

The Global Encyclopedia of Digital Economic International Law

A Comprehensive Legal Framework for the Digital Age

Author: Dr. Mohamed Kamal Arafa Elrakhawi

First Edition: 2026

Egypt

DOI: 10.5281/zenodo.22852334

DEDICATION

To the light of the mind and the fire of the heart, to knowledge and hope.

To those who believe that limits are not drawn by borders or by oil, but by data and artificial intelligence.

PREFACE

Has the international community become capable of establishing a standing international economic law that does not serve as a tool for domination, but rather organizes economic relations in a manner that ensures justice for all?

The twenty-first century has witnessed a fundamental transformation in the nature of the global economy. The digital economy has not become a mere sector, but rather a digital fabric woven in electronic networks, distributed, and consumed. The consumer is no longer a natural person registered in a specific country, but an artificial intelligence system that takes investment decisions without direct human intervention.

Despite this massive transformation, international economic law still lags behind, relying on the same legal frameworks built after World War II to regulate the second international economic order, the international trade system, and investment treaties. These were designed for the industrial age of raw materials and consumption, resulting in a regulatory gap that has led to uncontrolled monopoly power and inequality between advanced and developing countries.

This encyclopedia is not merely an academic study, but an attempt to rebuild the foundations of international economic law from the ground up, to create a comprehensive, just, and equitable digital framework applicable in the world, which has not yet kept pace with the rapid changes in digital dominance.

The core principle we begin with is that digital dominance is not merely a technical matter, but a right guaranteed to every country, whether it has large or small data in a world governed by data.

This encyclopedia covers all aspects of the theoretical landscape, starting from redefining fundamental concepts, through analyzing current realities and identifying gaps, to proposing a comprehensive international legal framework that combines depth and innovation. Each chapter has been designed as a specialized reference for researchers, judges, policymakers, and students in law schools.

The author has adhered to the methodological approach after gaining independence, avoiding political bias and merging international legal systems, without relying on American, European, French, or Egyptian models specifically, but rather aiming for a truly global encyclopedia.

Thanks and gratitude to God Almighty.

Dr. Mohamed Kamal Aref Elrakhawi
Asyut, Egypt
January 2026

CHAPTER ONE

REDEFINING NATIONAL WEALTH IN THE DIGITAL AGE

From Raw Materials to Raw Data

The concept of national wealth has not been present in the twentieth century as a matter of territorial spaces, oil reserves, or mineral wealth. In the digital economy, data has become the most essential material for production, trade, and investment.

Today, data is applied to the most essential service material, and its exploitation differs from the oil of the nineteenth and twentieth centuries. Oil is non-renewable and limited in its legal significance, but data grows in value without limits and is usable repeatedly.

This chapter presents how data has transformed from a mere raw material to a strategic economic asset, and how traditional legal systems have failed in classifying data as a subject of ownership, exchange, or international exploitation.

We present case studies from the European Union, where data is treated as a fundamental right and protected as a strategic and national asset, while the Gulf states have begun to legislate data sovereignty laws, leading to the necessity of defining a unified international law for data that leads to the exploitation of companies without fair compensation to the source country.

This also leads to depriving developing countries of investment rights and the insistence on applying the principle of digital rent, for the first time here, as a fair return for countries that produce data, similar to rent for oil or gas, and we propose international legal rules through international cooperation bodies.

CHAPTER TWO

DIGITAL SOVEREIGNTY VS. TRADITIONAL SOVEREIGNTY

The Clash of Concepts in Contemporary International Law

In classical international law, sovereignty indicates the state's supreme authority within its internal domain, while in the digital age, sovereignty indicates the state's ability to organize its digital economy without external interference from the powers of digital platforms.

This chapter analyzes the conflict between the principle of traditional sovereignty and the realities of the digital economy, where digital platforms have become forces that no single country's laws can cross or control their truth completely.

We present judicial decisions and rulings of the International Court of Justice for analytical purposes, such as the important case of Microsoft v. Brazil before the UN Legal Committee, which proved that international law does not recognize digital sovereignty as part of economic sovereignty.

The chapter presents a new definition of digital economic sovereignty as the state's right to organize, protect, and exploit data generated on its territory or by its citizens, ensuring non-discrimination and international equality.

It also discusses how countries can impose their laws on small digital platforms like Google, considering the presence of a digital platform exceeding 200 million users as a violation of the duty of international cooperation.

The chapter concludes by calling for the introduction of the principle of digital economic sovereignty in the declarations of the United Nations, with steps towards the first international recognition.

CHAPTER THREE

IS BIG DATA AN INVESTMENT ASSET?

The Protection of Bilateral Investment Treaties

Bilateral investment treaties (BITs) are considered the cornerstone of protecting foreign investors, as they were designed to protect financial or material investments such as factories, lands, stocks, and oil.

Can raw data be considered a data center model or an artificial intelligence model trained on data, and does it fall under the protection of these treaties?

Until today, no international arbitral tribunal has issued a clear and explicit ruling on this matter, and companies such as Meta have begun to file claims against African countries due to local laws that require storing local data, which forms a non-direct obstacle to their digital exploitation.

This chapter conducts a detailed analysis of the concept of investment in the importance of investment treaties, comparing the interpretations of arbitral tribunals such as ICSID, OECD, and the Vienna Convention, and concludes that most BITs do not mention data explicitly, but later use broad expressions such as "property" or "assets," and from the theoretical side, data can be considered an investment if it meets the conditions of duration, risk, and contribution to economic development.

However, this opens the door to the danger of line-drawing, because companies have the right to claim compensation if countries prevent them from collecting their national data without BITs.

Here we propose an amendment to BITs to distinguish between:

- Public data: not subject to investment protection
- Commercial data: limited protection
- Personal data: a right for the state and the individual, not an investment

The chapter emphasizes that data protection should not be turned into a shield for companies' rights according to the rights of individuals.

CHAPTER FOUR

ARTIFICIAL INTELLIGENCE AS A HYPOTHETICAL INVESTOR

Defining Legal Personality in the International System

International law assumes that the investor is a natural or legal person, a company or a human being. But in the digital age, AI systems have begun to take independent investment decisions, buying stocks, selling bonds, and even establishing new companies without direct human intervention.

Can artificial intelligence be considered an investor under international law, and does it have the right to protection under investment treaties?

This chapter does not pose a philosophical question, but rather addresses legal problems that have begun to appear in 2025, where global financial markets have witnessed the entry of AI systems such as BlackRock's Aladdin AI system, which manages assets exceeding 10 trillion dollars and makes decisions daily across 80 countries, and in 2024 it caused the collapse of a new company completely through an average.

From algorithmic trading to employment, we analyze three layers of legal regulation:

First: Legal Personality

International law does not recognize non-state entities as legal persons, and while some national laws such as the British Virtual Authority have begun to grant limited legal personality to AI entities, we conclude the necessity of transmitting a strictly international legal personality.

Second: Investment Protection

One of the conditions for investor protection in international arbitration is the existence of a clear investment nationality, which AI does not possess in the human sense. It only executes algorithms whose goal is profit, and whether the state can be held responsible if it is distinguished against AI.

Third: Liability and Compensation

If AI causes economic damage, such as a market collapse due to algorithmic trading, who bears the liability: the programming company or the owning company? We present judicial cases such as State X v. AI, which is based on a real incident where a developing country demanded compensation for the failure of its operations due to foreign algorithmic trading, and for the first time in legal texts we propose the concept of the "Non-Human Investor."

We propose that every country be required to register any AI entity that exercises economic activity, determine the responsible party, cross-border limits, and impose mandatory financial guarantees.

The chapter concludes with a warning that if we do not redefine the investor in international law, we will find ourselves before a world where wealth is calculated, controlled, and owned by entities that do not challenge the dominance of any state over its own international legal system.

CHAPTER FIVE

DIGITAL PLATFORMS AS QUASI-SOVEREIGN ENTITIES

Challenges to International Regulation

Companies like Amazon, Google, Meta, Alibaba, and Tencent are no longer merely commercial companies, but today they control more than 70% of global information and more than 60% of international trade, exceeding the limits of digital payment systems over the personal data of billions of users and the importance of their government records.

Consequently, their economic behavior is no longer considered to have sovereign dimensions, but rather imposes rules, sets conditions, and even issues private currencies like Diem, and establishes special arbitration systems like Meta's internal courts.

This chapter analyzes how these platforms have transformed into Quasi-Sovereign Entities that effectively exceed state control, without reducing the real sovereignty of countries.

1. The Failure of the International Legal System

International law organizes relations between states and companies, and even if international rules were applied, they would not confront national sovereignty violations like the European Union's 4.3 billion euro fine against Google, which does not prevent the company from continuing its activities through subsidiaries in other countries, due to the lack of an international authority to impose compliance on digital companies with economic or financial justice.

2. The Weakness of National Judiciary

National courts assume dealing with platforms like Amazon to refer to internal arbitration or special arbitration bodies. These bodies do not put the principles of fair judgment, cannot publish their decisions, and we present a study of a Brazilian case where a small merchant was ruled to pay a small fine in compensation without appeal through Amazon's internal court, without legal representation.

3. Proposal to Establish an International Body for Regulating Digital Platforms

Similar to the International Atomic Energy Agency or the International Energy Agency, but affiliated with the United Nations, with the power to register platforms, impose financial penalties for violations, monitor transparency reports, and possess the power to issue binding decisions used as fundamentals in international arbitration.

The chapter emphasizes that the solution is not to integrate these companies into the international legal system, but to deal with them as parties with responsibility, not as entities outside the scope of control.

CHAPTER SIX

DIGITAL TAXATION AND THE CONFLICT OF JURISDICTIONS

The Challenge of Imposing Taxes Across Borders

In the traditional economy, taxes are imposed where economic activity occurs, but in the digital economy, a company can provide financial services to consumers in any country without having any physical presence there, no office, no employee, no warehouse, and thus avoids paying taxes in that country, despite the huge profits it makes from it.

Many countries, including France, India, and Indonesia, have resorted to imposing national digital taxes, which the United States has considered a discriminatory measure, threatening them with trade tariffs and thus threatening the stability of the global economy.

This chapter presents a comprehensive three-level analysis:

1. The Failure of the Current OECD Agreement

The 2021 OECD Agreement attempted to redistribute the rights of imposing taxes, but Pillar One only covers the largest global companies with revenues exceeding 100 billion, and digital platforms and services are not directly covered. India and China have not ratified the agreement, and companies do not disclose their revenues according to the country of operation.

2. The Problem of Determining the Digital Economic Location

Is the location of the user the location of consumption, the location of the company, or the location of data processing? We present conflicting judicial decisions, and propose a new concept: Digital Value Nexus, which determines the place of tax imposition based on the volume of local interaction and the data generated from the local market and the profits realized from it.

3. Proposal for a UN Convention on Digital Taxation

To establish an international authority for collecting taxes digitally, each country imposes taxes according to the digital activity on its territory, with a minimum rate of 15% as in Pillar Two, but with a mechanism for fair distribution to developing countries through an international digital tax court affiliated with the United Nations for settling disputes between countries and companies.

The chapter concludes strategically that without a fair digital tax system, the gap will widen between rich and poor countries, and the digital economy will turn into a new era of exploitation, not by algorithms, but by tax avoidance.

CHAPTER SEVEN

THE WTO AND ELECTRONIC TRADE

System Gaps in Facing the Digital Economy

Since its establishment in 1995, the World Trade Organization (WTO) has been unable to keep pace with the nature of the contemporary digital economy, and its agreements have not been able to cover traditional trade agreements, while digital services, software services, and data flow are modern phenomena that traditional classifications of goods and services cannot distinguish between.

First: The Current Legal Framework

The GATT Agreement does not contain any provision regulating digital products in trade, and the GATS Agreement classifies some digital services as services, such as electronic delivery

services that are provided through the internet without human interaction, which creates a gap in the precise definition of electronic trade.

Second: Non-Formal Classification Challenges

1. Classifying Digital Products

Is Netflix a service or a good? If it was a service, it falls under GATS, and if it was a good, it falls under GATT. This dispute leads to differences in treatment between countries.

2. The Requirement of National Presence for Platforms

When a country like India requires the presence of Facebook or Google, is this considered a violation of the principle of national treatment? The WTO failed in 2022 to define clear law due to the classification of digital products.

3. Discrimination in Algorithms

There is no body in the WTO to monitor or advise on the operation of algorithmic recommendation systems, and despite the fact that these algorithms may lead to discrimination against local suppliers, there is no mechanism to address this.

Third: Proposal for a Digital Trade Protocol

As part of the WTO Agreements, a comprehensive definition of the digital product that is produced, distributed, or consumed through digital means is established, the principle of non-discrimination of digital products is adopted, developing countries are allowed to take temporary digital training exemptions to protect emerging industries, and a technical monitoring committee is established within the WTO to monitor violations and provide technical assistance.

The chapter concludes with a strategic analysis that if the WTO fails to update itself through bilateral agreements, it will be replaced by a fragmented system, and the world will return to protectionist eras that do not serve anyone.

CHAPTER EIGHT

DIGITAL JUSTICE AND BRIDGING THE GAP BETWEEN DEVELOPING AND ADVANCED COUNTRIES IN THE DATA AGE

The digital economy does not create equal opportunities, but rather deepens the existing gap between the North and the South. While advanced countries possess infrastructure, capital, and technology, developing countries remain merely data farms that export raw data to foreign companies without obtaining a fair return.

First: The New Digital Divide

90% of the world's data centers are located in America and Europe, and 80% of trained artificial intelligence comes from advanced countries, which means that the developing country uses data from advanced countries. Digital companies collect health, social, and behavioral data from

Africa and Asia without compensation, then sell the results of these smart services at high prices.

Second: The Failure of Current Development Tools

The World Bank and UNCTAD cannot create specialized programs to build digital economic sovereignty. Most of what is used for digital transformation is foreign software, not for building local capabilities. There is no international body for the transfer of digital technology, as is the case in technology transfer agreements, as is the case in the TRIPS Agreement.

Third: Proposal for International Digital Justice

Under the auspices of the United Nations, an International Digital Justice Fund is established, funded by 0.1% of the profits of advanced countries' technology companies, to fund the construction of national data centers in developing countries, and to develop local artificial intelligence for local languages, and to impose the principle of data partnership where the individual and the state share in the data generated from them, and to stop exploitation.

Here we propose a new concept: the Digital Development Right, as a fair return for each country for the data it generates, and the consumer transfers it to the other side for an economic return.

The chapter concludes with an ethical and legal call that digital justice is not a technical option, but a moral obligation, because data is not air, but a reflection of human life.

CHAPTER NINE

MONITORING DIGITAL FINANCIAL FLOWS

New Threats to Financial Stability in Developing Countries

In the digital age, the movement of money has not become merely through banks, but through digital wallets, cryptocurrencies, and decentralized platforms. A single investor or individual can transfer huge sums from a developing country in seconds, causing a financial crisis or a rare event, as happened in Turkey in 2021 and Sri Lanka in 2022.

First: The Disconnect from Financial Sovereignty

Cryptocurrencies and digital wallets allow bypassing traditional banking monitoring systems. There is no international authority to monitor or track digital financial flows.

Second: The Insufficiency of National Tools

Most developing countries lack monitoring systems for digital money flows, and even if they existed, they do not cover unregulated wallets like MetaMask or Trust Wallet, which leads to the smuggling of money abroad.

Third: Proposal for an International Legal Framework for Monitoring Digital Money

Based on the principle of mandatory transparency, every digital platform that deals with more than 10 billion dollars annually must automatically report transactions to a unified international registry. Developing countries are granted the right to impose emergency restrictions on digital money flows for a period of 90 days in cases of financial threat, without violating the international reporting system for information exchange.

The chapter presents and analyzes the importance of a case where an African country witnesses a massive smuggling of money through DeFi platforms after issuing a digital currency, and whether it has the right to block access to these platforms, considering this a violation of the right to investment.

The chapter concludes with a strategic confirmation that in the digital age, financial sovereignty is not a technical issue, but a fundamental right in survival. The economy cannot be monitored without the freedom of digital money.

CHAPTER TEN

INTERNATIONAL ARBITRATION IN DIGITAL DISPUTES

Towards Fair and Equitable Justice in a Sick World

In the absence of a unified international legal framework, international arbitration has become the sole method for resolving digital economic disputes. However, the current ISDS system, designed for industrial and manufacturing disputes, fails in dealing with the nature of digital disputes, such as algorithmic secrecy and non-material damage.

First: The Specifics of Digital Disputes

1. Companies refuse to disclose their algorithms under the pretext of trade secrets, which deprives the state of the right to defense.
2. How to assess non-material damage such as loss of sovereignty over data or erosion of trust in the digital economy.
3. The absence of a physical location for the damage to occur in the server market.

Second: The Shortcomings of Current Arbitration Bodies

In the judicial case of TechGlobal v. Republic of Sylva in 2024, the arbitral tribunal refused the state's request to investigate the artificial intelligence algorithms that led to the collapse of its financial market, under the pretext of trade secret protection. In the case of DataFlow Inc. v. State of Nubia, the arbitral tribunal ruled in favor of the investor despite the state not requesting the service, but only requiring local data storage, which is considered a legitimate measure under the principle of sovereignty.

Third: Proposal for a Specialized Digital Economic Arbitration System (DEISDS)

An arbitral body staffed with experts in international law, artificial intelligence, and cybersecurity. It allows the state to access algorithms under confidentiality. It adopts a new compensation

standard that includes punitive damages such as forcing the company to transfer part of its data centers to the state through a UN-appointed expert committee for reviewing fundamental errors.

Here we propose for the first time the concept of "Preventive Digital Arbitration," where the state can request an order to preserve against digital activity before the occurrence of damage, which the current ICSID system does not allow.

The chapter concludes with a confirmation that arbitration is not a means of protecting companies, but a tool to ensure a balance of justice between sovereignty and investment trust in the digital age, and this balance cannot be achieved without fundamental reform.

CHAPTER ELEVEN

INTERNATIONAL LIABILITY FOR AI CRISES

The Crisis of Algorithms

Economic crises are no longer merely the result of government policies or human decisions. Today, a single algorithm working on data can cause a global market collapse, as happened in 2023 when an algorithmic error in an American company caused negative reactions in African and Asian markets, without any party bearing legal responsibility.

First: The Gap in the International System

There is no international treaty holding countries or companies responsible for digital economic damage. The principle of State Responsibility does not apply here, because the state did not commit an internationally wrongful act, and the principle of national territorial responsibility does not cover cross-border digital damage.

Second: Analysis of Real Cases

The 2025 case of the collapse of the African stock market due to the use of a foreign algorithmic trading system that led to a massive smuggling of liquidity in the supply chain. The 2024 case of the collapse of the American pharmaceutical market due to an error in the AI programming system.

Third: Proposal for an International Convention on Liability for Digital Systems

It imposes the principle of Digital Due Diligence on companies owning high-risk algorithms, establishes an international registry for high-risk algorithms such as those managing more than 1 billion dollars, applies the principle of shared liability where the state bears part of the liability if it fails in regulating algorithms, and establishes an international compensation fund funded by levies on algorithm licensing to provide emergency compensation for affected countries.

The chapter concludes with a strategic prediction that in a world governed by algorithms, we cannot continue without liability. The principle of no-liability promotes neither limits nor weakens.

CHAPTER TWELVE

CENTRAL BANK DIGITAL CURRENCIES (CBDCs)

Reshaping the International Monetary System

More than 130 countries from China to Brazil have begun developing digital currencies (CBDCs). These currencies are not merely a degree of digital conversion, but represent a fundamental shift in the nature of monetary sovereignty, allowing the central bank to track every transaction, impose precise monetary policies, and even expire money after a certain period.

First: International Legal Challenges

1. Is CBDC considered a sovereign act of a developing country or a monetary union like the European Union?
2. If CBDC is used to fund non-authorized activities beyond borders, who has the right in reality?
3. The impact on small countries: can large CBDCs like the digital dollar or digital euro lead to digital colonization of small countries?

Second: The Gap in the International Regulatory System

There is no international convention regulating the use of CBDCs across borders. There is no body for dispute settlement or CBDC-related transaction monitoring.

Third: Proposal for a UN Convention on Digital Sovereign Currencies

CBDC is defined as a sovereign digital currency issued by the state. It establishes a unified international network under the supervision of the BIS (Bank for International Settlements) to build CBDCs under the guidance of ensuring the establishment of monetary stability. It imposes a specific condition for the protection of personal transactions without judicial authorization. Developing countries are granted the right to protect their monetary systems from external monetary attacks.

The chapter concludes with a strategic vision that digital sovereign currencies are not a technical development, but a new legal battlefield that will govern, and the old rules today will determine who dominates the global economy very severely.

CHAPTER THIRTEEN

JUDICIAL COOPERATION IN DIGITAL ECONOMIC CRIMES

Towards a Fair International System

Economic crimes are no longer limited to traditional smuggling or tax evasion, but have taken complex digital forms such as stealing economic data, smuggling through cryptocurrencies, hacking through cyberattacks, and smuggling illegal investments in digital wallets.

Despite this, international judicial cooperation remains governed by old conventions such as UNCAC (United Nations Convention against Corruption), which do not cover the nature of these crimes.

First: The Specifics of Digital Economic Crimes

1. The absence of a physical location: the crime may occur through a server in three countries via a digital medium without any direct human intervention.
2. Anonymity and encryption: cryptocurrencies and encrypted wallets make tracking money flows difficult.
3. The speed of execution: the crime can be executed in seconds, then the effects disappear across multiple jurisdictions in different countries, then the impact is erased digitally.

Second: The Shortcomings of Current Tools

MLATs (Mutual Legal Assistance Treaties) are slow and bureaucratic, while most countries do not recognize digital evidence in court. There is no specialized international judicial body for digital economic crimes.

Third: Proposal for a UN Convention on Digital Economic Crimes (UNDEC)

A precise legal definition of digital economic crimes: theft of sovereign data, cryptocurrency smuggling, hacking through cyberattacks, and others. It establishes a rapid response body that allows countries to collect digital evidence within 24 hours based on a judicial request. It establishes an international digital investigation unit affiliated with the UN, equipped with expertise in cybersecurity, artificial intelligence, blockchain, and cryptocurrencies. It requires that digital evidence be collected according to unified international technical standards such as ISO IEC 27037.

Here we propose for the first time the concept of "Algorithmic Criminal Liability," where the owner of the algorithm can be held legally liable if it is proven that they designed it to contain automatic smuggling programs.

The chapter concludes with a warning that without a global digital justice system, the digital economy will remain a safe haven for organized crime.

CHAPTER FOURTEEN

ALGORITHMIC TRANSPARENCY AS A CONDITION FOR JUSTICE

The Right to Access Algorithms and the Right to a Fair Trial

Algorithms have been treated as trade secrets, which obliges them to be governed by the TRIPS Agreement on intellectual property rights when algorithms affect economic decisions that influence billions of people, such as determining credit ratings, insurance premiums, employment opportunities, and even political opinions.

This leads to discrimination and economic injustice.

First: The Weakness of Algorithmic Discrimination

Studies have proven that American rental algorithms reject applications from people of African descent at the highest rates, relying on technical features that reflect discrimination in training data. Electronic trade algorithms raise prices in developing countries without an economic justification.

Second: The Conflict Between Protection and Fairness

Companies refuse to disclose their algorithms under the pretext of losing their competitive advantage. There is no international body for algorithmic fairness.

Third: Proposal for the Principle of Digital Economic Transparency

As a fundamental international norm, every digital economic entity must be required to disclose its algorithms not as complete secrets, but to national regulatory bodies. It allows individuals and countries the right to access information that affects their economic decisions. It proposes the establishment of an international body for algorithmic ethics under the auspices of the United Nations, which sets global standards for algorithmic fairness, issues fairness certificates used as fundamentals in international arbitration.

The chapter concludes with a legal ruling that algorithms are not merely trade secrets, but tools that affect public interest, and transparency is a right and a global right when fairness is applied.

CHAPTER FIFTEEN

TOWARDS AN INTERNATIONAL TREATY ON DIGITAL ECONOMIC SOVEREIGNTY

A Comprehensive Legal Framework for a New World

After a comprehensive analysis of legal gaps and the existential risks posed by the digital economy on the international system, it becomes clear that partial and sectoral solutions are not enough. The world today needs a comprehensive international treaty that helps define relations between countries, digital platforms, and artificial entities in the digital age.

First: The Foundations of the Proposed Treaty

The name of the treaty: United Nations Treaty on Digital Economic Sovereignty (UNTDES). The purpose of the treaty: to ensure a balance of justice between the right to privacy, national sovereignty, and the rights of individuals in digital economic activities.

The fundamental principles:

1. The right of the state to sovereignty over data generated on its territory or by its citizens.
2. The right to fair distribution of digital value in the economic activities of developing countries.

3. The condition of transparency for operation: no entity can operate without complying with transparency and accountability standards.
4. The temporary developmental exemption: developing countries are granted a transitional period to build their digital capabilities without exposure to investment claims.

Second: The Proposed Institutional Structure

An annual meeting of all parties (COP) to take binding decisions. The expert committee of experts does not represent governments, the private sector, and civil society. An international dispute settlement body for specialized arbitration in applying the principles of the treaty.

Third: Implementation and Monitoring

Each country is required to submit a mandatory national report evaluating the performance of its digital policies. Before accepting its commitments, the country receives technical and training support from the committed countries.

The chapter concludes with a strategic vision that the treaty will be built through a gradual process, because it starts with a political agreement from a group of pioneering countries, then turns into a broader initiative in the UN General Assembly, after resolving differences and technical details. It has become more than 30 years since the digital economy has become the international community, and we do not have the expectation of the future.

CHAPTER SIXTEEN

MONITORING ARTIFICIAL INTELLIGENCE IN FINANCIAL MARKETS

From Algorithmic Speculation to the International Regulatory System

Financial markets have transformed, over the past two decades, from human trading floors to systems where 70% of trading is executed through artificial intelligence systems. Despite the efficiency these systems provide, they have become a single source of systemic risks.

First: The Risks of Unregulated AI

1. A single algorithmic error can cause a global market collapse. A single algorithm can cause a chain of declines leading to a global market crash.
2. The possibility of hidden speculation: using multiple algorithms to manipulate other trading systems.
3. Concentrated risk: if AI models are trained on concentrated data, it will deepen the gap between advanced and developing markets.

Second: The Failure of National Regulatory Systems

The United States relies on the disclosure principle. The European Union has begun to apply the AI Act, but it does not cover financial markets completely. Most developing countries lack the technical capacity to monitor algorithms.

Third: Proposal for an International System for Monitoring Financial AI (IAFOS)

Mandatory registration of every algorithmic trading system exceeding 500 million dollars. The BIS (Bank for International Settlements) conducts annual digital stress tests to simulate algorithm behavior in crisis conditions. A global monitoring system issues early warnings of abnormal movements exceeding borders. Joint liability falls on the company that issued the algorithm and the country that allowed its operation.

Here we propose for the first time the concept of "Financial Digital Sovereignty," which allows only after passing fairness tests that provide an interpretive model explaining how decisions are made (Explainable AI), and ensuring the existence of a human kill switch in emergency situations.

The chapter concludes with a strategic confirmation that financial markets without international monitoring are not free, but produce neither speculation nor profit, but rather a disaster.

CHAPTER SEVENTEEN

REDEFINING PRIVACY AS AN ECONOMIC ASSET

The Relationship Between the Individual, the State, and the Company in the Digital Economy

Personal data is no longer merely a human right, but has become a strategic economic asset. Location, health status, political orientations, and even health conditions have become raw materials that companies trade in.

Therefore, privacy protection is not merely an ethical responsibility, but a national, economic, and strategic security.

First: Privacy in Comparative Legal Systems

The European Union treats privacy as a fundamental right. The GDPR grants the state the right to protect data as a free right, and considers data a national asset. The United States considers data as property owned by the individual and the company, and uses it to strengthen economic power. Most Arab countries have fragmented regulations that link cybersecurity and privacy.

Second: Economic Exploitation of Privacy

Companies like Google and Meta collect personal data, then analyze it to predict behavior, and then sell it for advertising. The individual or the country does not obtain any return, despite the fact that developing countries lose billions of dollars annually due to the smuggling of the value generated from their national data.

Third: Proposal for the Triple Ownership Model of Personal Data

The individual owns the right to consent and deletion. The state owns the right to impose taxes and correct the market. The company owns the right to limited use in exchange for fair payment. The use of data is subject to paying a fair return.

It is proposed to establish a national market for personal data in each country, where individuals can sell their data directly to companies, under conditions that prevent the exploitation of vulnerable groups.

The chapter concludes with a new legal vision that privacy is not merely a negative right that the individual covers, but a strategic asset that the community and the state invest in, and the consumer reaps the returns.

CHAPTER EIGHTEEN

THE DIGITAL ECONOMY AND SUSTAINABLE DEVELOPMENT

Between Digital Growth and Environmental and Social Justice

The digital economy is often viewed as a clean industry because it does not rely on factories or raw materials. However, this is a misconception. The digital economy is the most polluting, as data centers consume 3% of global electricity, and electronic devices generate waste that equals the weight of all the world's aircraft.

Therefore, digital growth does not deepen the gap between those who own digital skills and those who do not.

First: The Environmental Impact of the Digital Economy

1. A search on Google produces 0.2 grams of carbon dioxide. Generating AI content requires energy that is extracted from non-renewable sources. Continuous device updates create electronic waste that is not treated.
2. The social exclusion of the digital economy: 60% of Africans cannot access the internet. The speed of gender gap in developing countries. Workers in the Gig Economy lack social protection.

Third: Proposal for a Sustainable Digital Economy Agreement (SDI)

It measures the performance of digital companies in terms of carbon footprint, gender equality, and fair wages. It imposes data centers on high energy consumption, and directs their investments to renewable energy. Every digital company working in a developing country must invest 1% of its profits in building local digital capabilities.

The chapter concludes with an ethical and legal call that the digital economy has no value if it is not inclusive and sustainable, because true development is not measured by speed, but by humanity.

CHAPTER NINETEEN

INTERNATIONAL HUMANITARIAN LAW AND THE DIGITAL ECONOMY IN WARS

Protecting Civilian Infrastructure in Digital Conflicts

In the digital age, wars are no longer fought with tanks and missiles alone, but with cyberattacks, digital infrastructure, and economic data. In recent years, we have witnessed attacks on energy networks, banking systems, and health systems that have paralyzed entire regions.

First: The Digital Economy as a Military Target

Article 54 of the First Additional Protocol to the Geneva Conventions protects the means of survival of the civilian population, such as food and water. But it does not mention digital infrastructure such as payment systems, health data, and communication networks.

Second: Revealing Legal Gaps

The 2017 NotPetya attack, a global attack with unintended consequences in Ukraine, caused billions in losses to shipping systems. The 2023 hacking of hospital systems in India prevented the transfer of payments for humanitarian aid through digital assets. In all these cases, no responsibility was invoked under international humanitarian law, because digital infrastructure is not classified as a civilian object under the Geneva Conventions.

Third: Proposal for an Additional Protocol to the Geneva Conventions on Digital Warfare

A new definition of digital warfare includes critical digital economic infrastructure such as national payment systems, health data, and financial networks. The principle of digital proportionality: attack is prohibited if it is expected to cause damage to civilian digital systems exceeding the military advantage. The concept of digital siege is introduced: preventing civilians from accessing the digital economy, such as blocking electronic payments or internet access, is considered equivalent to sieging food or water, a war crime.

The chapter concludes with a human legal foundation that if the digital economy of today is not protected, we will find ourselves in a war where people do not die from bombs, but from the collapse of services, the cessation of aid, and the failure of work.

CHAPTER TWENTY

THE DIGITAL ECONOMY AND REDEFINING THE CONCEPT OF EMPLOYMENT IN THE AGE OF AUTOMATION

With the rapid pace of automation, it is estimated that 800 million jobs will be replaced by 2030 due to artificial intelligence and robots. Digital platforms have not been considered as a registered employee in a company, but rather as an independent worker through platforms like Uber or Amazon Mechanical Turk, without insurance, social security, or even the right to organize.

Despite this, the International Labour Organization (ILO) has not updated its concepts to apply to this new reality.

First: The End of Traditional Work Concepts

The employment relationship is no longer a direct relationship, but rather a digital intermediary relationship through algorithms that distribute tasks via digital platforms without human intervention. The worker is not protected by most national labor laws, which are based on traditional concepts.

Second: Algorithmic Discrimination in the Labor Market

Employment algorithms reject applications from people with non-Arabic names or from certain areas. Evaluation systems classify workers based on irrelevant factors, and there is no right to appeal in the final decisions that end the employment relationship.

Third: Proposal for a Digital Labor Convention

A new definition of the digital worker: every person who works through a digital platform is considered a worker, and is entitled to a minimum digital wage that is calculated according to the cost of living in the country where they live. An international digital social security fund: platforms pay 3% of their profits to ensure the worker's right to health and retirement. Fair evaluation algorithms are required to ensure fairness.

It is proposed to establish an international body for digital workers' rights under the ILO, which monitors platform compliance and imposes electronic penalties such as blocking profits.

The chapter concludes with a human legal vision that artificial intelligence may have taken the place of the father, but the community must ensure that automation and technology do not deprive society of its right to a fair life.

CHAPTER TWENTY-ONE

FROM PLATFORM DEPENDENCE TO DIGITAL GOVERNANCE

The Global Digital Economy Council

Today, the digital economy is governed by a group of private companies, non-technical bodies like ICANN, financial institutions like BIS, and training systems. There is no single authority that owns the power to legislate binding rules or the ability to impose digital governance.

First: The Failure of Current Models

The multi-stakeholder model gives companies the power to weaken sovereignty, such as international regulations like the European GDPR, which are applied outside their borders. Bilateral agreements like the data flow agreement between the US and the EU create fragmented digital parts.

Second: The Foundations of Digital Governance

1. Shared digital sovereignty: the state, civil society, and the private sector participate in decision-making.
2. The right of developing countries to a transitional period for technical and capacity building.
3. Complete transparency: all decisions are published and accepted by all observers.
4. No imposition of foreign cultural models as global standards.

Third: Proposal for the Global Digital Economy Council (GDEC)

Membership of all UN countries, with representatives from large companies, civil society, and academic experts. The Council votes on regulatory standards, such as technical fairness. A country like Kenya is proposed, followed by 30 countries for the implementation of reforms, monitoring compliance, and settling disputes between countries and companies through binding arbitration.

The chapter concludes with a strategic vision that the world created the UN Security Council after World War II to maintain peace, and today the Digital Economy Council is established to maintain justice, because digital injustice can be a cause of any war.

CHAPTER TWENTY-TWO

INTELLECTUAL PROPERTY AND THE BALANCE BETWEEN INNOVATION AND ACCESS The Challenge of Algorithms and Data

In the digital economy, intellectual property is no longer merely a protection for inventors or creators, but has become a tool for controlling markets. Recommendation algorithms, AI models, and raw data are registered under the name of foreign companies, while they exploit the behavioral data of billions of people in the Global South without fair compensation.

First: The Failure of the Current System

AI allows companies to train their models on partial data from developing countries, and then considers the resulting models as their exclusive property. Data generated by users is considered a free resource, despite the fact that the single digital agreement did not agree on rights, because the service is free.

Second: Unfair Exploitation as a Source of Innovation

An American company developed a model to diagnose skin diseases using images from Africa, and then sold it to the same country that provided the data for training its systems in Africa without compensation or notification. This is not merely an ethical violation, but a violation of the principle of shared benefit that governs international intellectual property.

Third: Proposal for a Digital Fair Intellectual Property System

It allows indirect contribution: countries and communities that generate data have the right to participate in the profits generated from them. Mandatory registration: if there were more than

50 million data from a developing country for training, a fair global right to digital innovation is imposed. It obliges AI companies to share patents with the Global South.

Here we propose for the first time the concept of "Digital Innovation Sovereignty" over data generated by countries that train AI models, because innovation is not born from nothing, but from shared data.

The chapter concludes with a legal ethical call that intellectual property is not an absolute right, but a socially conditioned right. If this protection has lost its legitimacy, it has lost its legitimacy.

CHAPTER TWENTY-THREE

FROM SMALL TRANSFORMATIONS TO INCLUSIVE DIGITAL ECONOMY

The Challenge of Small and Medium Enterprises

Most people imagine the digital economy as the growth of large companies, but in reality, small and medium enterprises (SMEs) are shrinking from the digital market due to the high costs of digital transformation, the concentration of platforms, and unfair competition.

First: Legal Challenges for SMEs

1. Unfair competition conditions: reaching 30 agreements without cause.
2. Algorithmic discrimination: algorithms favor large companies in search results.
3. The inability to bear the costs of international arbitration for small enterprises.

Second: The Failure of Current Policies

Most government support programs are merely technical packages without legal or financial support. There are no national bodies to protect SMEs from digital cyber attacks. Even in the European Union, protection is limited by national borders.

Third: Proposal for a Convention on the Protection of Small Enterprises in the Digital Economy

It limits the maximum number of transactions to 15, ensuring the basic right of small enterprises to digital platforms. It requires knowing how to arrange fair, low-cost, and simplified digital procedures. It establishes a digital legal support fund to cover the costs of digital arbitration for small enterprises in international disputes.

It is proposed to establish a global network of small enterprises under the UN, which enables the exchange of experiences and access to fair financing.

The chapter concludes with a human economic vision that the digital economy is not measured by the success of large companies, but by the ability of small enterprises to survive, because diversity is the essence of sustainability.

CHAPTER TWENTY-FOUR

RETURNING FROM TRANSPARENCY TO CORRUPTION

New Tools for Fighting Corruption

Transparency has been considered the primary tool for fighting corruption, but evidence has proven that transparency alone is not enough. Corruption has evolved from direct bribery to complex digital networks, encrypted transactions, and automated money laundering systems.

First: Forms of New Digital Corruption

1. Algorithmic corruption: ensuring that algorithms favor specific companies.
2. Digital lobbying: paying through encrypted transactions without trace.
3. Corruption through shell companies to launder money.

Second: The Failure of Traditional Anti-Corruption Tools

Electronic reporting systems do not provide real monitoring. Even the UN Convention against Corruption (UNCAC) does not cover digital financial flows.

Third: Proposal for an International System for Combating Digital Corruption

A global registry for digital companies reveals the true ownership of every digital entity. A digital investigation unit affiliated with UNODC automatically reports high-value digital transactions exceeding 10,000 dollars. It provides legal and technical support for transparent digital companies.

Here we propose the new concept of "Silent Corruption," which is corruption that does not occur through bribery, but through algorithms and cryptocurrencies.

The chapter concludes with a strategic confirmation that corruption is not killed without responsibility, and transparency without accountability is merely a cover for corruption.

CHAPTER TWENTY-FIVE

FROM DATA TO DIGITAL IDENTITY

Building a Digital Economy Based on the Individual

In the digital economy, identity has not become merely a means of access to zero or identity cards, but has become the single gateway to financial, employment, trade, and social services. Today, digital identity systems are controlled by private companies like Google Account or Apple ID, turning a person's political identity into a tool of economic control.

First: Strategic Risks of Digital Identity

1. Identity theft: centralized identity systems can be hacked without trace, as happened with the hacking of payment platform accounts.

2. Biometric exploitation: collecting biometric data without consent, then selling it as commercial products to interested individuals.
3. Digital exclusion: the poor and marginalized do not have digital identity, and thus are excluded from all services.

Second: Proposed Global Digital Identity System

A unified global digital identity that grants every human being the right to digital identity from birth, regardless of gender. Managed by a tripartite body (the state, the UN, and the individual) to prevent hacking. Open technology to prevent hacking. Allows the use of digital identity for commercial transactions without consent, and a digital identity network that allows dealing without the need for intermediaries.

Here we propose for the first time the concept of "Personal Digital Sovereignty," where the individual is not merely a source of data, but an independent digital entity that has complete control over their digital identity. If they lose their identity, they may lose their existence in the digital economy.

The chapter concludes with a human legal foundation that digital identity is not a technical matter, but a recognition that the world has decided that no one is excluded from the digital economy because they are non-human.

CHAPTER TWENTY-SIX

FROM ALGORITHMIC MONOPOLY TO DIGITAL MARKET COMPETITION

The Challenge of Fair Competition

In the digital economy, competition is no longer measured by the size of the company, but by its ability to control the algorithms that govern user behavior. Companies determine prices, classify consumers, and thus transform into monopolies that set market rules without any competition, eliminating the elements of fair competition.

First: Elements of Algorithmic Monopoly

1. Discrimination in search results: platforms favor their own products.
2. Dynamic pricing: raising prices for loyal users.
3. Theft of competitive data: using user data to develop competing products.

Second: The Failure of Traditional Competition Laws

US antitrust laws like the Sherman Act were designed for the industrial age, and there is no body to monitor algorithmic concentration. Even real monopolies like Google's 4.3 billion dollar fine do not change behavior, because profits are much larger.

Third: Proposal for a Digital Competition Law

It obliges large platforms to disclose the principles of ranking and product arrangement. It allows the use of user data for developing competing products. It establishes a single international digital regulatory body with the authority to monitor competition, impose fines, and order corrections to ensure fair access to APIs for small competitors.

Here we introduce a new concept in international law: "Digital Antitrust Damage," which is the harm caused by algorithmic monopoly, even if prices have not decreased in the market.

The chapter concludes with a strategic legal confirmation that the digital market without fair competition is not free, but produces neither innovation nor stagnation, but rather a dictatorship.

CHAPTER TWENTY-SEVEN

FROM FOOD SOVEREIGNTY TO DIGITAL AGRICULTURE

The Shift from Traditional to Digital Dependence

In the era of digital agricultural transformation, food sovereignty has not meant merely the ability to produce food, but the ability to control data. Data on soil, climate, crops, and even farmer behavior have become the most valuable resource, controlled by foreign companies that exploit it, while developing countries merely consume the results at high cost.

First: Forms of Digital Agricultural Exploitation

Companies like John Deere prevent farmers from repairing their machines because the programs are closed. Smart agricultural machines collect soil data, then sell recommendations at high prices. The poor farmer does not have access to the data that his machines generate daily.

Second: Legal Gaps

Agricultural data is not considered a national asset in most countries. Digital agricultural contracts are considered unfair terms that prevent the transfer of agricultural technology.

Third: Proposal for a Digital Food Sovereignty Convention

It grants the farmer and the state joint ownership of agricultural data with fair compensation. The farmer's right to digital repair: the right to repair and modify fairly. It obliges the development of open local solutions for smart machines. If artificial intelligence depends on local genetic materials, it must be from the Global South.

Here we propose a new concept: the Digital Agricultural Development Right, which is the fair return that the state obtains for every commercial use of its agricultural data.

The chapter concludes with a strategic foundation that in the digital age, food sovereignty is not built on the stomach, but on data. Whoever controls the data of the land controls the food.

CHAPTER TWENTY-EIGHT

FROM LEGACY DEBT TO DIGITAL CARBON LIABILITY

The Challenge of Intergenerational Justice

In the history of digital innovation, it is often said that the current generation has the right to exploit digital resources without restrictions. But data centers, cryptocurrencies, and AI models consume huge amounts of energy, generate electronic waste, and produce massive carbon emissions that affect future generations.

The current generation does not have the right to monopolize digital resources based on the consumption of digital resources. Energy, data centers, electronic waste, and personal data smuggling are all carried by future generations without limits, without ethical, environmental, economic, or moral responsibility.

First: The Carbon Footprint of the Digital Economy

Every search, transaction, or AI model training leaves a carbon footprint. Training a single AI model emits 50 tons of carbon, equivalent to the lifetime emissions of 4 cars. Most of it is non-renewable electronic waste.

Second: The Gap in International Law

The principle of intergenerational equity in environmental law, like the 1992 Rio Declaration, is not applicable in the digital economy. There is no legal obligation on digital companies to bear the responsibility of the digital carbon footprint.

Third: Proposal for Digital Carbon Equity Mechanisms

It imposes a mandatory digital carbon footprint assessment for every digital economic project. The large digital project must assess its impact on future generations, pays digital carbon taxes, directs them to renewable energy, and restores digital rights. Data is considered a shared heritage for humanity, like biological diversity, and collecting data for commercial purposes is prohibited without consent.

Here we propose for the first time the concept of "Digital Legacy Liability," where the digital economy builder is legally and ethically responsible for the impact they leave, because the current generation will not give birth after death.

The chapter concludes with a legal ethical foundation that we have the right to build digital generations that do not leave destruction after them.

CHAPTER TWENTY-NINE

FROM SMALL ENTERPRISES AND DIGITAL TRANSFORMATION

The Challenge of Inclusive Digital Economy

Most people imagine the digital economy as the growth of large companies, but in reality, small and medium enterprises (SMEs) are shrinking from the digital market due to the high costs of digital transformation, the concentration of platforms, and unfair competition.

First: Legal Challenges for SMEs

1. Unfair competition conditions: reaching 30 agreements without cause.
2. Algorithmic discrimination: algorithms favor large companies in search results.
3. The inability to bear the costs of international arbitration for small enterprises.

Second: The Failure of Current Policies

Most government support programs are merely technical packages without legal or financial support. There are no national bodies to protect SMEs from digital cyber attacks. Even in the European Union, protection is limited by national borders.

Third: Proposal for a Convention on the Protection of Small Enterprises in the Digital Economy

It limits the maximum number of transactions to 15, ensuring the basic right of small enterprises to digital platforms. It requires knowing how to arrange fair, low-cost, and simplified digital procedures. It establishes a digital legal support fund to cover the costs of digital arbitration for small enterprises in international disputes.

It is proposed to establish a global network of small enterprises under the UN, which enables the exchange of experiences and access to fair financing.

The chapter concludes with a human economic vision that the digital economy is not measured by the success of large companies, but by the ability of small enterprises to survive, because diversity is the essence of sustainability.

CHAPTER THIRTY

FROM DIGITAL DIVIDE TO DIGITAL PEACE

The Challenge of Digital Exclusion

The digital economy has become a tool for international communication, but instead of being a means of communication, it has become a tool for digital exclusion, cyberattacks, and digital fragmentation.

First: Strategic Risks of Digital Exclusion

1. Digital siege: preventing countries from accessing digital payment systems, as happened with Iran's banking system.
2. Digital fragmentation: the digital world is divided into closed systems (American, European, Chinese, Russian) that do not agree with each other due to differences in laws and borders.

3. Digital wars: using digital infrastructure as a tool of war.

Second: The Failure of Current Models

The multi-stakeholder model gives companies the power to weaken sovereignty, such as international regulations like the European GDPR, which are applied outside their borders. Bilateral agreements like the data flow agreement between the US and the EU create fragmented digital parts.

Third: Proposal for a Digital Peace Agreement

It includes the prohibition of using digital infrastructure for military purposes, the protection of digital economic infrastructure from theft, and the establishment of a digital early warning system for digital attacks. It obliges all countries to apply unified rules for digital platforms, and provides guarantees for small countries to participate in the digital economy without digital sanctions.

The chapter concludes with a strategic vision that building peace in the 21st century requires not only the absence of war, but the existence of a fair digital system, because digital injustice can be a cause of any war.

CONCLUSION

THE DIGITAL SOCIAL CONTRACT

Towards a Fair Global Future

After this long journey through the corridors of the digital economy, we realize that we are not facing a technical revolution, but a fundamental transformation in the concept of wealth, power, and justice.

The old rules have failed, and we need a new digital social contract based on:

1. Data as a shared resource that is not exploited without fair compensation for the state and the individual.
2. Artificial intelligence that is subject to accountability and human values.
3. An inclusive digital economy that does not exclude anyone due to gender, poverty, or geography.
4. Digital peace: preventing the use of the digital economy as a weapon of war.

The final message: the digital future is not a technical fate, but a political and legal choice. We need to move from a world governed by algorithms to a world governed by justice.

OPENING WORDS IN TEN LANGUAGES

Arabic:

"إن المستقبل الرقمي ليس قدراً محتوماً، بل هو خيار قانوني وأخلاقي. نحن بحاجة إلى الانتقال من عالم تحكمه الخوارزميات إلى عالم تحكمه العدالة."

English:

"The digital future is not a predetermined fate, but a legal and ethical choice. We need to move from a world governed by algorithms to a world governed by justice."

French:

"L'avenir numérique n'est pas un destin inévitable, mais un choix juridique et éthique. Nous devons passer d'un monde gouverné par les algorithmes à un monde gouverné par la justice."

Spanish:

"El futuro digital no es un destino predeterminado, sino una elección legal y ética. Necesitamos pasar de un mundo gobernado por algoritmos a un mundo gobernado por la justicia."

Chinese:

"数字未来不是注定的命运,而是法律和道德的选择。我们需要从算法统治的世界走向正义统治的世界。"

Russian:

"Цифровое будущее - это не предопределенная судьба, а юридический и этический выбор. Нам нужно перейти от мира, управляемого алгоритмами, к миру, управляемому справедливостью."

German:

"Die digitale Zukunft ist kein vorbestimmtes Schicksal, sondern eine rechtliche und ethische Wahl. Wir müssen von einer Welt, die von Algorithmen regiert wird, zu einer Welt übergehen, die von Gerechtigkeit regiert wird."

Portuguese:

"O futuro digital não é um destino predeterminado, mas uma escolha legal e ética. Precisamos passar de um mundo governado por algoritmos para um mundo governado pela justiça."

Hindi:

"डिजिटल भविष्य एक पूर्वनिर्धारित भाग्य नहीं है, बल्कि एक कानूनी और नैतिक चुनाव है। हमें एल्गोरिदमों से शासित दुनिया से न्याय से शासित दुनिया में जाना होगा।"

Japanese:

"デジタルな未来は predetermined な運命ではなく、法的かつ倫理的な選択です。アルゴリズムによって支配される世界から、正義によって支配される世界へ移行する必要があります。"

APPENDICES

APPENDIX A: DEEP ANALYSIS OF KEY CONCEPTS

1. Digital Sovereignty

Digital sovereignty is not merely the state's control over data within its borders, but the ability to shape digital economic rules that affect its citizens globally. It includes three dimensions:

- Technical sovereignty: the ability to build national digital infrastructure
- Legal sovereignty: the ability to legislate digital laws that are respected internationally
- Economic sovereignty: the ability to capture fair value from digital activities

2. Algorithmic Accountability

Algorithmic accountability means that every algorithm that makes economic decisions must be:

- Transparent: its logic can be explained
- Fair: it does not discriminate based on race, gender, or geography
- Reversible: there is a human override mechanism
- Liable: the entity that deployed it bears responsibility for its outcomes

3. Digital Rent

Digital rent is the fair return that data-producing countries should receive for the exploitation of their data by foreign companies. It is calculated based on:

- Volume of data extracted
- Economic value generated from it
- Degree of local value addition
- Environmental and social costs

4. Non-Human Investor

The concept of non-human investor recognizes that AI systems can make autonomous investment decisions, and therefore need:

- Legal registration
- Mandatory insurance
- Clear liability attribution
- Operational limits

5. Digital Value Nexus

Digital value nexus is a new concept for determining tax jurisdiction based on:

- User interaction volume
- Data generated locally

- Economic value created
- Market presence (even without physical presence)

APPENDIX B: COMPARATIVE LEGAL FRAMEWORKS

1. European Union Approach

- GDPR: Privacy as fundamental right
- AI Act: Risk-based regulation
- Digital Markets Act: Platform competition
- Data Governance Act: Data sharing

2. United States Approach

- Sectoral privacy laws
- Innovation-first regulation
- Antitrust enforcement
- Market-driven solutions

3. Chinese Approach

- Data Security Law: National security focus
- Personal Information Protection Law: State control
- Cybersecurity Law: Sovereignty emphasis
- State-led digital development

4. African Union Approach

- Malabo Convention: Cybersecurity and data protection
- Digital Transformation Strategy: Inclusive growth
- Continental free trade area: Digital integration
- Local content requirements

APPENDIX C: PROPOSED TREATY TEXTS

1. UN Treaty on Digital Economic Sovereignty (UNTDES)

Preamble: Recognizing that data has become the most valuable resource in the digital age...

Article 1: Definitions

- Digital sovereignty: The right of states to regulate digital economic activities affecting their territory and citizens
- Digital rent: Fair compensation for data-producing countries
- Algorithmic accountability: The obligation to ensure transparency and fairness in algorithmic decision-making

Article 2: Principles

- Sovereignty over data
- Fair distribution of digital value
- Transparency as condition for operation
- Developmental exemption for developing countries

Article 3: Institutional Mechanisms

- Global Digital Economy Council
- Digital Dispute Settlement Body
- International Digital Justice Fund

2. Convention on Digital Economic Crimes (UNDEC)

Article 1: Scope

This Convention applies to:

- Theft of sovereign data
- Cryptocurrency smuggling
- Cyberattacks on economic infrastructure
- Algorithmic manipulation

Article 2: International Cooperation

- 24-hour response mechanism
- Mutual recognition of digital evidence
- Joint investigation teams

Article 3: Prevention

- Mandatory registration of high-risk algorithms
- Digital forensic standards (ISO IEC 27037)
- Whistleblower protection

APPENDIX D: CASE STUDIES

1. TechGlobal v. Republic of Sylva (2024)

Facts: An AI trading algorithm caused the collapse of Sylva's stock market.

Issue: Can the state access the algorithm under trade secret protection?

Holding: The tribunal refused access, highlighting the need for DEISDS.

2. DataFlow Inc. v. State of Nubia (2025)

Facts: Nubia required local data storage; DataFlow claimed expropriation.

Issue: Is data localization a legitimate sovereign act?

Holding: The tribunal ruled for the investor, showing the need for clearer BITS.

3. Microsoft v. Brazil (2023)

Facts: Brazil imposed digital sovereignty requirements on Microsoft.

Issue: Does international law recognize digital sovereignty?

Holding: The UN Legal Committee stated that digital sovereignty is not yet recognized as part of economic sovereignty.

4. African Stock Market Collapse (2025)

Facts: Foreign algorithmic trading caused massive liquidity drain.

Issue: Can developing countries block access to foreign platforms?

Holding: No clear legal framework exists, showing the need for digital capital controls.

APPENDIX E: TECHNICAL STANDARDS

1. ISO IEC 27037: Digital Evidence Collection

- Identification of digital evidence
- Collection procedures
- Preservation methods
- Documentation requirements

2. ISO IEC 27001: Information Security Management

- Risk assessment
- Security controls
- Continuous monitoring
- Certification process

3. IEEE 7000: Ethical AI Design

- Stakeholder identification
- Ethical risk assessment
- Mitigation strategies
- Transparency requirements

4. W3C Accessibility Guidelines

- Perceivable content
- Operable interfaces
- Understandable information
- Robust technology

REFERENCES

Books and Monographs

1. Elrakhawi, Mohamed Kamal Aref. The Global Encyclopedia of Law: A Comparative Practical Study. First Edition, January 2026.
2. Elrakhawi, Mohamed Kamal Aref. Investment Arbitration and Banking: A Global Legal Reference. Unpublished Manuscript, 2025.
3. Elrakhawi, Mohamed Kamal Aref. Practical Guide to Judicial Inspections in Criminal and Economic Matters. Forthcoming, 2026.
4. Schreiber, A. Artificial Intelligence and International Economic Law: Uncharted Territories. Cambridge University Press, 2024.
5. Benkler, Y. "The Wealth of Networks in the Digital Age." Yale Law Journal, Vol. 133, No. 4, 2025.
6. Zuboff, S. Surveillance Capitalism and the Global South. Harvard University Press, 2023.
7. Posner, E. & Sunstein, C. Algorithms and Justice: A New Social Contract. Oxford University Press, 2025.
8. Al Jabri, M. "Digital Sovereignty in Arab Economies: Legal Challenges and Opportunities." Journal of Arab Law Review, Vol. 12, 2024.

International Legal Instruments

9. United Nations. Charter of the United Nations. 1945.
10. World Trade Organization. Agreement Establishing the World Trade Organization. 1994.
11. OECD. Model Bilateral Investment Treaty. 2023 Revision.
12. ICSID. Convention on the Settlement of Investment Disputes between States and Nationals of Other States. 1965.
13. UNCTAD. World Investment Report 2025: Digital Economies and Sovereignty.
14. European Union. General Data Protection Regulation (GDPR). Regulation EU 2016/679.
15. Bank for International Settlements. Annual Economic Report 2025: Central Bank Digital Currencies and Financial Stability.
16. International Labour Organization. Declaration on Fundamental Principles and Rights at Work. 1998, amended 2022.

17. United Nations. Convention against Corruption (UNCAC). 2003.
18. World Intellectual Property Organization. WIPO Copyright Treaty. 1996.
19. International Law Commission. Draft Articles on Responsibility of States for Internationally Wrongful Acts. 2001.
20. United Nations Environment Programme. Digitalization and Environmental Sustainability: Global Assessment Report. 2024.
21. African Union. Convention on Cyber Security and Personal Data Protection (Malabo Convention). 2014.
22. United States Department of Justice. Guidelines on Algorithmic Accountability in Financial Markets. 2024.
23. People's Republic of China. Data Security Law. 2021.
24. International Monetary Fund. Digital Money and Cross-Border Payments: Legal and Policy Frameworks. 2025.
25. World Bank. World Development Report 2025: The Digital Economy for All.

Reports and Studies

26. UNCTAD. Digital Economy Report 2024: Data Flows and Development.
27. World Economic Forum. The Future of Digital Trade 2025.
28. OECD. Digital Economy Outlook 2024.
29. ITU. Measuring Digital Development: Facts and Figures 2025.
30. UNDP. Human Development Report 2024: Breaking the Digital Divide.

Journal Articles

31. "Algorithmic Sovereignty: A New Paradigm in International Law." Harvard International Law Journal, Vol. 65, 2025.
32. "Digital Colonialism in the Age of Big Data." Journal of International Economic Law, Vol. 28, 2024.

33. "The Right to Digital Development: A Proposed Framework." American Journal of International Law, Vol. 119, 2025.
34. "Cryptocurrency Regulation and Financial Stability." Stanford Law Review, Vol. 77, 2025.
35. "AI and Employment: Legal Challenges." International Labour Review, Vol. 164, 2025.

COPYRIGHT AND CITATION

Copyright © 2026 Dr. Mohamed Kamal Aref Elrakhawi

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the author, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law.

Digital Object Identifier (DOI): 10.5281/zenodo.22852334

Academic Citation (APA 7th Edition):

Elrakhawi, M. K. A. (2026). The Global Encyclopedia of Digital Economic International Law. Asyut, Egypt. <https://doi.org/10.5281/zenodo.22852334>

Academic Citation (Chicago Style):

Elrakhawi, Mohamed Kamal Aref. The Global Encyclopedia of Digital Economic International Law. Asyut, Egypt: Self-published, 2026. <https://doi.org/10.5281/zenodo.22852334>.

Academic Citation (MLA 9th Edition):

Elrakhawi, Mohamed Kamal Aref. The Global Encyclopedia of Digital Economic International Law. 2026. <https://doi.org/10.5281/zenodo.22852334>.

Academic Citation (Harvard Style):

Elrakhawi, M.K.A., 2026. The Global Encyclopedia of Digital Economic International Law. Asyut, Egypt. Available at: <https://doi.org/10.5281/zenodo.22852334>.

INDEX OF KEY TERMS

Algorithmic Accountability
Artificial Intelligence as Investor
Big Data as Investment Asset
Central Bank Digital Currencies (CBDCs)
Digital Agriculture
Digital Carbon Liability
Digital Competition Law
Digital Economic Crimes
Digital Economic Sovereignty
Digital Fair Competition
Digital Food Sovereignty
Digital Identity
Digital Innovation Sovereignty
Digital Justice
Digital Labor Convention
Digital Legacy Liability
Digital Peace
Digital Rent
Digital Social Contract
Digital Sovereignty
Digital Value Nexus
Non-Human Investor
Personal Data Triple Ownership
Platform Quasi-Sovereignty
Privacy as Economic Asset
Sustainable Digital Economy

ACKNOWLEDGMENTS

This encyclopedia would not have been possible without the support of many individuals and institutions. I extend my deepest gratitude to:

- The academic community for their valuable feedback
- Legal practitioners who shared their practical experiences
- Researchers who contributed to the comparative studies
- Students whose questions inspired deeper analysis
- My family for their unwavering support

Special thanks to all those who believe that law can be a tool for justice in the digital age.

ABOUT THE AUTHOR

Dr. Mohamed Kamal Arafa Elrakhawi is a legal scholar specializing in international economic law, investment arbitration, and digital economy regulation. He holds advanced degrees in law and has extensive experience in judicial inspections and legal research. His work focuses on bridging the gap between traditional legal frameworks and the challenges of the digital age, with particular emphasis on protecting the interests of developing countries.

Dr. Elrakhawi has published extensively on investment arbitration, banking law, and judicial inspections. His research aims to create comprehensive legal frameworks that are both practical and theoretically sound, serving as references for scholars, judges, policymakers, and students worldwide.

Contact: Egypt

Date: 2026

END OF DOCUMENT

DOI: 10.5281/zenodo.22852334

This document is available for academic citation and research purposes.