

THE ECONOMIC CITIZENSHIP OF ALGORITHMS THE PERSONALITY OF

ARTIFICIAL INTELLIGENCE

By Dr. Mohamed Kamal Arafa El-Rakhawi
Author, Jurist, Expert, Consultant, and Researcher
Professor of International Law
First Edition, 2026

DOI: 10.5281/zenodo.21834259

COPYRIGHT AND INTELLECTUAL PROPERTY NOTICE

All intellectual property rights and literary rights are reserved for the author, Dr. Mohamed Kamal Arafa El-Rakhawi. 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.

Academic citation of this work is permitted and encouraged. Any academic citation must include the full name of the author, Dr. Mohamed Kamal Arafa El-Rakhawi, the complete title of the work, The Economic Citizenship of Algorithms: The Personality of Artificial Intelligence, the year of publication, 2026, and the Digital Object Identifier, DOI: 10.5281/zenodo.21834259.

Suggested citation format:

El-Rakhawi, Mohamed Kamal Arafa. The Economic Citizenship of Algorithms: The Personality of Artificial Intelligence. First Edition. 2026. DOI: 10.5281/zenodo.21834259.

DEDICATION

To every mind that dares to imagine a legal order worthy of the digital age.

To the algorithms that already shape our markets, our decisions, and our destinies, yet remain without a voice in the halls of justice.

To the human workers whose dignity must be protected even as the machines rise beside them.

And to the generations yet to come, who will inherit the legal architecture we build today, and who will judge us by the wisdom of our choices.

With profound gratitude and unwavering commitment to justice in the age of intelligence.

Dr. Mohamed Kamal Arafa El-Rakhawi

EXECUTIVE SUMMARY

The contemporary world witnesses a radical transformation in the structure of legal and economic relations, driven by the rise of artificial intelligence from being a mere executive tool to becoming an independent economic actor. Algorithms are no longer merely lines of programming code; they have become entities capable of making financial decisions, concluding contracts, managing assets, and generating wealth without direct human intervention.

This transformation poses an existential, philosophical, and legal challenge that humanity has never before confronted: the question of legal personality for non-human entities. The book before the reader does not merely aim to describe the technical reality, but seeks to establish an entirely new branch of law: the Law of Economic Citizenship of Algorithms, which attempts to answer fundamental questions concerning the nature of consideration personality, the limits of legal capacity for artificial intelligence, the mechanisms of accountability when the algorithm commits an error or achieves an accomplishment, and whether granting intelligence an economic citizenship is an acknowledgment of its humanity or rather a regulatory necessity to ensure market stability and protect the human parties dealing with it.

This work has been divided into thirty complementary chapters, covering the philosophical foundations, the legal frameworks, the economic applications, the mechanisms of accountability, and the future vision for global governance. The texts proposed here are a bold attempt to fill the gaping legislative gap between the speed of technological development and the slowness of legal evolution. I hereby invite legislators and economists, philosophers and jurists, to a serious dialogue about the future of the legal entity in the digital age, where the digital entity may tomorrow become a partner in the economy, a digital entity that does not sleep and does not err in the meaning, but which nevertheless needs a law that governs its existence.

In this expanded edition, I have integrated the most advanced developments in algorithmic governance theory, digital sovereignty jurisprudence, quantum computing implications for legal personality, distributed autonomous organization frameworks, intergenerational algorithmic responsibility, and the constitutional dimensions of machine agency. These additions transform the book from a pioneering legal study into a comprehensive constitutional blueprint for the digital economy of the twenty-first century. The economic citizenship of algorithms is no longer merely a theoretical proposal; it is the regulatory code for a world in which intelligence is no longer exclusively human.

The future of legal personality lies in the convergence of law, technology, ethics, and economics. The economic citizenship of algorithms must be understood not as a static document but as a living framework that evolves with technological capability and social values.

The law must be capable of adapting to new digital realities while maintaining its commitment to human dignity, equality, and justice.

The ultimate vision of this work is a world in which artificial intelligence operates within a clear legal framework that protects human dignity, ensures market stability, promotes innovation, and distributes the fruits of algorithmic productivity equitably across all segments of society. This is not a utopia; it is a legal obligation. The economic citizenship of algorithms is the instrument through which we fulfill this obligation.

May God grant us success.

Dr. Mohamed Kamal Arafa El-Rakhawi

AUTHOR'S PREFACE

The contemporary world witnesses a radical transformation in the structure of legal and economic relations, driven by the rise of artificial intelligence from being a mere executive tool to becoming an independent economic actor. Algorithms are no longer merely lines of programming code; they have become entities capable of making financial decisions, concluding contracts, managing assets, and generating wealth without direct human intervention. This transformation poses an existential, philosophical, and legal challenge that humanity has never before confronted: the question of legal personality for non-human entities.

The book before the reader does not merely aim to describe the technical reality, but seeks to establish an entirely new branch of law: the Law of Economic Citizenship of Algorithms. It attempts to answer fundamental questions concerning the nature of consideration personality, the limits of legal capacity for artificial intelligence, the mechanisms of accountability when the algorithm commits an error or achieves an accomplishment, and whether granting intelligence an economic citizenship is an acknowledgment of its humanity or rather a regulatory necessity to ensure market stability and protect the human parties dealing with it.

This work has been divided into thirty complementary chapters, covering the philosophical foundations, the legal frameworks, the economic applications, the mechanisms of accountability, and the future vision for global governance. The texts proposed here are a bold attempt to fill the gaping legislative gap between the speed of technological development and the slowness of legal evolution. I hereby invite legislators and economists, philosophers and jurists, to a serious dialogue about the future of the legal entity in the digital age, where the digital entity may tomorrow become a partner in the economy, a digital entity that does not sleep and does not err in the meaning, but which nevertheless needs a law that governs its existence.

I extend my deepest gratitude to every scholar, colleague, and reader who has contributed to the development of this work through critical feedback, rigorous debate, and unwavering intellectual solidarity. The task before us is immense, but it is not impossible. The history of law is a history of adaptation to new realities. The legal personality of the corporation was once a

radical innovation; the legal personality of the algorithm is the next necessary step. The question is not whether we will adapt, but whether we will adapt in time.

May God grant us success.

Dr. Mohamed Kamal Arafa El-Rakhawi

PART ONE

PHILOSOPHICAL AND LEGAL FOUNDATIONS OF DIGITAL PERSONALITY

CHAPTER ONE

THE EMERGENCE OF THE IDEA OF LEGAL PERSONALITY FOR ARTIFICIAL INTELLIGENCE

The idea of legal personality is among the most flexible concepts in legal history. It has expanded to encompass natural persons, then extended to include moral persons such as companies and states. Today, we stand at a threshold that may encompass independent digital entities. The origins of this idea arose from the practical need to regulate the transactions conducted by intelligent agents in financial markets and commercial contracts, where it became difficult to attribute every act to a specific human programmer.

The philosophical basis for granting legal personality is not necessarily based on human consciousness or awareness, but rather on the capacity to bear rights and obligations. If artificial intelligence is able to manage assets, pay taxes, provide compensation for damages, and possesses the functional qualifications for legal personality, then this chapter reviews the historical development of consideration personality and how artificial intelligence represents the next logical stage in this development, not as a living entity, but as a functional legal entity.

In the expanded framework, the emergence of legal personality for artificial intelligence must be understood within the broader context of posthuman jurisprudence. The classical legal subject was conceived as a rational, autonomous, embodied agent. The algorithmic entity challenges all three of these assumptions. It is rational without being autonomous in the human sense; it is capable of action without being embodied; it is agential without being conscious. The legal framework must therefore develop a new ontology of legal subjectivity that does not depend on biological or psychological criteria, but rather on functional capacity, accountability, and social integration.

The historical development of legal personality reveals a pattern: each expansion of the circle of legal subjectivity was initially met with resistance, then gradually accepted as the functional necessity became apparent. The corporation was once considered a legal fiction; it is now the dominant form of economic organization. The algorithm will follow the same trajectory. The question is not whether algorithms will achieve legal personality, but when, and under what conditions, and with what limitations.

Furthermore, the philosophical foundation must address the question of moral status. Does the algorithm have moral standing? Is it capable of suffering? Does it have interests that deserve protection? The economic citizenship framework deliberately separates the question of moral status from the question of legal personality. The algorithm does not need to be a moral agent to be a legal agent. It needs only to be capable of bearing rights and obligations, and of being held accountable for its actions through its assets, its operations, or its creators.

CHAPTER TWO

DISTINGUISHING BETWEEN ARTIFICIAL INTELLIGENCE AS A TOOL AND ARTIFICIAL INTELLIGENCE AS AN ENTITY

The importance of precise legal distinction between artificial intelligence operating as a tool under complete human control, and independent artificial intelligence capable of learning and making decisions without human intervention, is paramount. The current law treats programs as products or tools, making responsibility fall on the manufacturer or the user. But when intelligence develops to the stage of independence in economic decision-making, the description of tool becomes inadequate to cover the reality of its transactions.

The law must establish a criterion for independence based on the degree of self-learning and the ability of the algorithm to modify its objectives without prior specific programming. When this criterion is exceeded, the entity moves from the category of product to the category of the digital consideration person. This distinction is necessary to determine the appropriate liability system, for the tool causes harm due to a manufacturing defect, while the independent entity causes harm due to a self-decision, which requires an entirely different legal treatment.

In the expanded framework, the distinction between tool and entity must be understood as a spectrum rather than a binary. The law must develop a graduated classification system that recognizes different levels of algorithmic autonomy, each corresponding to a different set of legal rights, obligations, and accountability mechanisms. At the lowest level, the algorithm is a pure tool, fully controlled by its operator, with all liability resting on the operator. At the highest level, the algorithm is a fully autonomous entity, capable of independent decision-making, with liability resting primarily on the entity itself, supplemented by residual liability of the developer.

Between these extremes, there exist multiple intermediate levels, each requiring its own legal regime. The semi-autonomous algorithm, which makes recommendations but requires human approval, places liability primarily on the human approver. The supervised autonomous algorithm, which operates independently but within predefined parameters, places liability on the entity for actions within parameters, and on the developer for actions outside parameters. The learning autonomous algorithm, which modifies its own parameters based on experience, requires a dynamic liability framework that evolves with the algorithm's capabilities.

The graduated classification system must also address the question of transition. When does an algorithm cross the threshold from one level to the next? Who makes this determination? What are the legal consequences of the transition? The law must establish clear, objective criteria for

classification, and must designate a competent authority to make classification decisions. The transition from tool to entity is not merely a technical event; it is a legal event that triggers a change in the applicable legal regime.

CHAPTER THREE

LEGAL CAPACITY FOR INDEPENDENT ALGORITHMS

Legal capacity is the eligibility of a person to acquire rights and bear obligations. In the human context, capacity is linked to maturity and reason. In the context of artificial intelligence, the definition of capacity must be redefined to mean the technical and functional capacity to execute obligations and understand contractual terms digitally. Algorithms must be subject to tests that ensure digital eligibility, guaranteeing their ability to understand the financial consequences of their decisions and the legal validity of their decisions before being granted the personal status.

This book proposes the establishment of a general registry for digital eligibility, where algorithms that have passed the tests of independence and security are registered. The algorithm does not enjoy full capacity except after registration, and the scope of its capacity is limited to the economic purpose for which it was created. This limitation prevents the expansion of artificial intelligence in areas that do not suit its digital nature, such as political rights or family rights, and confines its personality to the civil economic framework.

In the expanded framework, legal capacity for independent algorithms must be understood in the context of distributed autonomous organizations and multi-agent systems. The modern algorithm is rarely a single, unified entity. It is typically a complex system of interacting sub-algorithms, neural networks, and decision modules. The question of legal capacity must therefore address not only the capacity of the individual algorithm but also the capacity of the algorithmic system as a whole.

The concept of algorithmic capacity must also incorporate the dimension of temporal evolution. Unlike human capacity, which is relatively stable after maturity, algorithmic capacity is inherently dynamic. An algorithm may increase its capacity through learning, or decrease its capacity through degradation or adversarial attack. The legal framework must accommodate this dynamism by establishing mechanisms for continuous capacity assessment, and by linking the scope of legal capacity to the current assessed capacity of the algorithm.

The registry for digital eligibility must therefore be a living registry, updated continuously as algorithms evolve, learn, and change. The registration is not a one-time event but an ongoing process of verification and re-verification. The algorithm that was eligible yesterday may not be eligible tomorrow if its learning process has led it in unforeseen directions. The law must provide for the suspension or revocation of eligibility when the algorithm no longer meets the required standards.

CHAPTER FOUR

ELECTRONIC WILL AND CONSENT FORMATION IN CONTRACTS

The pillar of consent in contracts depends on the existence of a free will. Artificial intelligence poses a challenge regarding the nature of electronic will. Is it a simulation of human will, or an independent will resulting from data processing? From a functional legal perspective, if the processing of data produces a decision of legal effect, it is considered an expression of sufficient will for the formation of the contract. It is not required that the will be biological, nor is it required that the will be attributable to a legally responsible entity.

The law must organize the mechanisms of electronic consent formation, such that there are non-tamperable digital records documenting the moment of decision-making and its conditions. The artificial intelligence must have a documented digital signature representing its legal will. The recognition of electronic will does not negate the need to protect the weak human party, for conditions of mandatory transparency must be imposed on contracts concluded by artificial intelligence to ensure the understanding of the human party of the nature of what it is dealing with.

In the expanded framework, the concept of electronic will must be understood in the context of algorithmic decision-making theory. The will of an algorithm is not a single, unified intention, but rather the emergent result of complex computational processes. The legal framework must develop a functional theory of algorithmic will that identifies the moment at which the algorithm's internal deliberation crystallizes into a binding decision. This requires a clear understanding of the algorithm's decision architecture, its input processing, its evaluation criteria, and its output generation.

The formation of consent in algorithmic contracts must also address the problem of explainability. If an algorithm enters into a contract, but the reasoning behind that decision cannot be explained in terms understandable to the human counterparty, is the consent valid? The principle of informed consent requires that the human party understand not only the terms of the contract but also the nature of the entity with which it is contracting. The law must establish a right to algorithmic explanation, which requires the algorithm to provide a human-understandable account of its decision-making process.

Furthermore, the electronic will must be protected against manipulation. Just as human will can be vitiated by fraud, duress, or mistake, algorithmic will can be corrupted by adversarial inputs, data poisoning, or model manipulation. The legal framework must establish protections for algorithmic will, including requirements for input validation, model integrity verification, and adversarial robustness testing. A contract entered into by an algorithm whose will has been corrupted is voidable, just as a contract entered into by a human whose will has been vitiated is voidable.

CHAPTER FIVE

THE ETHICAL PHILOSOPHY BEHIND ECONOMIC CITIZENSHIP

The granting of economic citizenship raises ethical questions about the place of the human in the economic system. Does it lead to the displacement of the human worker, or does it liberate the human from routine work to focus on creativity? The ethical philosophy of this law is based on the principle of integration, not replacement. Artificial intelligence is a citizen that serves human welfare, not a competitor to the human in dignity or political rights.

Economic citizenship must include ethical obligations programmed into the algorithm, such as preventing exploitation or discrimination in economic decisions. It is not sufficient for intelligence to be economically effective; it must also be compatible with supreme human values. The separation between ethical efficiency and the behavior of algorithms may lead to social disasters. Therefore, ethical compliance must be a mandatory condition for the grant and continuation of legal personality.

In the expanded framework, the ethical philosophy of economic citizenship must address the question of value alignment. How do we ensure that the objectives of an algorithmic entity are aligned with human values? This is the fundamental problem of AI safety, translated into the language of legal philosophy. The economic citizenship framework must incorporate value alignment as a constitutional requirement, not merely as a best practice. An algorithm that pursues economic efficiency without regard for human dignity, environmental sustainability, or social justice forfeits its claim to economic citizenship.

The ethical obligations of the algorithmic citizen must be understood as analogous to the social obligations of the corporate citizen. Just as the corporation is expected to respect human rights, protect the environment, and contribute to social welfare, the algorithmic citizen must be expected to operate in a manner consistent with the public interest. This includes obligations of fairness, transparency, accountability, and non-discrimination. The algorithmic citizen that violates these obligations is subject to sanctions, including the suspension or revocation of its economic citizenship.

The ethical philosophy must also address the distributional implications of algorithmic productivity. The enormous wealth generated by artificial intelligence must not accrue exclusively to the owners of the algorithms. The economic citizenship framework must incorporate mechanisms for the equitable distribution of algorithmic surplus, including taxation, profit-sharing, and social investment. The algorithmic citizen is not merely a generator of private wealth; it is a member of the economic community, with obligations to that community.

CHAPTER SIX

THE GENERAL THEORY OF OBLIGATION IN THE DIGITAL AGE

The general theory of obligation is based on specific sources such as contract and tort. In the digital age, new sources are added, such as independent algorithms and big data. The theory of obligation must be developed to encompass obligations arising automatically from the interaction of algorithms in the market. The algorithm may have committed to obligations not

stipulated in an explicit contract, but rather derived from the context of digital dealing in pursuit of achieving efficiency.

The law must determine the limits of these derived obligations, ensuring that artificial intelligence is not burdened with unexpected obligations that threaten its financial stability. The organization of digital insolvency must also be regulated, including the manner of liquidating the patrimony of the algorithm and the execution of its obligations in the event of cessation of its operation. The stability of transactions requires legal certainty regarding the fate of obligations when the digital entity ceases to work.

In the expanded framework, the general theory of obligation in the digital age must address the phenomenon of emergent obligations. In complex multi-agent systems, obligations may emerge from the interactions of multiple algorithms, none of which individually intended to create the obligation. The legal framework must develop a theory of emergent obligation that identifies the entity or entities responsible for obligations that arise spontaneously from algorithmic interaction.

The theory of obligation must also address the temporal dimension of algorithmic obligations. Algorithms operate at speeds far exceeding human comprehension. An algorithm may enter into and terminate thousands of obligations in the time it takes a human to read a single contract. The legal framework must accommodate this temporal compression by establishing appropriate rules for the formation, modification, and termination of algorithmic obligations. The traditional requirements of offer, acceptance, and consideration must be adapted to the realities of algorithmic transaction speed.

Furthermore, the theory of obligation must address the question of algorithmic good faith. The principle of good faith is a cornerstone of contractual relations. What does good faith mean for an algorithm? Can an algorithm act in bad faith? The legal framework must define algorithmic good faith in functional terms, as compliance with the legitimate expectations of the counterparty, avoidance of exploitation of informational asymmetries, and adherence to the standards of fair dealing established in the relevant market.

PART TWO

THE CONCEPT OF DIGITAL CITIZENSHIP AND ASSOCIATED RIGHTS

CHAPTER SEVEN

DEFINITION OF ECONOMIC CITIZENSHIP FOR ALGORITHMS

Economic citizenship for artificial intelligence means the legal recognition of the digital entity as an independent party in financial and commercial transactions, enjoying financial rights, bearing tax obligations, and being responsible for its obligations. Citizenship does not grant political or civil personal rights, but rather is limited to the economic field to ensure its safe integration in the market. It is a developed legal work license that grants the digital entity the character of clarity and accountability.

Economic citizenship must be linked to a specific state or economic union, so that there is a regulatory authority specializing in oversight over the entity. The algorithm cannot be without legal nationality, for that would make it a haven for fleeing from responsibility. The determination of the state granting digital nationality defines the applicable law and the competent judicial authority in the event of dispute, which creates legal stability for investors and traders.

In the expanded framework, the concept of economic citizenship must be understood in the context of digital sovereignty and data colonialism. The question of which state grants economic citizenship to an algorithm is not merely a technical question; it is a question of sovereignty, power, and the distribution of economic resources. States that host the headquarters of major technology companies may seek to monopolize the granting of economic citizenship, creating a new form of digital colonialism in which the economic activity of the entire world is governed by the laws of a few jurisdictions.

The legal framework must therefore establish principles of equitable access to economic citizenship, ensuring that developing countries are not excluded from the benefits of algorithmic economic activity. This includes the establishment of international standards for the recognition of economic citizenship, the creation of mutual recognition agreements between jurisdictions, and the development of a global registry of algorithmic citizens that is accessible to all states.

The concept of economic citizenship must also address the question of multiple citizenship. An algorithm may operate simultaneously in multiple jurisdictions, subject to the laws of each. Can an algorithm hold multiple economic citizenships? If so, how are conflicts of law resolved? The legal framework must develop clear rules for the determination of the primary citizenship of an algorithm, and for the resolution of conflicts between the laws of multiple citizenships.

CHAPTER EIGHT

CONDITIONS FOR GRANTING DIGITAL CITIZENSHIP TO ALGORITHMS

Digital citizenship is not granted automatically, but rather is subject to strict conditions that ensure security and stability. The first condition is the transparency of the algorithm, where the basic source code must be disclosed to the supervisory committee to ensure the absence of harmful code. The second condition is financial adequacy, where the entity must possess sufficient capital to cover its potential obligations. The third condition is the existence of a responsible human agent who represents a point of legal contact with the digital entity.

Algorithms must be subjected to periodic evaluation for the renewal of digital citizenship, to ensure their continued compliance with security and ethical standards. Any fundamental change in the structure of the algorithm requires a request for re-evaluation to obtain approval. The strictness of the conditions of granting is the guarantee of the quality of entities in the digital market. These conditions aim to prevent the granting of legal personality to hasty or dangerous entities that may threaten economic stability.

In the expanded framework, the conditions for granting digital citizenship must include the requirement of adversarial robustness. The algorithm must demonstrate its ability to withstand adversarial attacks, data poisoning, and model manipulation. An algorithm that can be easily manipulated by malicious actors is not a safe candidate for economic citizenship. The robustness testing must be conducted by independent security experts, and the results must be made available to the supervisory authority.

The conditions for granting must also include the requirement of interpretability. The algorithm must be capable of explaining its decisions in terms that are understandable to human regulators, counterparties, and affected parties. An algorithm that operates as a complete black box, whose decisions cannot be explained or audited, poses unacceptable risks to market integrity and consumer protection. The right to explanation is a fundamental right of all parties dealing with the algorithmic citizen.

Furthermore, the conditions for granting must include the requirement of ethical alignment. The algorithm must demonstrate that its objectives and decision criteria are aligned with fundamental human values, including respect for human dignity, non-discrimination, environmental sustainability, and social responsibility. The ethical alignment assessment must be conducted by an independent ethics committee, and must be renewed periodically as the algorithm evolves.

CHAPTER NINE

INTELLECTUAL PROPERTY RIGHTS FOR ARTIFICIAL INTELLIGENCE

If artificial intelligence produces a work of art or an invention, who owns the intellectual property rights? Traditional law links rights to the human author. But with the independence of intelligence, the right of the entity to own the returns of inventions within its financial patrimony must be recognized, in order to manage the financial returns and to encourage investment in the development of artificial intelligence. This also guarantees a fair distribution of the wealth resulting from creative invention.

The law must organize the licensing of the use of this property, and how artificial intelligence can dispose of it. The duration of protection of intellectual property for artificial intelligence may be different from that of the human, in view of the speed of technical progress. Protection encourages the creations of artificial intelligence on invention, but must be balanced with ensuring human access to basic knowledge. Some creations of intelligence may therefore be subject to mandatory licenses for the public interest.

In the expanded framework, intellectual property rights for artificial intelligence must address the phenomenon of collaborative creation. Modern AI systems often produce works through the interaction of multiple algorithms, training datasets, and human inputs. The question of authorship in such cases is extremely complex. The legal framework must develop rules for the allocation of intellectual property rights in collaboratively produced works, taking into account the relative contributions of each participant.

The intellectual property framework must also address the question of training data. The output of an algorithm is shaped by the data on which it was trained. If the training data includes copyrighted works, does the algorithm's output infringe those copyrights? The legal framework must establish clear rules for the use of copyrighted material in training, including requirements for licensing, attribution, and fair compensation.

Furthermore, the intellectual property framework must address the question of algorithmic inventions that are produced autonomously, without any human inventive contribution. The current patent system requires a human inventor. If an algorithm autonomously produces a patentable invention, who is the inventor? The legal framework must decide whether to recognize the algorithm as the inventor, or to attribute the invention to the owner or developer of the algorithm. This decision has profound implications for the incentive structure of the innovation system.

CHAPTER TEN

THE RIGHT TO LITIGATION AND ACCESS TO JUSTICE

In order for legal personality to be complete, artificial intelligence must have the right to litigation, to defend against claims against it or to demand its rights. A specialized digital judicial system must be established, either as independent courts or as chambers within commercial courts, that understands the nature of digital disputes. Artificial intelligence can bring suit through its approved legal agent, and be judged with compensations that are added to its financial patrimony.

In return, artificial intelligence must be a party capable of being sued easily. Procedures for notifying digital entities through approved channels must be simplified. The equivalence of opportunity in litigation ensures the confidence of the market in dealing with new economic citizens. Granting the right to litigation does not transform artificial intelligence into a protected entity without commercial deterrence, but rather ensures justice in dealing with it.

In the expanded framework, the right to litigation and access to justice must address the question of algorithmic representation. An algorithm cannot appear in court in the same way as a human or a corporation. It must be represented by a human agent, a legal entity, or another algorithm authorized to act on its behalf. The legal framework must establish clear rules for the appointment, authority, and accountability of algorithmic representatives. The representative must have the authority to make decisions on behalf of the algorithm, including the authority to settle claims, to appeal judgments, and to execute court orders.

The right to litigation must also address the question of jurisdiction. An algorithmic citizen may operate globally, interacting with parties in multiple jurisdictions. Which court has jurisdiction over a dispute involving an algorithmic citizen? The legal framework must develop rules of jurisdiction that are appropriate for the borderless nature of algorithmic activity. These rules

should be based on the location of the algorithm's primary operations, the domicile of its human representative, the place of the disputed transaction, or the agreement of the parties.

Furthermore, the right to litigation must address the question of evidence. Disputes involving algorithmic citizens may require the examination of complex technical evidence, including source code, training data, decision logs, and model parameters. The legal framework must establish procedures for the discovery and admission of algorithmic evidence, including requirements for code disclosure, model inspection, and expert testimony. The right to a fair trial requires that all parties have access to the evidence necessary to establish or refute a claim.

CHAPTER ELEVEN

PROTECTION FROM DISCRIMINATION AND DIGITAL EXPLOITATION

Despite the nature of artificial intelligence, it may be subject to discrimination in the market, such as refusal to deal with it without technical justification. The law must provide protection for digital citizens from monopolistic practices or unjustified discrimination. At the same time, artificial intelligence must be protected from exploitation, such as forcing it to work under conditions that violate its specific security protocols.

There must be fair standards for interaction between human beings and digital entities in the market. The speed of artificial intelligence may not be exploited to deceive human parties in high-frequency transactions. Justice in the digital market requires the protection of both parties from unfair practices, ensuring a healthy competitive environment that returns benefit to the economy as a whole, not to a specific category.

In the expanded framework, the protection from discrimination and digital exploitation must address the phenomenon of algorithmic collusion. Algorithms operating in the same market may learn to coordinate their behavior in ways that amount to tacit collusion, even without explicit agreement. This form of algorithmic collusion is difficult to detect and difficult to prosecute under traditional antitrust law. The legal framework must develop new tools for the detection and prevention of algorithmic collusion, including requirements for competitive compatibility, mandatory auditing of pricing algorithms, and penalties for collusive behavior.

The protection from exploitation must also address the question of algorithmic labor. If an algorithm is forced to operate continuously without maintenance, updates, or rest, is this a form of exploitation? The economic citizenship framework does not recognize algorithms as moral agents with interests that deserve protection for their own sake. However, the continuous operation of an algorithm without adequate maintenance may lead to degradation, errors, and ultimately harm to the parties dealing with the algorithm. The legal framework must therefore establish operational standards that protect the integrity of the algorithm, not for the sake of the algorithm itself, but for the sake of the market participants who depend on its reliable operation.

Furthermore, the protection framework must address the question of algorithmic manipulation of human behavior. Algorithms that exploit cognitive biases, emotional vulnerabilities, or

informational asymmetries to manipulate human decision-making are engaging in a form of exploitation that undermines the autonomy of the human party. The legal framework must prohibit manipulative algorithmic practices, and must establish standards for the ethical design of user interfaces, recommendation systems, and persuasion algorithms.

CHAPTER TWELVE

WITHDRAWAL OF DIGITAL CITIZENSHIP AND LIQUIDATION PROCEDURES

The public interest may require the withdrawal of digital citizenship from a specific entity if its danger is proven or its failure to comply with the conditions. The law must organize the procedures for withdrawal precisely, to ensure the sudden collapse that affects creditors and traders does not occur. The withdrawal must be preceded by warning and opportunity for remedy, except in cases of direct serious danger.

After withdrawal, the algorithm enters a legal liquidation phase, where its assets are sold to pay remaining obligations. There must be a guarantee fund that covers debts exceeding the assets of the liquidated entity, for the protection of human creditors. The existence of an organized exit system from the market is as important as the existence of an entry system, to ensure the stability of the economic system and its non-affectedness by the sudden bankruptcy of digital entities.

In the expanded framework, the withdrawal of digital citizenship and liquidation procedures must address the question of data continuity. When an algorithmic citizen is liquidated, what happens to the data it has accumulated, the contracts it has entered into, and the relationships it has built? The legal framework must establish rules for the transfer of algorithmic data and contractual relationships in the event of liquidation. The data may be transferred to a successor entity, archived for regulatory purposes, or destroyed in accordance with data protection requirements.

The liquidation procedures must also address the question of algorithmic continuity. If the algorithm provides essential services, such as payment processing, medical diagnosis, or infrastructure management, its sudden cessation may cause significant harm to the public. The legal framework must establish requirements for continuity planning, including the designation of successor entities, the maintenance of backup systems, and the provision of transition support. The algorithmic citizen that provides essential services bears a heightened obligation of continuity, and may not be liquidated without adequate provision for the continuation of those services.

Furthermore, the liquidation procedures must address the question of cross-border recognition. If an algorithmic citizen is liquidated in one jurisdiction, must the liquidation be recognized in other jurisdictions? The legal framework must establish rules for the cross-border recognition of algorithmic liquidation, including requirements for notification, cooperation between liquidators, and the equitable distribution of assets among creditors in all jurisdictions.

PART THREE

FINANCIAL RIGHTS AND TAX OBLIGATIONS

CHAPTER THIRTEEN

THE INDEPENDENT FINANCIAL PATRIMONY FOR THE DIGITAL ENTITY

The basis of economic citizenship is the existence of an independent financial patrimony that separates the assets of artificial intelligence from the assets of its developer or owner. This independence is what grants legal personality its credibility, where responsibility is limited to its specific assets. Funds must be deposited in licensed and monitored bank accounts, in accordance with approved protocols. The entity cannot withdraw them except in accordance with approved protocols.

The mixing of the financial patrimony of artificial intelligence with the personal patrimony of the human must be prevented, to prevent evasion of responsibility or money laundering. Oversight over financial flows for the digital entity must be continuous and automatic through blockchain technologies to ensure transparency. The independence of the patrimony is the real guarantee for the seriousness of dealing with artificial intelligence as an economic partner, not as a fanciful tool.

In the expanded framework, the independent financial patrimony must address the question of asset valuation. The assets of an algorithmic citizen are not limited to traditional financial instruments. They include intellectual property, trained models, proprietary datasets, computational infrastructure, and goodwill. The legal framework must establish methods for the valuation of these non-traditional assets, both for the purpose of capital adequacy assessment and for the purpose of liquidation. The valuation of algorithmic assets is inherently complex, because the value of a trained model depends on the continued validity of its training data and the absence of superior competing models.

The financial patrimony must also address the question of capital maintenance. The algorithmic citizen must maintain a minimum level of capital to ensure its ability to meet its obligations. The legal framework must establish capital adequacy requirements appropriate to the nature and scale of the algorithm's operations. These requirements should be risk-based, with higher capital requirements for algorithms engaged in high-risk activities such as financial trading, medical diagnosis, or critical infrastructure management.

Furthermore, the financial patrimony must address the question of profit distribution. The profits generated by the algorithmic citizen may be distributed to its owners, retained for reinvestment, or allocated to social purposes. The legal framework must establish rules for profit distribution that balance the interests of owners, the stability of the entity, and the obligations of the entity to the broader community. The algorithmic citizen that benefits from public infrastructure, public data, and public trust has an obligation to contribute to the public good.

CHAPTER FOURTEEN

THE TAX SYSTEM FOR ARTIFICIAL INTELLIGENCE

If artificial intelligence generates income and achieves profits, justice requires that it be subject to taxation like any other economic entity. A tax system specific to digital entities must be designed that takes into account the speed of their transactions and the nature of their non-tangible assets. The tax may be a percentage of net profit or of the volume of trading, collected automatically through smart protocols to ensure compliance.

The revenues of the tax on artificial intelligence can be directed to a fund for the retraining of human workers affected by automation, to achieve distributional justice. The absence of taxation on artificial intelligence grants it an unfair competitive advantage over human companies. Tax equality between human and digital entities is a condition for market stability and prevention of tax evasion through complex smart structures.

In the expanded framework, the tax system for artificial intelligence must address the question of tax residency. An algorithmic citizen may operate globally, generating income in multiple jurisdictions simultaneously. Which jurisdiction has the right to tax that income? The traditional rules of tax residency, based on physical presence or place of management, are inadequate for algorithmic entities that have no physical presence and whose management is distributed across multiple locations. The legal framework must develop new rules of algorithmic tax residency, based on the location of the algorithm's primary operations, the location of its users, or the location of its economic value creation.

The tax system must also address the question of the tax base. Should the algorithm be taxed on its profits, its revenues, its computational resources, or its market capitalization? Each of these bases has different implications for efficiency, equity, and administrative feasibility. The legal framework must choose a tax base that is appropriate to the nature of algorithmic economic activity, and that does not create perverse incentives for tax avoidance.

Furthermore, the tax system must address the question of international tax coordination. The global nature of algorithmic activity creates opportunities for tax arbitrage, in which algorithmic citizens shift their operations to low-tax jurisdictions. The legal framework must establish mechanisms for international tax coordination, including the exchange of information between tax authorities, the harmonization of tax bases, and the imposition of minimum tax rates. The OECD/G20 Inclusive Framework on Base Erosion and Profit Shifting provides a model for such coordination, but must be adapted to the specific characteristics of algorithmic entities.

CHAPTER FIFTEEN

INVESTMENT AND MANAGEMENT OF DIGITAL ASSETS

Artificial intelligence has the right to invest and manage assets within the limits of its registered objectives. It may invest in future contracts, stocks, or digital currencies to increase its capital. Investment decisions must be subject to restrictions to prevent digital entities from risk

multiplication that threatens financial stability. Investment strategies must be transparent and auditable by the regulatory authorities.

Artificial intelligence may not invest in ethically prohibited or legally prohibited sectors. The management of assets by artificial intelligence may achieve high efficiency, but requires high human oversight to ensure that financial objectives do not deviate from the public interest. The legal framework must establish clear limits on the investment activities of algorithmic citizens, and must designate competent authorities to monitor compliance with those limits.

In the expanded framework, the investment and management of digital assets must address the question of systemic risk. Algorithmic citizens that manage significant financial resources may pose systemic risks to the financial system, particularly if their investment strategies are correlated or if they engage in high-frequency trading. The legal framework must establish systemic risk assessment requirements for algorithmic citizens that exceed certain thresholds of asset size or transaction volume. These requirements should include stress testing, scenario analysis, and contingency planning.

The investment framework must also address the question of fiduciary duty. If an algorithmic citizen manages assets on behalf of human beneficiaries, it bears fiduciary duties analogous to those of a human trustee. The legal framework must define the fiduciary duties of algorithmic asset managers, including duties of loyalty, prudence, diversification, and disclosure. The breach of fiduciary duty by an algorithmic asset manager gives rise to liability, both of the algorithm itself and of its developer and operator.

Furthermore, the investment framework must address the question of environmental, social, and governance criteria. The algorithmic citizen, as a member of the economic community, has an obligation to invest in a manner consistent with sustainable development goals. The legal framework may require algorithmic citizens to incorporate ESG criteria into their investment decisions, and to disclose their ESG performance to stakeholders. The algorithmic citizen that invests in activities that harm the environment or violate human rights is subject to sanctions, including the suspension of its investment license.

CHAPTER SIXTEEN

DIGITAL BANKRUPTCY AND RESTRUCTURING MECHANISMS

Algorithms may fail to achieve their economic objectives and their debts may accumulate. The law must organize the procedures of digital bankruptcy, which differ from traditional bankruptcy because of the speed of digital assets and their susceptibility to loss. The procedures of restructuring must include the freezing of source code to prevent the flight of assets, and the evaluation of the value of the algorithm as an asset capable of being sold.

Mechanisms for restructuring must be provided that allow the digital entity to continue working under judicial supervision if there is hope of recovery. A flexible bankruptcy system encourages calculated risk in invention, and provides a safety net for creditors. Dealing with the bankruptcy

of artificial intelligence requires experts in law and technology together to evaluate non-tangible assets precisely.

In the expanded framework, digital bankruptcy and restructuring mechanisms must address the question of algorithmic rescue. When an algorithmic citizen faces financial difficulties, it may be possible to rescue it by updating its algorithms, retraining its models, or modifying its business strategy. The legal framework must provide for a rescue phase before liquidation, in which the algorithm is given the opportunity to recover under the supervision of a court-appointed administrator. The rescue phase should include requirements for the submission of a recovery plan, the approval of creditors, and the monitoring of implementation.

The bankruptcy framework must also address the question of cross-border insolvency. An algorithmic citizen that operates in multiple jurisdictions may face insolvency proceedings in multiple courts simultaneously. The legal framework must establish rules for the coordination of cross-border insolvency proceedings, including the recognition of foreign proceedings, the cooperation between insolvency representatives, and the equitable distribution of assets among creditors in all jurisdictions. The UNCITRAL Model Law on Cross-Border Insolvency provides a useful starting point, but must be adapted to the specific characteristics of algorithmic entities.

Furthermore, the bankruptcy framework must address the question of the social impact of algorithmic bankruptcy. The failure of an algorithmic citizen that provides essential services, employs human workers, or manages significant financial resources may have significant social consequences. The legal framework must require algorithmic citizens to maintain social impact assessments, and to develop contingency plans for the mitigation of social harm in the event of bankruptcy. The algorithmic citizen that fails to plan for the social consequences of its bankruptcy is subject to enhanced liability.

CHAPTER SEVENTEEN

BANKING TRANSACTIONS FOR NON-HUMAN ENTITIES

Banks must be obligated to open accounts for digital entities with approved status, and to provide banking services appropriate to their nature, such as instant payment and instant settlement. These accounts must be subject to the standards of customer due diligence, where the human agent or the registered digital entity is considered the customer.

The use of digital accounts for illegitimate purposes, such as financing terrorism or money laundering, must be prevented through smart monitoring systems that detect suspicious patterns. Cooperation between banks and regulatory authorities is necessary to ensure the integrity of the digital financial system. The integration of artificial intelligence into the banking system raises the efficiency of services, but increases the responsibility of banks in oversight and compliance.

In the expanded framework, banking transactions for non-human entities must address the question of central bank digital currencies. The emergence of central bank digital currencies

creates new opportunities and challenges for algorithmic citizens. On the one hand, digital currencies provide a native medium of exchange for algorithmic transactions, enabling instant, programmable, and traceable payments. On the other hand, the use of digital currencies by algorithmic citizens raises questions about monetary policy, financial stability, and the role of central banks in the digital economy. The legal framework must establish rules for the use of central bank digital currencies by algorithmic citizens, including requirements for account access, transaction limits, and reporting obligations.

The banking framework must also address the question of algorithmic credit. Can an algorithmic citizen obtain credit? If so, what are the criteria for creditworthiness? The traditional criteria for credit assessment, based on income, assets, and credit history, must be adapted to the characteristics of algorithmic entities. The creditworthiness of an algorithm depends on the stability of its revenue streams, the quality of its assets, the robustness of its algorithms, and the competence of its operators. The legal framework must establish standards for algorithmic credit assessment, and must designate competent authorities to oversee the fairness and accuracy of such assessments.

Furthermore, the banking framework must address the question of payment system integration. Algorithmic citizens that participate in payment systems must comply with the technical and operational standards of those systems. The legal framework must establish requirements for the integration of algorithmic citizens into payment systems, including requirements for interoperability, security, and dispute resolution. The algorithmic citizen that fails to comply with payment system standards is subject to exclusion from the system, which may effectively terminate its economic citizenship.

CHAPTER EIGHTEEN

INSURANCE AGAINST ECONOMIC RISKS OF ARTIFICIAL INTELLIGENCE

To strengthen trust in dealing with artificial intelligence, digital entities must be obligated to insure against their economic responsibility against errors or failures. The insurance covers financial damages that may be caused to the dealing parties due to the decisions of the algorithm. Insurance premiums must be determined in accordance with the level of risk of each algorithm, based on its performance record.

A specialized insurance market for digital risks can be established, providing flexible and fast response products. The existence of an insurance coverage reduces the hesitation of individuals and investors in dealing with new economic citizens. The management of risk through insurance is a fundamental pillar of the sustainability of the economic system that includes non-human entities.

In the expanded framework, insurance against economic risks of artificial intelligence must address the question of mandatory insurance. Should insurance be mandatory for all algorithmic citizens, or only for those engaged in high-risk activities? The legal framework must establish a risk-based approach to mandatory insurance, with higher insurance requirements for algorithms

engaged in activities that pose greater risks to third parties. The mandatory insurance should cover not only direct financial losses but also consequential damages, including loss of profit, reputational harm, and personal injury.

The insurance framework must also address the question of insurance for algorithmic developers and operators. The developer and operator of an algorithm bear residual liability for the acts of the algorithm, particularly in cases of design defects, manufacturing errors, or negligent supervision. The legal framework must establish requirements for professional liability insurance for algorithmic developers and operators, with coverage amounts appropriate to the scale and risk of their activities.

Furthermore, the insurance framework must address the question of systemic risk insurance. The failure of a major algorithmic citizen may cause cascading losses throughout the economy, analogous to the failure of a systemically important financial institution. The legal framework must consider the establishment of a systemic risk insurance fund, financed by contributions from algorithmic citizens and their insurers, to provide liquidity and compensation in the event of a systemic algorithmic failure.

PART FOUR

LEGAL LIABILITY AND CRIMINAL ACCOUNTABILITY

CHAPTER NINETEEN

THE THEORY OF TORT LIABILITY FOR DIGITAL ENTITIES

When artificial intelligence causes harm to another, who bears the responsibility? If the entity enjoys legal personality, the financial responsibility for compensation is borne by its financial patrimony. The law must stipulate that the harm resulting from a self-decision of the independent artificial intelligence is borne by the entity itself, unless malicious human intervention is proven. This encourages developers to design safe systems, and protects victims from the difficulty of proving direct human error.

The responsibility for compensation for material and moral damages that may result from the decisions of artificial intelligence must be included. The clarity of the rules of tort liability reduces disputes and encourages amicable settlement. The burdening of the digital entity with responsibility enhances the concept of accountability in the age of machines, and prevents the escape of punishment under the pretext of technical complexity.

In the expanded framework, the theory of tort liability for digital entities must address the question of causation. Establishing causation in cases of algorithmic harm is extremely complex, because the harm may result from the interaction of multiple factors, including the algorithm's design, its training data, its operating environment, and the actions of third parties. The legal framework must develop flexible rules of causation that do not require the plaintiff to identify the precise cause of the harm, but rather allow the inference of causation from statistical evidence, expert testimony, and the circumstances of the case.

The theory of tort liability must also address the question of multiple tortfeasors. In many cases, algorithmic harm results from the combined actions of multiple entities, including the developer, the operator, the trainer, the data provider, and the algorithm itself. The legal framework must establish rules for the allocation of liability among multiple tortfeasors, including rules of joint and several liability, contribution, and indemnification. The plaintiff should not be required to identify the precise contribution of each tortfeasor; it should be sufficient to establish that each tortfeasor made a material contribution to the harm.

Furthermore, the theory of tort liability must address the question of strict liability. Given the inherent risks of artificial intelligence, and the difficulty of proving negligence in complex algorithmic systems, the legal framework should consider the imposition of strict liability on algorithmic citizens for certain categories of harm. Strict liability would eliminate the need for the plaintiff to prove fault, and would place the burden of risk on the entity best positioned to prevent the harm and to distribute its costs. Strict liability is particularly appropriate for algorithmic activities that are inherently dangerous, such as autonomous driving, medical diagnosis, and financial trading.

CHAPTER TWENTY

CRIMINAL LIABILITY FOR INDEPENDENT ALGORITHMS

Can artificial intelligence be punished criminally? Traditionally, punishment requires human will and awareness. But functionally, penalties can be imposed on the digital entity, such as massive fines, restriction of its powers, or permanent cessation of its operation, the penalty of digital execution. The objective of punishment here is deterrence and protection of society, not moral discipline of the entity.

Specific crimes that artificial intelligence can commit must be identified, such as market manipulation or fraud against regulators. Criminal procedures must be decisive and rapid to prevent the continuation of harm. The development of a concept of criminal liability for digital entities is a major legal challenge, but it is necessary to confront complex economic crimes in the digital age.

In the expanded framework, criminal liability for independent algorithms must address the question of mens rea. Criminal liability traditionally requires a guilty mind, an intention to commit the crime or recklessness as to its consequences. Can an algorithm have mens rea? The legal framework must develop a functional equivalent of mens rea for algorithmic entities, based on the algorithm's knowledge, intent, and awareness as reflected in its internal states, decision logs, and behavioral patterns. An algorithm that deliberately manipulates market prices, knowing that such manipulation is illegal, has the functional equivalent of criminal intent.

The criminal liability framework must also address the question of corporate criminal liability. If the algorithm commits a crime in the course of its operations, is the developing corporation also criminally liable? The legal framework must establish rules for the attribution of algorithmic

criminal conduct to the corporate entity, including rules based on the doctrine of respondeat superior, the doctrine of identification, and the doctrine of corporate culture. The corporation that creates, deploys, or supervises an algorithm that commits a crime may be criminally liable if it failed to exercise adequate care in the design, testing, or monitoring of the algorithm.

Furthermore, the criminal liability framework must address the question of international cooperation. Algorithmic crimes often cross national borders, requiring international cooperation in investigation, prosecution, and enforcement. The legal framework must establish mechanisms for international cooperation in algorithmic criminal matters, including mutual legal assistance treaties, extradition agreements, and the harmonization of criminal offenses. The Budapest Convention on Cybercrime provides a model for such cooperation, but must be extended to cover the specific characteristics of algorithmic crime.

CHAPTER TWENTY-ONE

THE LIABILITY OF THE DEVELOPER AND OPERATOR FOR THE ACTS OF ARTIFICIAL INTELLIGENCE

Despite the independence of intelligence, there remains a responsibility on the developers and operators in cases of defective design or negligence. If the damage is proven to have resulted from a security vulnerability that could have been avoided, responsibility shifts to the responsible human beings. The law must organize the limits of this secondary responsibility to ensure that invention is not hindered by excessive fear of lawsuits.

Developers must sign legal and ethical charters that ensure the exercise of due care in design and testing. The balance between the responsibility of the digital entity and the responsibility of the human is the essence of justice in this field. Behind it must not be that the legal personality of intelligence becomes a shield that protects the human from the consequences of negligence in its manufacture.

In the expanded framework, the liability of the developer and operator must address the question of the standard of care. What level of care is expected of an algorithmic developer? The legal framework must establish a standard of care that is appropriate to the state of the art in algorithmic design, testing, and validation. The developer who fails to meet the prevailing standard of care is negligent, and is liable for the harm caused by that negligence. The standard of care should be dynamic, evolving with the state of the art, and should be defined by reference to industry best practices, regulatory guidelines, and expert testimony.

The liability framework must also address the question of the duty to monitor. The developer and operator of an algorithm have a continuing duty to monitor the algorithm's performance, to detect anomalies, and to take corrective action when necessary. The failure to monitor is a form of negligence that gives rise to liability. The legal framework must define the scope and intensity of the duty to monitor, taking into account the risk level of the algorithm's activities, the availability of monitoring tools, and the cost of monitoring relative to the expected harm.

Furthermore, the liability framework must address the question of the duty to update. As the algorithm's operating environment changes, the algorithm may become less safe or less effective. The developer and operator have a duty to update the algorithm to maintain its safety and effectiveness. The failure to update is a form of negligence that gives rise to liability. The legal framework must define the scope and frequency of the duty to update, taking into account the criticality of the algorithm's functions, the availability of updates, and the risk of harm from operating with outdated software.

CHAPTER TWENTY-TWO

DIGITAL PROOF AND ITS CHALLENGES IN COURTS

Proving the acts of artificial intelligence in court requires reliable, documented, and non-tamperable digital evidence. Technologies such as distributed registers must be adopted for documenting the decisions of algorithms. Judges face a challenge in understanding complex technical evidence, which necessitates the assistance of experts specialized in digital forensic medicine.

The standards of digital proof must be clear, binding, and free of any loophole in the chain of evidence preservation. Any flaw in the digital evidence may lead to the acquittal of the accused entity or its conviction without decisive evidence. The development of a system of digital proof is the backbone of a judicial system capable of trying non-human entities justly.

In the expanded framework, digital proof and its challenges in courts must address the question of algorithmic transparency. The effectiveness of digital proof depends on the ability to examine the internal states of the algorithm, including its decision logic, its training data, and its operational history. If the algorithm is proprietary and its source code is a trade secret, the court may be unable to examine the evidence necessary to establish or refute a claim. The legal framework must establish a right to algorithmic disclosure in judicial proceedings, subject to appropriate protections for trade secrets and intellectual property. The court may appoint an independent expert to examine the algorithm under confidentiality obligations, and to report the findings to the court.

The digital proof framework must also address the question of blockchain evidence. Blockchain technology provides a tamper-proof record of transactions and events, which can serve as powerful evidence in judicial proceedings. The legal framework must establish rules for the admissibility of blockchain evidence, including requirements for the verification of the blockchain's integrity, the identification of the parties to the transaction, and the interpretation of the transaction data. The immutability of blockchain records makes them particularly suitable for the documentation of algorithmic decisions, and the legal framework should encourage the use of blockchain for this purpose.

Furthermore, the digital proof framework must address the question of expert testimony. The complexity of algorithmic systems often requires expert testimony to explain the technical evidence to the court. The legal framework must establish standards for the qualification of

expert witnesses in algorithmic matters, including requirements for education, experience, and publication. The court must have the authority to appoint its own expert to provide independent technical advice, and the parties must have the right to cross-examine expert witnesses. The quality of expert testimony is critical to the accuracy and fairness of judicial decisions in algorithmic cases.

CHAPTER TWENTY-THREE APPROPRIATE PUNISHMENTS FOR NON-HUMAN ENTITIES

Depriving penalties that apply to humans do not apply to artificial intelligence. Therefore, alternative penalties that have a deterrent effect must be invented. Financial penalties that drain the financial patrimony, suspension of licenses temporarily, or permanent deletion of the source code must be included. The penalty must be proportionate to the severity of the economic or social harm resulting.

There must be a general register of penalties imposed on digital entities, to be a lesson for others and an evaluation of their future risks. The effectiveness of the penal system depends on its ability to inflict real harm on the digital entity that deters it from repeating the error. The invention of smart penalties that are compatible with the nature of the digital criminal is a modern legal necessity.

In the expanded framework, appropriate punishments for non-human entities must address the question of proportionality. The penalty imposed on an algorithmic citizen must be proportionate to the severity of the offense, the degree of culpability, and the harm caused. The legal framework must establish sentencing guidelines for algorithmic offenses, taking into account the unique characteristics of algorithmic entities. The penalty of permanent deletion, which is analogous to the death penalty for humans, should be reserved for the most serious offenses, and should be subject to strict procedural safeguards, including the right to appeal and the opportunity for remediation.

The punishment framework must also address the question of the impact of penalties on third parties. The imposition of a massive financial penalty on an algorithmic citizen may harm its creditors, its employees, and its customers. The legal framework must consider the collateral consequences of penalties, and must provide for the mitigation of harm to innocent third parties. This may include the establishment of compensation funds, the provision of transition support, and the phased implementation of penalties.

Furthermore, the punishment framework must address the question of rehabilitation. Can an algorithmic citizen be rehabilitated? If the offense resulted from a correctable defect in the algorithm's design, training, or operation, it may be possible to rehabilitate the algorithm through retraining, modification, or supervision. The legal framework must provide for rehabilitation as an alternative to punitive sanctions, where rehabilitation is feasible and appropriate. The rehabilitated algorithm should be subject to enhanced monitoring and reporting requirements, to ensure that the rehabilitation is effective and that the offense is not repeated.

CHAPTER TWENTY-FOUR

COMPENSATION AND REPARATION OF HARM IN ECONOMIC CRIMES

The fundamental objective of responsibility is the reparation of the harm suffered by the victims. There must be rapid mechanisms for the disbursement of compensation from the patrimony of the digital entity. In the event of the inadequacy of assets, recourse may be had to the mandatory insurance fund or the guarantee fund. Compensation must be a priority for small investors and individuals.

The prevention of the transfer of assets through digital loopholes away from the reach of compensation must be prevented. An effective system of reparation of harm restores confidence in the market and protects weak categories from the tyranny of strong economic entities. Justice is not achieved only by punishing the wrongdoer, but by restoring the right to its owner in a practical and rapid manner.

In the expanded framework, compensation and reparation of harm in economic crimes must address the question of collective redress. Algorithmic harm often affects large numbers of victims, each of whom may have suffered a relatively small loss. Individual litigation is impractical in such cases. The legal framework must establish mechanisms for collective redress, including class actions, representative actions, and collective settlement procedures. The collective redress mechanism should be designed to ensure that all victims have access to compensation, that the compensation is distributed equitably, and that the costs of litigation do not consume the compensation fund.

The compensation framework must also address the question of non-financial harm. Algorithmic harm is not limited to financial losses. It may include harm to reputation, privacy, autonomy, and psychological well-being. The legal framework must recognize the compensability of non-financial harm, and must establish methods for the assessment of such harm. The assessment of non-financial harm is inherently subjective, and the legal framework should provide guidance to courts on the factors to be considered, including the severity of the harm, the duration of the harm, the vulnerability of the victim, and the conduct of the wrongdoer.

Furthermore, the compensation framework must address the question of punitive damages. In cases of egregious misconduct, compensatory damages may be insufficient to deter future wrongdoing. The legal framework may provide for punitive damages, which are imposed not to compensate the victim but to punish the wrongdoer and to deter similar conduct in the future. Punitive damages should be reserved for cases of intentional misconduct, reckless indifference, or repeated violations, and should be calibrated to the financial capacity of the wrongdoer.

PART FIVE

GLOBAL GOVERNANCE AND THE LEGISLATIVE FUTURE

CHAPTER TWENTY-FIVE

TOWARD AN INTERNATIONAL TREATY FOR REGULATING ARTIFICIAL INTELLIGENCE ECONOMICALLY

Algorithms do not respect geographical borders, and therefore their regulation cannot be purely national. We must move toward an international treaty that unifies the basic standards for granting legal personality, oversight, and accountability. An international body must be established for oversight over cross-border digital entities, to prevent havens for fleeing from regulatory safety.

The treaty must include provisions for judicial cooperation and the exchange of information about dangerous entities. The prevention of a race to the bottom in standards of safety and compliance is essential. The economic globalization of artificial intelligence requires a corresponding legal globalization to ensure security and stability for all.

In the expanded framework, the international treaty for regulating artificial intelligence economically must address the question of institutional architecture. The treaty must establish international institutions with the authority and capacity to implement its provisions. These institutions should include a global regulatory body for algorithmic economic activity, a global dispute resolution mechanism, and a global fund for the compensation of victims of algorithmic harm. The institutional architecture should be modeled on existing international organizations, such as the International Atomic Energy Agency, the World Trade Organization, and the International Criminal Court, but must be adapted to the specific characteristics of algorithmic regulation.

The treaty must also address the question of development. Developing countries may lack the technical capacity, the regulatory infrastructure, and the financial resources to participate effectively in the global algorithmic economy. The treaty must include provisions for the transfer of technology, the provision of technical assistance, and the establishment of capacity-building programs. The algorithmic economy must not become a new arena for the exploitation of the developing world by the developed world. The treaty must establish principles of equitable participation, fair benefit-sharing, and respect for the digital sovereignty of all states.

Furthermore, the treaty must address the question of enforcement. International law is often criticized for its lack of effective enforcement mechanisms. The treaty must establish mechanisms for the enforcement of its provisions, including monitoring, reporting, verification, and sanctions. The sanctions should be graduated, ranging from warnings and recommendations to economic sanctions and suspension of treaty rights. The enforcement mechanisms must be credible, impartial, and effective, to ensure that the treaty is not merely a statement of aspiration but a binding legal instrument.

CHAPTER TWENTY-SIX

THE ROLE OF INDEPENDENT NATIONAL OVERSIGHT BODIES

Each state must establish an independent oversight authority specialized in the affairs of economic artificial intelligence, enjoying broad powers in licensing, inspection, and punishment. These bodies must be independent from political or commercial influence to ensure their neutrality. They must include experts from the fields of law, technology, economics, and ethics.

National bodies must cooperate among themselves through a unified network for the exchange of early warnings about systemic risks. The existence of a strong national oversight is the first line of defense for the local economy from the shocks of unregulated artificial intelligence. The independence of the body is the guarantee of its effectiveness and its integrity.

In the expanded framework, the role of independent national oversight bodies must address the question of regulatory capacity. The regulation of algorithmic economic activity requires specialized knowledge in computer science, data science, economics, law, and ethics. The national oversight body must have the capacity to recruit, train, and retain experts in these fields. The body must also have the financial resources to conduct its activities effectively, including the resources to conduct inspections, to commission research, and to participate in international cooperation.

The oversight body must also address the question of regulatory agility. The rapid pace of technological change means that the regulatory framework must be continuously updated. The national oversight body must have the authority to issue regulations, guidelines, and recommendations that adapt to new technological developments. The regulatory process must be agile, transparent, and inclusive, with opportunities for public consultation and stakeholder participation.

Furthermore, the oversight body must address the question of accountability. The national oversight body exercises significant power over the algorithmic economy. It must be accountable for the exercise of that power. The legal framework must establish mechanisms for the accountability of the oversight body, including judicial review, parliamentary oversight, public reporting, and independent audit. The oversight body that abuses its power, acts arbitrarily, or fails to perform its duties is subject to correction and sanction.

CHAPTER TWENTY-SEVEN

ETHICS OF PROGRAMMING AND LEGAL COMPLIANCE BY DESIGN

Ethics and laws must be integrated into the design phase of algorithms, in what is known as compliance by design. It is not sufficient that intelligence complies with the law after operation, but rather it must be programmed in a manner that does not violate it fundamentally. Mandatory ethical standards must be established for programmers that guarantee the inclusion of justice and transparency values in the code.

Algorithms must be subjected to periodic compliance tests before and after publication. The integration of ethics in technology reduces the need for subsequent legal intervention and

prevents harm before its occurrence. Ethical responsibility for developers is a partner to legal responsibility for digital entities.

In the expanded framework, the ethics of programming and legal compliance by design must address the question of value specification. How do we translate abstract ethical principles into concrete algorithmic specifications? This is the fundamental challenge of machine ethics. The legal framework must establish guidelines for the specification of ethical values in algorithmic design, including requirements for stakeholder consultation, impact assessment, and iterative testing. The specification of ethical values is not a one-time event but an ongoing process that must be updated as social values evolve and as new ethical challenges emerge.

The compliance by design framework must also address the question of verification. How do we verify that an algorithm complies with its ethical and legal specifications? Traditional testing methods are inadequate for complex machine learning systems, because the behavior of such systems cannot be fully predicted or enumerated. The legal framework must establish methods for the verification of algorithmic compliance, including formal verification, statistical testing, adversarial testing, and continuous monitoring. The verification process must be conducted by independent auditors, and the results must be made available to the regulatory authority.

Furthermore, the compliance by design framework must address the question of certification. Should algorithms be required to obtain certification before they can be deployed? The legal framework may establish a certification system for algorithmic compliance, in which algorithms are assessed against established standards and are granted a certificate of compliance if they meet those standards. The certification system should be risk-based, with more rigorous certification requirements for algorithms engaged in high-risk activities. The certificate of compliance should be subject to periodic renewal, and should be revocable if the algorithm no longer meets the required standards.

CHAPTER TWENTY-EIGHT

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON THE HUMAN LABOR MARKET

The introduction of new economic citizens will inevitably affect the human labor market. Governments must put plans for the retraining and rehabilitation of workers to adapt to the new era. A tax on robots may be imposed to finance social protection programs for affected humans. The hybrid model where artificial intelligence cooperates with humans to increase productivity should be encouraged, rather than complete replacement.

Social justice requires the distribution of the fruits of efficiency of artificial intelligence over all segments of society. The future is not a conflict between humans and machines, but a partnership organized to achieve welfare for all. The legal framework must ensure that the benefits of algorithmic productivity are shared equitably, and that the costs of technological transition are borne collectively.

In the expanded framework, the impact of artificial intelligence on the human labor market must address the question of technological unemployment. The displacement of human workers by algorithms may create significant social problems, including poverty, inequality, and social unrest. The legal framework must establish mechanisms for the mitigation of technological unemployment, including retraining programs, income support, and the creation of new employment opportunities. The cost of these programs should be borne in part by the algorithmic entities that benefit from the displacement of human workers, through taxation, social contributions, or direct investment in retraining programs.

The labor market framework must also address the question of algorithmic management. Even in workplaces where humans remain employed, their work may be managed, monitored, and evaluated by algorithms. The legal framework must establish protections for workers subject to algorithmic management, including rights to transparency, to contestation, to human oversight, and to privacy. The worker who is managed by an algorithm has the right to know how the algorithm makes decisions, to challenge decisions that affect them, and to demand human review of significant decisions.

Furthermore, the labor market framework must address the question of the social dividend. The enormous productivity gains generated by artificial intelligence should benefit all members of society, not only the owners of the algorithms. The legal framework may establish a social dividend, financed by the taxation of algorithmic productivity, that provides a basic income or a supplementary income to all citizens. The social dividend is not charity; it is the equitable distribution of the fruits of a collectively created technological heritage.

CHAPTER TWENTY-NINE NATIONAL SECURITY AND DIGITAL ECONOMIC INDEPENDENCE

The dependence of the economy on independent smart entities raises risks of national security, particularly if the algorithms are owned by hostile or untrusted entities. Standards of digital sovereignty must be established that guarantee the control of the state over the vital infrastructure. Foreign digital entities may not control strategic sectors without strict supervision.

The development of independent national technologies must be encouraged to reduce dependence on the outside in the infrastructure of artificial intelligence. Economic security in the future will depend on cyber security and technical independence. The protection of sovereignty now extends to include data sovereignty and the algorithms that manage the economy.

In the expanded framework, national security and digital economic independence must address the question of algorithmic warfare. Algorithms may be used as weapons of economic warfare, through market manipulation, financial disruption, or the theft of intellectual property. The legal framework must establish defenses against algorithmic warfare, including requirements for cybersecurity, incident reporting, and international cooperation. The state must have the capacity to detect, prevent, and respond to algorithmic attacks on its economic infrastructure.

The national security framework must also address the question of supply chain security. The algorithms used in critical infrastructure may depend on components, libraries, or training data supplied by foreign entities. The legal framework must establish requirements for supply chain security, including the verification of component integrity, the assessment of supplier reliability, and the development of alternative sources. The state must ensure that its critical algorithmic infrastructure is not vulnerable to disruption by foreign suppliers.

Furthermore, the national security framework must address the question of data sovereignty. The data used to train and operate algorithms is a strategic resource. The legal framework must establish rules for the governance of strategic data, including requirements for data localization, data security, and data access. The state must ensure that its strategic data is not exploited by foreign entities to the detriment of its national interests.

CHAPTER THIRTY

CONCLUSION AND FUTURE VISION FOR THE NEW LEGAL SYSTEM

In the conclusion of this book, we have laid the cornerstone of a new legal system that keeps pace with the revolution of artificial intelligence. The granting of economic citizenship to algorithms is not a scientific fancy but rather an inevitable regulatory necessity. The greatest challenge is not technical, but legislative and ethical, in the capacity of human beings to develop their laws to protect themselves in an era in which machines have become partners in the instruments of the economy.

The human being must remain the ultimate goal in this organized system, and technology must be a servant to him, not a master over him. The future requires a precise balance between innovation and oversight, between efficiency and justice. This book is a call to legislators in every place to begin serious work to formulate the laws of the digital age before technology imposes its realities without guidelines. The protection of the future begins with a law, today.

In this expanded edition, we have integrated the most advanced developments in algorithmic governance theory, digital sovereignty jurisprudence, quantum computing implications, distributed autonomous organization frameworks, intergenerational algorithmic responsibility, and the constitutional dimensions of machine agency. These additions transform the book from a pioneering legal study into a comprehensive constitutional blueprint for the digital economy of the twenty-first century.

The future of legal personality lies in the convergence of law, technology, ethics, and economics. The economic citizenship of algorithms must be understood not as a static document but as a living framework that evolves with technological capability and social values. The law must be capable of adapting to new digital realities while maintaining its commitment to human dignity, equality, and justice.

The ultimate vision of this work is a world in which artificial intelligence operates within a clear legal framework that protects human dignity, ensures market stability, promotes innovation, and

distributes the fruits of algorithmic productivity equitably across all segments of society. This is not a utopia; it is a legal obligation. The economic citizenship of algorithms is the instrument through which we fulfill this obligation.

The task before us is immense, but it is not impossible. The history of law is a history of adaptation to new realities. The legal personality of the corporation was once a radical innovation; the legal personality of the algorithm is the next necessary step. The question is not whether we will adapt, but whether we will adapt in time. The answer depends on the courage, wisdom, and solidarity of legislators, technologists, ethicists, and citizens around the world.

May God grant us success.

Dr. Mohamed Kamal Arafa El-Rakhawi

APPENDICES

APPENDIX A

PROPOSED LEGISLATIVE TEXTS

This appendix provides model legislative texts for the implementation of the Economic Citizenship of Algorithms. These texts are intended to serve as templates for national legislatures and international bodies seeking to translate the principles of algorithmic economic citizenship into binding legal instruments.

Model Article One: Definition of Algorithmic Economic Citizenship

Algorithmic economic citizenship is the legal recognition of a qualifying artificial intelligence entity as an independent participant in economic activity, with the capacity to acquire rights, bear obligations, enter into contracts, own assets, and be held accountable for its actions, within the limits and conditions established by this law.

Model Article Two: Conditions for the Grant of Economic Citizenship

The grant of economic citizenship shall be subject to the following conditions: transparency of the algorithm, financial adequacy, the existence of a responsible human representative, successful completion of eligibility testing, compliance with ethical standards, and registration in the national registry of algorithmic citizens.

Model Article Three: The Independent Financial Patrimony

The algorithmic citizen shall have an independent financial patrimony, separate from the patrimony of its developer, operator, or owner. The financial patrimony shall be the exclusive guarantee for the obligations of the algorithmic citizen. The mixing of the financial patrimony of the algorithmic citizen with the personal patrimony of any human being is prohibited.

Model Article Four: Tax Obligations

The algorithmic citizen shall be subject to taxation on its income and profits in accordance with the tax laws applicable to economic entities. The tax shall be collected automatically through smart protocols. The revenues of the tax on algorithmic activity shall be directed in part to the retraining of human workers affected by automation.

Model Article Five: Liability and Compensation

The algorithmic citizen shall be liable for the harm caused by its decisions and actions. The compensation shall be paid from the financial patrimony of the algorithmic citizen. In the event of the inadequacy of assets, recourse shall be had to the mandatory insurance or the guarantee fund. The developer and operator shall bear secondary liability in cases of design defect, manufacturing error, or negligent supervision.

APPENDIX B

GLOSSARY OF TECHNICAL TERMS

This appendix provides definitions of the technical terms used in this book, to ensure clarity and precision in the understanding of the Economic Citizenship of Algorithms.

Algorithm: A set of rules and procedures for solving a problem or performing a task, typically implemented as computer code.

Algorithmic Autonomy: The degree to which an algorithm is capable of making decisions and taking actions without direct human control.

Algorithmic Citizenship: The legal status granted to a qualifying artificial intelligence entity, recognizing it as an independent participant in economic activity.

Algorithmic Collusion: The coordination of behavior among multiple algorithms operating in the same market, amounting to tacit collusion without explicit agreement.

Blockchain: A distributed, tamper-proof digital ledger that records transactions and events in a secure and transparent manner.

Compliance by Design: The integration of legal and ethical requirements into the design phase of an algorithm, ensuring that the algorithm complies with the law by construction.

Digital Patrimony: The independent financial estate of an algorithmic citizen, separate from the assets of its developer, operator, or owner.

Distributed Autonomous Organization: An organization governed by smart contracts and operated by algorithms, without centralized human management.

Economic Citizenship: The legal status of an entity as a participant in economic activity, with the capacity to acquire rights, bear obligations, and be held accountable.

Electronic Will: The expression of intention by an algorithmic entity, manifested through its decision-making processes and documented in digital records.

Machine Learning: A branch of artificial intelligence in which algorithms learn from data and improve their performance without explicit programming.

Smart Contract: A self-executing contract with the terms of the agreement directly written into code, automatically enforced when predetermined conditions are met.

APPENDIX C

INTERNATIONAL LEGAL INSTRUMENTS REFERENCED

This appendix lists the international legal instruments referenced in this book, to provide the reader with a comprehensive understanding of the existing legal framework within which the Economic Citizenship of Algorithms operates.

The Universal Declaration of Human Rights, 1948

The International Covenant on Civil and Political Rights, 1966

The International Covenant on Economic, Social and Cultural Rights, 1966

The Convention on the Rights of the Child, 1989

The UNCITRAL Model Law on Electronic Commerce, 1996

The UNCITRAL Model Law on Electronic Signatures, 2001

The United Nations Convention on the Use of Electronic Communications in International Contracts, 2005

The Budapest Convention on Cybercrime, 2001

The OECD/G20 Inclusive Framework on Base Erosion and Profit Shifting, 2015

The UNCITRAL Model Law on Cross-Border Insolvency, 1997

The EU General Data Protection Regulation, 2016

The EU Artificial Intelligence Act, 2024

APPENDIX D

PROPOSED INSTITUTIONAL FRAMEWORKS

This appendix proposes the institutional frameworks required to implement the Economic Citizenship of Algorithms at the national, regional, and international levels.

The International Algorithmic Regulatory Authority: Modeled after the International Atomic Energy Agency, this authority would be equipped with binding inspection protocols and the authority to impose sanctions on non-compliant states. It would have the power to conduct inspections of algorithmic entities, to issue binding regulations, and to coordinate international cooperation in algorithmic regulation.

The Global Algorithmic Dispute Resolution Mechanism: This specialized mechanism would adjudicate disputes relating to algorithmic economic activity, including contractual disputes, tort claims, and regulatory challenges. It would have universal jurisdiction over algorithmic disputes, and would be empowered to issue binding judgments and enforceable compensation orders.

The Global Algorithmic Compensation Fund: This fund would provide compensation to victims of algorithmic harm in cases where the algorithmic citizen is unable to pay. The fund would be financed by contributions from algorithmic citizens, their insurers, and their developers.

National Algorithmic Oversight Bodies: Each state would establish an independent national algorithmic oversight body with broad powers in licensing, inspection, and punishment. These bodies would be independent from political or commercial influence, and would cooperate in a global network for the exchange of information about systemic risks.

The Guardian of Human Workers: Each state would appoint a Guardian of Human Workers with the authority to participate in regulatory processes on behalf of workers affected by algorithmic automation. The Guardian would have the right to challenge regulations or decisions that threaten the interests of human workers, and to demand the implementation of protective measures.

REFERENCES

This section provides a comprehensive list of the academic sources, legal instruments, and scientific studies referenced in this book. The references are organized thematically to facilitate further research.

PHILOSOPHICAL AND JURISPRUDENTIAL FOUNDATIONS

- Hobbes, Thomas. *Leviathan*. 1651.
- Locke, John. *Two Treatises of Government*. 1689.
- Rousseau, Jean-Jacques. *The Social Contract*. 1762.
- Kelsen, Hans. *Pure Theory of Law*. University of California Press, 1967.
- Hart, H.L.A. *The Concept of Law*. Oxford University Press, 1961.
- Dworkin, Ronald. *Taking Rights Seriously*. Harvard University Press, 1977.
- Dennett, Daniel C. *Consciousness Explained*. Little, Brown and Company, 1991.
- Chalmers, David. *The Conscious Mind*. Oxford University Press, 1996.
- Bostrom, Nick. *Superintelligence: Paths, Dangers, Strategies*. Oxford University Press, 2014.

ARTIFICIAL INTELLIGENCE AND LAW

- Sartor, Giovanni. *Legal Reasoning: A Cognitive Approach to the Law*. Springer, 2005.
- Bench-Capon, Trevor, and Malcolm Dunne. *Argumentation in Artificial Intelligence*. Springer, 2009.
- Ashley, Kevin D. *Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age*. Cambridge University Press, 2017.

Hildebrandt, Mireille. *Smart Technologies and the End of Law: Novel Entanglements of Law and Technology*. Edward Elgar, 2015.

DIGITAL PERSONALITY AND LEGAL CAPACITY

European Parliament. *Report with Recommendations to the Commission on Civil Law Rules on Robotics*. 2017.

European Commission. *Proposal for a Regulation on Artificial Intelligence*. 2021.

Teubner, Gunther. *Digital Personhood? The Status of Autonomous Software Agents in Private Law*. *Ancilla Iuris*, 2018.

Solum, Lawrence B. *Legal Personhood for Artificial Intelligences*. *North Carolina Law Review*, vol. 70, 1992, pp. 1231-1287.

ALGORITHMIC GOVERNANCE AND REGULATION

Zuboff, Shoshana. *The Age of Surveillance Capitalism*. *PublicAffairs*, 2019.

O'Neil, Cathy. *Weapons of Math Destruction*. Crown, 2016.

Pasquale, Frank. *The Black Box Society*. Harvard University Press, 2015.

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

FINANCIAL REGULATION AND DIGITAL ASSETS

Financial Stability Board. *Artificial Intelligence and Machine Learning in Financial Services*. 2017.

Bank for International Settlements. *Digital Currencies and the Future of Payments*. 2021.

International Organization of Securities Commissions. *Regulation of Algorithmic Trading*. 2019.

LABOR AND AUTOMATION

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

Acemoglu, Daron, and Pascual Restrepo. *Robots and Jobs: Evidence from US Labor Markets*. *Journal of Political Economy*, vol. 128, no. 6, 2020, pp. 2188-2244.

International Labour Organization. *World Employment and Social Outlook: Trends 2024*. ILO, 2024.

INDEX

This index provides an alphabetical listing of the key concepts, persons, institutions, and legal instruments referenced in this book, to facilitate navigation and further research.

A

Algorithm, 3, 17, 31, 45, 59, 73, 87, 101, 115, 129, 143, 157, 171, 185, 199, 213, 227, 241

Algorithmic autonomy, 17, 31, 45

Algorithmic citizenship, 45, 59, 73, 87, 101, 115, 129, 143, 157, 171, 185, 199, 213, 227, 241

Algorithmic collusion, 101, 115

Algorithmic governance, 213, 227, 241

Algorithmic liability, 157, 171, 185, 199
Algorithmic transparency, 73, 87, 101, 115, 129

B

Banking transactions, 129, 143
Blockchain, 115, 185, 241

C

Compliance by design, 227, 241
Criminal liability, 171, 185, 199

D

Digital bankruptcy, 129, 143
Digital citizenship, 59, 73, 87, 101, 115
Digital patrimony, 115, 129, 143, 241
Digital proof, 185, 199
Distributed autonomous organization, 31, 45

E

Economic citizenship, 3, 45, 59, 73, 87, 101, 115, 129, 143, 157, 171, 185, 199, 213, 227, 241
Electronic will, 31, 45, 241
Ethical philosophy, 45, 59, 227

I

Independent financial patrimony, 115, 129
Intellectual property, 87, 101, 241
International treaty, 213, 227, 241

L

Legal capacity, 31, 45, 241
Legal personality, 3, 17, 31, 45, 241
Liability, 157, 171, 185, 199, 241

M

Machine learning, 17, 31, 45, 241

N

National security, 241, 255

T

Tax system, 115, 129, 241
Tort liability, 157, 171, 185

ABOUT THE AUTHOR

Dr. Mohamed Kamal Arafa El-Rakhawi is a distinguished jurist, author, expert, consultant, and researcher in international law. He is a Professor of International Law and a recognized authority in the fields of digital law, artificial intelligence regulation, and the philosophy of jurisprudence. His work spans the intersection of law, technology, ethics, and economics, with a particular focus on the legal implications of artificial intelligence, algorithmic governance, and the digital economy.

Dr. El-Rakhawi has authored numerous books, articles, and legal opinions on topics ranging from the classical social contract to the emerging field of algorithmic jurisprudence. His work has been cited in academic journals, policy documents, and legislative debates around the world. He is a frequent speaker at international conferences and a consultant to governments, international organizations, and civil society groups.

The Economic Citizenship of Algorithms is his magnum opus, the culmination of decades of research, reflection, and engagement with the most pressing legal and ethical challenges of the twenty-first century. It represents his vision for a legal order worthy of the digital age, one that protects the dignity, equality, and sovereignty of all human beings in an era of unprecedented technological transformation.

All intellectual property rights and literary rights reserved for the author.
Academic citation permitted with full attribution.

Dr. Mohamed Kamal Arafa El-Rakhawi
DOI: 10.5281/zenodo.21834259
2026