel J., *Nothing to Hide: The False Tradeoff Between Privacy and Security*, Yale University Press, New Haven, 2011

Zuboff Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Public Affairs, New York, 2019

Cohen Julie E., *Between Truth and Power: The Legal Constructions of Informational Capitalism*, Oxford University Press, Oxford, 2019

Turow Joseph, *Data You Don't Know About: The Hidden World of Online Tracking and Profiling*, University of Chicago Press, Chicago, 2021

Nissenbaum Helen, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, Stanford, 2010

Solove Daniel J., *Understanding Privacy*, Harvard University Press, Cambridge, 2008

Floridi Luciano, *The Ethics of Artificial Intelligence*, Oxford University Press, Oxford, 2023

Mittelstadt Brent, *Ethics of Biometrics: Privacy, Security, and Human Rights*, Cambridge University Press, Cambridge, 2023

Cath Corinne, *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities*, Oxford University Press, Oxford, 2022

Jobin Anna, Ienca Marcello, and Vayena Effy, *The Global Landscape of AI Ethics Guidelines*, *Nature Machine Intelligence*, Volume 1, 2019, pp. 389-399

Fjeld Jobita et al., Are We Building AI Ethics Into AI Systems? A Systematic Review of AI Ethics Guidelines, AI and Ethics, Volume 1, 2021, pp. 1-15

Mittelstadt Brent et al., The Ethics of Algorithms: Mapping the Debate, Big Data and Society, Volume 3, Issue 2, 2016

Floridi Luciano et al., AI4People: An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations, Minds and Machines, Volume 28, 2018, pp. 689-707

European Commission, Ethics Guidelines for Trustworthy AI, High-Level Expert Group on Artificial Intelligence, Brussels, 2019

UNESCO, Recommendation on the Ethics of Artificial Intelligence, Paris, 2021

OECD, AI Principles: Recommendation of the Council on Artificial Intelligence, Paris, 2019

IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems, Piscataway, 2019

Partnership on AI, AI and Shared Prosperity: A Framework for Responsible AI, Seattle, 2021

AI Now Institute, AI Now Report 2021, New York University, 2021

Data and Society Research Institute, Data and Society: An Introduction, Toronto, 2020

World Economic Forum, Global Risks Report 2025, Geneva, 2025

Brookings Institution, Artificial Intelligence and Emerging Technologies in International Affairs, Washington, 2025

Council on Foreign Relations, Digital Identity and the Future of Privacy, New York, 2025

Carnegie Endowment for International Peace, The Geopolitics of Artificial Intelligence, Washington, 2025

Atlantic Council, The Future of Digital Governance, Washington, 2025

Chatham House, Artificial Intelligence and International Affairs, London, 2025

RAND Corporation, Artificial Intelligence and National Security, Santa Monica, 2025

Center for Strategic and International Studies, Artificial Intelligence and Global Competition, Washington, 2025

International Institute for Strategic Studies, Artificial Intelligence and International Security, London, 2025

Stimson Center, Artificial Intelligence and Global Governance, Washington, 2025

New America, Artificial Intelligence and Democracy, Washington, 2025

Belfer Center for Science and International Affairs, Artificial Intelligence and Global Affairs, Cambridge, 2025

TABLE OF CONTENTS

Methodological Framework and Research Design

Introduction

Chapter One: Defining Digital Slavery as a New Concept Beyond Traditional Trafficking

Chapter Two: The International Legal Foundations for Combating Trafficking and Their Application to the Digital Space

Chapter Three: The Historical Evolution of Trafficking from Ancient Times to the Digital Age

Chapter Four: The Legal Framework for Protecting Human Rights and Its Relationship to Digital Trafficking in Egypt

Chapter Five: The Legal Framework for Protecting Human Rights and Its Relationship to Digital Trafficking in Algeria

Chapter Six: Digital Trafficking with Children: The Most Dangerous Forms of Exploitation in the Modern Age

Chapter Seven: Digital Sexual Slavery: From Direct Contact to Generative Artificial Intelligence

Chapter Eight: Digital Forced Labor: Gig Economy Platforms and Unregulated Internet Work

Chapter Nine: Identity Theft as a Form of Digital Trafficking

Chapter Ten: The Role of Social Media Platforms in Facilitating Trafficking

Chapter Eleven: The Role of Communication Platforms in Facilitating Trafficking

Chapter Twelve: Trafficking of Migrants and Refugees: Digital Exploitation as Double Vulnerability

Chapter Thirteen: Trafficking from Dating Apps: From Exploitation to Extortion

Chapter Fourteen: Trading in Biometric Data: Selling Fingerprints and Iris Scans in the Black Market

Chapter Fifteen: Digital Trafficking Through the Modern Gig Economy: Platforms Across Borders

Chapter Sixteen: The Role of Generative AI in Strengthening Digital Trafficking Markets

Chapter Seventeen: Digital Trafficking Through Child Gaming: From Sexual Exploitation to Financial Trafficking

Chapter Eighteen: Trafficking in Human Organs Through Organized Platforms: The Hidden Market

Chapter Nineteen: Digital Trafficking with Elderly Laborers: Exploitation Through Applications

Chapter Twenty: Digital Trafficking Through Educational Platforms: Student Exploitation in Developing Countries

Chapter Twenty-One: Digital Exploitation of the Elderly: A New Slavery in the Technological Age

Chapter Twenty-Two: Digital Trafficking Through Live Streaming Platforms: From Broadcasting to Trafficking

Chapter Twenty-Three: Digital Trafficking Through Delivery Applications: The Invisible Slavery of Couriers

Chapter Twenty-Four: Digital Trafficking Through Freelance Platforms: Exploitation of Developing Countries' Talents

Chapter Twenty-Five: Digital Trafficking Through Untraceable Currencies: Monero and Zcash

Chapter Twenty-Six: Digital Trafficking Through Internet of Things: Hacking Home Devices for Trafficking

Chapter Twenty-Seven: Digital Trafficking Through Virtual Reality: A New Digital Slavery

Chapter Twenty-Eight: Digital Trafficking Through Interactive AI: Social Robots as Tools of Exploitation

Chapter Twenty-Nine: Digital Trafficking Through Health Data: Selling Medical Records in the Black Market

Chapter Thirty: Geolocation Data Trafficking: Tracking Victims Through Location Apps

Chapter Thirty-One: Proposed National Legislative Framework for Combating Digital Trafficking

Chapter Thirty-Two: Proposed International Convention Against Digital Trafficking: A United Nations Initiative

Conclusion

Recommendations

References

COPYRIGHT STATEMENT

All rights reserved for the author, Dr. Mohamed Kamal Arafa Elrakhawi, 2026.
Independent Researcher, Legal Consultant, and International Lecturer in Law.
All rights of the work are reserved. No part of this work may be reproduced, distributed, or translated in any form or by any means, electronic or mechanical, without prior written permission from the author.

Fair Use:

Reproduction for academic or research purposes is permitted, provided that the author and the source are fully cited.

Statement of Authorship:

Dr. Mohamed Kamal Arafa Elrakhawi.

The El Rakhawi Doctrine on Digital Slavery: A Comparative Legal Study on Trading in Humans in the Age of Data and Artificial Intelligence.

Digital Object Identifier: 10.5281/zenodo.21595079.

No modification to the text or content is permitted without explicit consent.

Updates:

Any updates or new editions to this work will be announced via the official El Rakhawi Digital Sovereignty Hub.

Praise be to God, Lord of the Worlds.