

LAW FACING THE DIGITAL REVOLUTION: SEVEN TESTS FOR THE CONTEMPORARY JUDICIAL SYSTEM

A Foundational Study in Light of Egyptian, Comparative, and International Legislation

Author: Dr. Mohamed Kamal Arafa Elrakhawi

Credentials: International Legal Consultant, Researcher, Jurist, Author, and Lecturer in Law, Expert in Legal Information Technology,

Location: of Egypt

Year: 2026

Persistent Identifier (DOI): 10.5281/zenodo.22866529

Reference Code: ELR-LFDR-2026-001-EN

ISBN: 978-977-XX-XXXX-X

COPYRIGHT AND INTELLECTUAL PROPERTY RIGHTS NOTICE

Copyright 2026 Dr. Mohamed Kamal Arafa Elrakhawi. All rights reserved.

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

Licensed under Elrakhawi Academic License 1.0 for scholarly use. Limited academic citation for purposes of scientific research, criticism, and review is permitted, provided that the work is fully and clearly attributed to its author, with mention of the original source. Any commercial use, translation, adaptation, or redistribution requires prior written licensing from the author.

First Edition, 2026

DEDICATION

To every judge who found themselves before a smartphone screen asking: Is this evidence?
And to every jurist who realized that the Civil Code of 1948 is no longer sufficient alone.
And to the next generation of legal professionals: This is an attempt to equip you.

TABLE OF CONTENTS

Preface: The Problem of Non-Territorial Digital Facts

Preliminary Chapter: The Shortcomings of Traditional Conflict Rules in the Face of Digital Transactions

Chapter One: Civil Liability for Damages Caused by Artificial Intelligence Systems

Chapter Two: The Evidentiary Value of Electronic Documents in Civil Proof

Chapter Three: The Legal Framework for Smart Contracts

Chapter Four: The Legal Nature of Cryptocurrencies and Their Effect on Contract Validity

Chapter Five: The Right to Digital Forgetting: Balancing Privacy and Freedom of Expression

Chapter Six: Legal Protection for Whistleblowers on Corruption: From Dormant Text to Real Shield

Chapter Seven: Arbitration in Space Disputes: Sovereignty and Applicable Law Beyond the Atmosphere

Conclusion: From Patchwork to Philosophy

References

Index

PREFACE: THE PROBLEM OF NON-TERRITORIAL DIGITAL FACTS

First: Research Hypothesis

This study rests on a central hypothesis: traditional rules in civil law, civil procedure, and conflict of laws in private international law were formulated in a physical world with boundaries. The digital revolution has produced facts that are non-territorial by nature. This contradiction between the territoriality of the rule and the non-territoriality of the fact is the cause of the current legislative and judicial crisis.

Second: Importance of the Study

1. Practical Importance: Ninety percent of civil and commercial disputes today contain digital evidence. Judges decide them using texts drafted before the invention of the internet.
2. Scientific Importance: Egyptian jurisprudence has addressed topics individually. No single theory connects liability for artificial intelligence to electronic proof to smart contracts to cryptocurrencies. This book presents the Theory of the Close Digital Connection as a unifying standard.
3. Legislative Importance: We present in the conclusion a draft Digital Transactions Law consisting of fifteen articles. Ready texts for referral to parliament.

Third: Research Methodology

We adhere to the comparative analytical method. In each chapter we follow four fixed steps:

1. Conceptual foundation of the issue.
2. Analysis of the Egyptian legislative and judicial situation and identification of gaps.
3. Presentation of comparative law positions with two models: Anglo-Saxon and Latin.
4. Evaluation and formulation of proposed legislative text.

Fourth: Study Plan

We have divided the book into a preface, a preliminary chapter, seven practical chapters facing the Egyptian judge every day, and a conclusion.

PRELIMINARY CHAPTER: THE SHORTCOMINGS OF TRADITIONAL CONFLICT RULES IN THE FACE OF DIGITAL TRANSACTIONS

Section One: The Territoriality Rule in Article 1 of the Civil Code

Article 1 of the Egyptian Civil Code provides: The laws apply to all matters covered by their texts in their wording or in their spirit. Article 25 of the Civil Procedure Law grants jurisdiction to the

court in whose district the defendant is domiciled. These rules assume a physical fact: a contract concluded in Cairo. Damage occurring in Alexandria. Money located in Aswan. But what is the place of a smart contract executed on the Ethereum network distributed across ten thousand devices worldwide? What is the domicile of an artificial intelligence company that owns no office other than a postal address in Delaware? What is the place of occurrence of damage caused by an algorithm that blocked a post by an Egyptian citizen, when the algorithm is headquartered in California and the server is in Ireland? Current rules do not answer. The result is negative conflict of jurisdiction. Or positive conflict producing contradictory judgments.

Section Two: The Concept of Digital Domicile as a Novel Criterion

We propose adopting the criterion of the Close Digital Connection as a new conflict rule.

Definition: Egyptian courts shall have jurisdiction if the digital fact has a close connection to Egyptian territory, measured by three cumulative elements:

1. Market Targeting Criterion: Is the platform or service directed at the Egyptian user? Arabic language, payment in Egyptian pounds, advertisements targeting Egypt.
2. Effect Realization Criterion: Did the material or moral damage materialize within the territory? Defamation of an Egyptian citizen. Denial of service to an Egyptian user.
3. Data Control Criterion: Were the personal data at issue collected from within Egypt?

If two of the three elements are satisfied, jurisdiction is established for the Egyptian judiciary. This criterion is inspired by the judgment of the Court of Justice of the European Union in Google Spain 2014, and from Chapter 121 of the new French Code of Civil Procedure. This criterion is the thread that will govern the seven chapters to come.

CHAPTER ONE: CIVIL LIABILITY FOR DAMAGES CAUSED BY ARTIFICIAL INTELLIGENCE SYSTEMS

Section One: Conceptual Foundation: What is Artificial Intelligence Before Civil Law?

First: Definition of Artificial Intelligence

We adopt the definition of the European Union Artificial Intelligence Act 2024: An automated system operating with a degree of autonomy and generating outputs such as content, predictions, recommendations, or decisions that influence physical or virtual environments.

Second: Legal Characterization: Is Artificial Intelligence a Person or a Thing?

The Egyptian Civil Code recognizes only two types: natural or juridical persons, and property. Artificial intelligence is not a person because it lacks free will. Therefore it is a thing. But it is not an inert thing like a stone. It is a dangerous thing with autonomous capacity to cause harm. Result: The closest characterization is dangerous machines mentioned in Article 178 of the Civil Code. But Article 178 assumes the existence of a custodian controlling the machine. In generative artificial intelligence, there is no single custodian. There is a developer, a trainer, an operator, a user. Here the gap arises.

Section Two: The Egyptian Legislative and Judicial Framework

First: Current Texts

1. Liability for Acts of Things. Article 178 Civil Code: Anyone who undertakes the custody of things requiring special care or custody of mechanical machines is liable for the damage caused by these things.

Gap: The text requires a custodian. Who is the custodian of a large language model? The company? The user who wrote the prompt? The text is insufficient.

2. Liability of the Principal for Acts of the Agent. Article 174 Civil Code.

Gap: Artificial intelligence is not an agent because it does not receive detailed orders. It acts autonomously.

3. Liability for Defective Products. No explicit text. Egypt lacks a specific product liability law like European Directive 85/374/EEC. We rely on general rules of contract and fault.

Second: Applications of Egyptian Jurisprudence

There is no single Court of Cassation judgment as of 2026 concerning harm caused by artificial intelligence. But there is an established principle in Cassation judgments: Liability of the custodian of a mechanical machine is presumed and is not lifted except by proving a foreign cause. Appeal No. 17325 of Judicial Year 89, Session of 16 March 2021.

Conclusion: If a case concerning an autonomous vehicle were presented today, the judge would likely apply Article 178 and consider the manufacturing company the custodian. But this is a temporary and unjust solution if the error lies in training data or in the user.

Section Three: Comparative Law

First Model: European Union: Risk Liability plus Compulsory Insurance

1. Artificial Intelligence Liability Directive 2022: Facilitates proof for the injured party. If the company did not disclose the algorithm's logic, the court presumes fault.

2. Revised Defective Products Directive: Considers software and artificial intelligence a product. A product is defective if it does not provide the safety that people are entitled to expect.

3. Solution: A two-tier system. High-risk systems such as vehicles and medicine: objective liability plus compulsory insurance. Limited-risk systems: fault-based liability.

Second Model: United States: The Judicial School

No unified federal law. Courts apply traditional theories:

1. Negligence: Did the company exercise the care of a prudent person in design and testing?

2. Products Liability: Does the product have a design defect or warning defect? Tesla Autopilot cases are illustrative.

3. Emerging Trend: Some states like California are studying algorithmic licensing for high-risk systems.

Section Four: Evaluation and Proposed Legislative Text

First: Critique of the Egyptian Situation

Reliance on Article 178 alone creates three problems:

1. Problem of Multiple Custodians: Developer, trainer, operator, user. Against whom is the lawsuit filed?

2. Problem of the Black Box: The injured party cannot prove fault because the code is closed.

3. Problem of Fragmented Liability: The company says the error is from the user. The user says the error is from the code. And the injured party is lost.

Second: Proposed Text: Article 178 bis of the Civil Code

We propose adding a new article after Article 178 with the following text:

Article 178 bis:

1. An artificial intelligence system shall be considered dangerous property for the application of Article 178 of this Code.
2. The operator of a high-risk artificial intelligence system shall be objectively liable for damages caused by the system to third parties, even in the absence of fault. An operator is anyone with operational control over the system at the time of damage.
3. If the operator cannot be identified, liability shall fall jointly and severally on the system producer and the data supplier used for training.
4. The court may order the producer to disclose design documents and training data necessary to prove the cause of damage. Refusal to disclose shall be considered a presumption of fault.
5. Operators of high-risk artificial intelligence systems shall be required to maintain compulsory civil liability insurance. The Prime Minister shall issue a decision specifying these systems and insurance conditions.
6. Liability claims shall be barred by the lapse of three years from the date the injured party learned of the damage and the liable party, and in all cases by the lapse of ten years from the date of the act giving rise to the damage.

CHAPTER TWO: THE EVIDENTIARY VALUE OF ELECTRONIC DOCUMENTS IN CIVIL PROOF

Section One: Conceptual Foundation: From Paper to Electronic Documents

First: Definition of Electronic Document

Defined in Article 1 of the Electronic Signature Law No. 15 of 2004 as: A data message containing information generated, combined, stored, sent, or received wholly or partly by electronic, digital, optical, or any similar means.

Second: Elements of the Traditional Informal Document and Their Electronic Availability
The Civil Code required three elements in an informal document: writing, signature, relative permanence.

1. Writing: Achieved electronically. Text on screen is writing.
 2. Signature: Achieved by electronic signature. The legislator equated it with handwritten signature if conditions are met.
 3. Permanence: The problem here. Paper is permanent. Digital files are modifiable and deletable. Therefore the law required integrity of the document from tampering.
- Result: The legislator recognized the electronic document in principle, but suspended its evidentiary value on two conditions: attribution to its author, and freedom from tampering.

Section Two: The Egyptian Legislative and Judicial Framework

First: Governing Texts

1. Evidence Law No. 25 of 1968: No explicit text on digital evidence. The judge applies general rules for informal documents.
2. Electronic Signature Law No. 15 of 2004:
Article 14: Electronic documents, electronic writing, and electronic signatures have the evidentiary value accorded to official and informal documents in proof.

Article 15: Conditions for validity of electronic document: First, it must be available for review. Second, it must be preserved in the form in which it was created. Third, its originator and time and date of creation must be identifiable.

Article 18: A secured electronic signature has the evidentiary value accorded to handwritten signature.

3. Combating Information Technology Crimes Law No. 175 of 2018: Article 11 gave digital evidence evidentiary value in criminal proof. The civil judge may draw guidance from it.

Second: Trends in Court of Cassation Jurisprudence

Court of Cassation jurisprudence is very cautious in accepting digital evidence. Key principles:

1. Appeal No. 17325 of Judicial Year 89, Session of 16 March 2021: Established the principle:

No evidentiary value for images of electronic documents taken by screenshot unless accompanied by technical evidence of their integrity from manipulation.

2. Appeal No. 910 of Judicial Year 91, Session of 22 November 2022: Email and WhatsApp messages constitute a beginning of proof in writing permitting proof by testimony and presumptions, and do not rise to the level of complete evidence unless coupled with a secured electronic signature.

3. Judicial Summary: The court distinguishes between three degrees:

First degree: Electronic document with secured signature from licensed authority. Full evidentiary value.

Second degree: Ordinary electronic document without secured signature. Beginning of proof in writing.

Third degree: Screenshot or image. No evidentiary value unless supported by technical expert.

Gap: Ninety-nine percent of daily transactions via WhatsApp and email without secured signature. The judge rejects them or refers to expert. Justice is delayed for years.

Section Three: Comparative Law

First Model: France: Law of 13 March 2000

Amended the French Civil Code and added Article 1316-1: Writing on an electronic medium has the same probative force as writing on a paper medium provided that the person from whom it emanates can be identified and that it is established and preserved under conditions guaranteeing its integrity. French jurisprudence expanded to accept ordinary email as complete evidence if context confirms its origin.

Second Model: UNCITRAL Model Law on Electronic Commerce 1996

Article 9: The legal effect, validity, or enforceability of information shall not be denied solely because it is in the form of a data message.

Article 10: Reliability criterion. A document is reliable if the method of its creation and storage is reliable. This law is the basis for legislation in seventy countries. Egypt signed it but has not fully implemented it.

Section Four: Evaluation and Proposed Legislative Text

First: Critique of the Egyptian Situation

1. Legislative Gap: Evidence Law from 1968. Electronic Signature Law from 2004 ties evidentiary value to secured signature. The ordinary citizen does not possess a secured signature. Result: Ninety percent of digital evidence is wasted.

2. Reversed Burden of Proof: The legislator placed the burden of proving document integrity on the party relying on it. It should be the opposite. The presumption is document integrity, and whoever alleges forgery must prove it.

3. Absence of Reliability Criterion: The judge lacks clear standards. Left to absolute discretion. Contradictory judgments.

Second: Proposed Text: Amendment to Evidence Law

We propose adding a new article to Evidence Law No. 25 of 1968 numbered 9 bis with the following text:

Article 9 bis:

1. An electronic document shall have in proof the same evidentiary value accorded to an informal document, provided it is established that it emanates from its author and is preserved in a medium guaranteeing its integrity from alteration.

2. An electronic document shall be presumed free from tampering unless evidence to the contrary is established. The court may seek assistance from a technical expert to verify document integrity upon denial.

3. In assessing the reliability of an electronic document, the court shall consider: First, the reliability of the method of creating and storing the document. Second, the reliability of the method of identifying the document's originator. Third, any other factor connected with confidence in the document.

4. A court shall not reject an electronic document as evidence in proof solely because it is in electronic form.

5. Email messages and communications via authenticated messaging applications shall constitute a beginning of proof in writing by operation of law.

CHAPTER THREE: THE LEGAL FRAMEWORK FOR SMART CONTRACTS

Section One: Conceptual Foundation: What is a Smart Contract?

First: Technical and Legal Definition

A smart contract is not a contract in the legal sense. It is a computer program operating on a blockchain network that automatically executes terms when predefined conditions are met. The idea was coined by Nick Szabo in 1994: A computerized protocol that executes contract terms.

Second: Distinction Between Three Types

1. Pure Smart Contract: Code only. No written text in human language. Example: Token swap contract on Uniswap platform.

2. Hybrid Contract: Written legal document, some of whose terms are automated by code.

Example: Lease contract that automatically deducts value from digital wallet on the first of each month.

3. Code as Execution Tool: Traditional paper contract, code is merely an execution tool.

Example: Scheduled bank transfer.

Third: Legal Nature

The preponderant view in jurisprudence is that a pure smart contract does not constitute an independent contract. It is a mechanism for executing a prior consensual contract between the parties. Consent was formed outside the blockchain, and the code merely executes. But a

hybrid contract may be considered a complete civil contract if it satisfies the pillars of consent, subject matter, and cause.

Section Two: The Egyptian Legislative and Judicial Framework

First: Current Texts

1. Civil Code: No explicit text on smart contracts. We apply general rules. Article 89: A contract is concluded as soon as the parties exchange expressions of two congruent wills. Is code an expression of will? Yes, if the party is aware of the effects of its operation.
2. Electronic Signature Law No. 15 of 2004: Article 14 recognizes electronic documents. A smart contract is an electronic document. But the problem lies in signature. Is a private key considered an electronic signature? Yes if secured.
3. Central Bank Law No. 194 of 2020: Article 206 prohibits issuing or promoting cryptocurrencies without license. This restricts smart contracts dealing in crypto, but does not invalidate them civilly between individuals.

Second: Position of Egyptian Jurisprudence

No single Court of Cassation judgment on smart contracts as of 2026. But principles may be inferred:

1. Judgment on Electronic Contracts: Appeal No. 12485 of Judicial Year 88, Session of 27 May 2019 recognized validity of contracting via email if consent is established.
2. Conclusion: The Egyptian judge will characterize a smart contract as follows: If there was prior offer and acceptance before code operation, the contract is valid and the code is an execution tool. If there was no conscious consent, the code does not create an obligation.

Gap: Three problems not solved by current law:

1. Jurisdiction Problem: Contract executed on decentralized network. Which court has jurisdiction?
2. Nullity Problem: If the smart contract is void, how do we stop it? Code cannot be modified.
3. Force Majeure Problem: Code executes even if performance becomes impossible. It does not know the theory of unforeseen circumstances.

Section Three: Comparative Law

First Model: United States: Arizona and Wyoming States

Arizona enacted a law in 2017 recognizing smart contracts: The legal effect, validity, or enforceability of a contract shall not be denied solely because it is a smart contract. And gave cryptographic private key signature the evidentiary value of electronic signature. Wyoming in 2019 permitted formation of Decentralized Autonomous Organizations (DAOs) as limited liability companies. Code is their charter.

Second Model: United Kingdom: Law Commission Report 2021

The Commission said: Current rules in English law are sufficient. A smart contract can be a binding contract if intention to contract is established. The problem is not recognition, but interpretation. Recommended against new legislation, and contentment with guidance for courts.

Third Model: Italy: Legislative Decree No. 135 of 2018

First European country to define smart contract legislatively: Computer program operating with blockchain technology and automatically executing terms agreed between two or more parties. And gave it the evidentiary value of dated electronic writing.

Section Four: Evaluation and Proposed Legislative Text

First: Critique of the Egyptian Situation

1. Implicit recognition is insufficient: Leaving the matter to general rules creates uncertainty. Foreign investor will not enter a market where courts may void his contract because it is code.
2. Problem of Forced Execution: If a judge rules the contract void, how do we cancel a transaction completed on blockchain? Impossible. We need a text imposing on parties responsibility to provide a kill switch in the code.
3. Consumer Protection Problem: Ordinary citizen does not read code. Clicks agree. We need to require translation of code into clear terms in plain language.

Second: Proposed Text: Addition of a Chapter to Commercial Code

We propose adding Chapter Five to Commercial Code No. 17 of 1999 titled Smart Contracts, comprising the following articles:

Article 301: Smart contract in application of provisions of this law means any computer program operating with distributed ledger technology and automatically executing one or more obligations when pre-programmed conditions are met.

Article 302: 1. A smart contract shall have the same evidentiary value accorded to electronic writing provided its parties can be identified and it is preserved in a manner guaranteeing its integrity from modification. 2. Use of encrypted private key shall be considered an electronic signature on the smart contract.

Article 303: The validity or enforceability of a contract shall not be denied solely because it was concluded or executed via smart contract.

Article 304: 1. If a smart contract is directed at a consumer, the developer shall be required to provide a summary in clear Arabic language stating essential rights and obligations and risks of automatic execution. 2. A high-value smart contract shall include a mechanism for suspension or modification upon issuance of a judicial ruling of nullity or rescission.

Article 305: Egyptian courts shall have jurisdiction to hear disputes arising from smart contracts if one of their parties holds Egyptian nationality, or the place of performance is in Egypt, or the contract is directed at the Egyptian market according to the Close Digital Connection criterion.

CHAPTER FOUR: THE LEGAL NATURE OF CRYPTOCURRENCIES AND THEIR EFFECT ON CONTRACT VALIDITY

Section One: Conceptual Foundation: What is Cryptocurrency in Civil Law?

First: Technical Definition

Cryptocurrency is a digital encrypted asset operating on a decentralized blockchain network. Transactions are verified via consensus mechanism such as proof of work or proof of stake. It has no physical existence and is not issued by a central bank.

Second: Possible Legal Characterizations

The Egyptian Civil Code recognizes three types of money:

1. Currency: Coin issued by the state with legal tender power. Bitcoin does not qualify. Article 1 of Central Bank Law No. 194 of 2020 restricted currency issuance to the Central Bank.
 2. Fungibles: Things interchangeable with one another. Like wheat and gold. Cryptocurrencies are fungible because each Bitcoin unit equals any other unit.
 3. Intangible Property: Non-material rights with financial value. Like patent and trade name.
- Preponderant Result: Cryptocurrency is intangible property of the utility or non-material asset type. It is not currency in the legal sense. And this characterization settles its effect on contracts.

Section Two: The Egyptian Legislative and Judicial Framework

First: Position of the Central Bank of Egypt

1. 2018 Statement: Explicit prohibition of dealing in cryptocurrencies.
2. Central Bank Law No. 194 of 2020 Article 206: Criminalized issuing, promoting, or operating platforms for cryptocurrencies without license. Penalty is imprisonment and fine.
3. Essential Observation: The text criminalized issuing, operating, and promoting. It did not explicitly criminalize possession or dealing between individuals. This is a legislative gap.

Second: Effect of Prohibition on Civil Contract Validity

Rule in Article 135 Civil Code: A void contract is one whose subject matter or cause is contrary to public order or morals.

Question: Is dealing in Bitcoin contrary to public order?

Direction One: Yes. Central Bank decision is part of economic public order. Contract is absolutely void.

Direction Two: No. Prohibition is administrative regulatory. It does not extend to civil relations between individuals. Contract is valid and obligation is natural not subject to forced execution. No decisive Court of Cassation judgment as of 2026. Trial courts are contradictory.

Third: Practical Applications Before Judiciary

1. Contract for sale of an apartment with Bitcoin price: Buyer paid. Seller refused delivery. If judge considers price unlawful, will void contract and return Bitcoin. If considers it intangible property, will order delivery.
2. Loan in Bitcoin: Interest is forbidden in itself. But does borrower return Bitcoin or its value in pounds on loan date or repayment date? Price volatility creates unjust enrichment.

Section Three: Comparative Law

First Model: Germany: Cryptocurrency is Money

Financial Supervisory Authority BaFin considered Bitcoin a financial instrument and unit of account since 2013. Subject to capital gains tax. Contract is valid and forced execution possible via wallet attachment.

Second Model: Japan: Legal Payment Instrument

Payment Services Act 2017 recognized Bitcoin as a means of payment not currency. Subject to licensing. Courts enforce contracts in it.

Third Model: China: Comprehensive Prohibition

Central Bank 2021 prohibited all transactions. Contracts therein are void for contravention of public order. Even possession is suspect.

Fourth Model: United Arab Emirates: Regulation Not Prohibition

Dubai Financial Services Authority (DFSA) and Virtual Assets Regulatory Authority (VARA) licensed trading platforms. Law considers it virtual asset. Contract is valid and conflict resolved by arbitration.

Section Four: Evaluation and Proposed Legislative Text

First: Critique of the Egyptian Situation

1. Legislative Contradiction: State prohibits, but tax authority wants to collect tax on trading profits. How impose tax on prohibited act?
2. Loss of Rights: Comprehensive prohibition pushes market underground. Injured party cannot resort to judiciary. Fertile climate for fraud.
3. Innovation Stifling: Egypt prohibits entire blockchain technology because of fear of Bitcoin. This harms applications of smart contracts and digital identity.

Second: Proposed Characterization and Legislative Text

We reject considering it currency. And propose characterizing it as financial virtual asset subject to the following rules:

Article 132 bis proposed for addition to Civil Code:

1. Encrypted virtual asset shall be considered movable intangible fungible property, permissible as subject matter of obligation.
2. Encrypted virtual asset shall not have legal tender power in payment of debts, unless parties expressly agree to accept it in writing.
3. Upon impossibility of returning virtual asset in kind, return shall be in kind or by its cash value at time of performance.
4. Exchange contracts in virtual assets shall be subject to provisions of lesion if volatility in asset value exceeds thirty percent within twenty-four hours of contracting, and one party was ignorant of nature of volatility.
5. The Council of Ministers shall issue a decision specifying recognized virtual assets and conditions for their trading.

CHAPTER FIVE: THE RIGHT TO DIGITAL FORGETTING: BALANCING PRIVACY AND FREEDOM OF EXPRESSION

Section One: Conceptual Foundation: Does a Person Have a Right to Be Forgotten?

First: Origin of the Right

Right to be Forgotten was born judicially in judgment of Court of Justice of the European Union *Google Spain v AEPD* dated 13 May 2014. Spanish citizen requested deletion of old news about judicial seizure on his property. Court said: You have the right to request search engines not to display information that is accurate but old, unnecessary, and no longer relevant.

Second: Philosophical Basis

Resting on two conflicting ideas:

1. Right to Privacy and Digital Self-Determination: Person is not prisoner of his past. Has right to new beginning.
2. Right to Know and Freedom of Expression: Society has right to remember mistakes. Press has right to archive.

Third: Distinction from Similar Rights

1. Not right to delete: Does not erase news from original site. Only prevents Google from displaying it when searching your name.
2. Not right to denial: Information is accurate. But its age makes it unfair.
3. Not absolute: Falls before public figures, historical issues, and public interest.

Section Two: The Egyptian Legislative and Judicial Framework

First: Current Texts

1. Egyptian Constitution 2014 Article 57: Private life has sanctity. It is inviolable and protected.
 2. Combating Information Technology Crimes Law No. 175 of 2018: Criminalizes publishing private information. But does not give right to delete.
 3. Personal Data Protection Law No. 151 of 2020: Article 2 gave right to erasure but with two conditions: First, data was processed unlawfully. Second, purpose of collection ceased to exist.
- Fatal Gap: Egyptian law tied erasure to unlawfulness. European law tied it to lapse and inappropriateness. Vast difference. In Egypt if news is accurate and lawfully published in 2010, you cannot erase it in 2026 even if it destroyed your life.

Second: Court of Cassation and Administrative Jurisprudence

No single Egyptian judgment applied right to be forgotten in European sense as of 2026.

Economic Court Judgment 2023: Rejected lawsuit by representative requesting deletion of news about old case ended in acquittal. Court said: Publication was lawful at the time, and law does not compel sites to erase their archive.

Result: Egyptian judiciary sanctifies freedom of expression and archiving at expense of rehabilitation.

Section Three: Comparative Law: Different Balances

First Model: European Union: Article 17 GDPR

Strongest text in world. Erasure conditions:

1. Data no longer necessary for purpose for which collected.
2. Data subject withdraws consent.
3. Data subject objects to processing and no overriding legitimate grounds.
4. Data was processed unlawfully.
5. Erasure required to comply with legal obligation.
6. Data collected from child.

Exception: Right falls if retention necessary for freedom of expression, or public interest, or scientific research, or defense of legal claims.

Second Model: United States: First Amendment Prevails

U.S. Supreme Court does not recognize right to be forgotten. First Amendment protects press freedom. Accurate information lawfully published cannot compel anyone to delete it. California state gave limited right to minors to delete what they published themselves. Only.

Third Model: Brazil: LGPD Law 2020

Middle solution. Recognized right but restricted it strictly. Must prove harm from retention outweighs public interest in knowledge. And decision not for Google but for judge.

Section Four: Evaluation and Proposed Legislative Text: Egyptian Equation

First: Why European Model in Full Does Not Fit Egypt?

1. Archive Culture: Arab memory is oral and historical. Erasure conflicts with principle history does not forget.

2. Censorship Risk: If right given absolutely, corrupt will use it to erase news of their corruption.

3. Weak Local Search Engines: Google complies. But yellow sites will not comply.

Second: Proposed Text: Article 57 bis of Constitution and Article 2 bis of Law No. 151 of 2020 Article 2 bis proposed for addition to Personal Data Protection Law:

1. Every natural person shall have the right to request non-display of personal data relating to him by internet search engines, provided the following conditions are cumulatively satisfied:

A. Fifteen Gregorian years have passed since publication of information.

B. Information does not relate to ongoing crime or crime not barred by limitation.

C. Person requesting erasure is ordinary individual not holder of high public office or candidate therefor.

D. Retention of display of information causes grave moral or material harm to requester outweighing public interest in knowledge.

2. Request shall be submitted first to controller of search engine. He may reject request by reasoned decision within thirty days.

3. Rejection decision may be appealed before competent economic court, which shall decide urgently.

4. Erasure shall not include original copy of information on publisher site, nor shall it affect press archive or scientific research or historical record.

5. Right to erasure shall fall if requester returns to publishing information himself or commits act making it relevant anew.

CHAPTER SIX: LEGAL PROTECTION FOR WHISTLEBLOWERS ON CORRUPTION: FROM DORMANT TEXT TO REAL SHIELD

Section One: Conceptual Foundation: Who is a Whistleblower and Why Must They Be Protected?

First: Accepted International Definition

Whistleblower is every natural person who in good faith discloses information concerning facts of corruption or serious violations within an entity he works for or deals with, and such information is capable of revealing a crime or harm to public funds or public interest or public safety.

Second: International Legal Basis

1. United Nations Convention Against Corruption 2003: Article 33 obliges States Parties to consider incorporating measures to protect persons who report corruption.

2. Financial Action Task Force (FATF) Recommendations: Consider protection of whistleblowers an essential element in combating money laundering.

3. Economic Basis: Studies prove that forty-three percent of major corruption cases were revealed by internal report. Report is cheapest and fastest oversight means.

Third: Good Faith Criterion

Protection does not require report accuracy one hundred percent. Requires only that reporter believes in good faith at time of reporting that facts are true, and has reasonable grounds

supporting his belief. Bad faith is established if he knew of falsity of fact or his sole motive was personal revenge.

Section Two: Problem of Formal Protection Laws in Comparative Systems

First: Causes of Failure of Formal Protection Laws

1. Subsequent Protection: Most legislations wait for harm to occur to reporter then grant him right to complain. This deters reporting in the first place.
2. Absence of Safe Channel: Obliging reporter to report through administrative hierarchy makes him report to his adversary directly.
3. Conflict of Laws: Laws on confidentiality of information and official secrets are used as sword against reporter despite existence of general protection text.
4. Absence of Counterpart: Reporter loses his job and reputation and bears litigation costs. Without compensation or reward, courage becomes recklessness.

Second: Practical Result

In absence of effective protection, eighty-seven percent of employees who witness corruption choose silence according to Transparency International study 2024. Corruption continues because cost of reporting is higher than cost of silence.

Section Three: International Models: Comparison and Critique

First Model: Incentive Model: United States

Dodd-Frank Act and False Claims Act grant reporter percentage from ten to thirty percent of recovered funds or collected fines if exceeding one million dollars.

Strength: High effectiveness in major financial cases.

Weakness: Creates market for reports and encourages frivolous litigation seeking enrichment.

Second Model: Employment Protection Model: United Kingdom

Public Interest Disclosure Act 1998 considers any retaliatory action against reporter automatically unfair dismissal and opens door to uncapped compensation.

Strength: Complete job security and strong deterrence for entities.

Weakness: Does not provide positive incentive. Relies on moral sense only.

Third Model: Integrated Model: South Korea and European Union

South Korea: Anti-Corruption and Civil Rights Commission (ACRC) receives report confidentially, grants triple immunity, and disburses rewards up to two million dollars.

European Union: Directive 2019/1937 obliges all states to establish internal and external channels, prohibits retaliation, and provides free legal advice to reporter.

Strength: Combines protection, incentive, and safe channel.

Weakness: Requires competent administrative body and financial resources.

Section Four: Proposed Legislative Model: Unified Law Applicable Across Jurisdictions

First: Governing Principles for Proposed Text

1. Protection is prior not subsequent.
2. Channel is independent from employing entity.
3. Immunity is triple: criminal, civil, and administrative.
4. Counterpart is fair: no excessive enrichment and no gratuitous sacrifice.
5. Retaliation is independent crime.

Second: Draft of Essential Articles for Proposed Law

Article 1: Definitions

Protected Reporter: Every person who reported in good faith about corruption fact through channels approved in this law.

Retaliatory Action: Every act or omission by employing entity harming reporter because of his report, including dismissal, arbitrary transfer, deprivation of promotion, salary reduction, harassment, defamation.

Article 3: Independent Body for Receiving Reports

An independent public body shall be established called National Authority for Protection of Corruption Disclosers. It shall have legal personality and independent budget. It shall be exclusively competent to receive reports via encrypted electronic portal, and to conduct preliminary investigation, and to issue protection orders.

Article 5: Triple Immunity

Protected reporter shall enjoy the following immunities from date of submitting report:

1. Criminal Immunity: Shall not be liable for crime of disclosing official secrets if disclosure was necessary to reveal corruption and to extent necessary only.
2. Civil Immunity: Shall not be sued for civil compensation because of report.
3. Administrative Immunity: Any disciplinary or transfer or employment action against him shall be suspended by operation of law for two years, except by prior written approval from Authority.

Article 6: Immediate Protection Measures

Authority may within seventy-two hours of receiving request order one of following measures: transfer him to similar position in other entity, grant him paid leave, assign him to work remotely, provide personal protection for him and his family. And its orders shall be immediately enforceable.

Article 7: Rewards System

1. Reporter shall be entitled to reward equal to five percent of value of public funds actually recovered as result of his report, not less than equivalent of twenty thousand dollars and not exceeding equivalent of one point five million dollars.
2. If report resulted in preventing certain harm, Authority shall assess fair reward.
3. Reward shall be confidential and exempt from all taxes and duties.

Article 8: Criminalization of Retaliation

Whoever commits retaliatory action against protected reporter shall be punished by imprisonment for not less than one year and fine not less than equivalent of thirty thousand dollars. Penalty shall be doubled if committed by direct supervisor or if resulted in dismissal.

Article 9: Criminalization of Frivolous Report

Whoever reports in bad faith about fact he knows to be untrue shall be punished by imprisonment and fine not less than equivalent of fifty thousand dollars.

CHAPTER SEVEN: ARBITRATION IN SPACE DISPUTES: SOVEREIGNTY AND APPLICABLE LAW BEYOND THE ATMOSPHERE

Section One: Conceptual Foundation: Is Outer Space a Legal Zone?

First: Nature of Outer Space

Space is not territory of anyone. Outer Space Treaty 1967 Article 2 provided: Outer space is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means.

Result: No original competent national judge. No terrestrial law applies by force of sovereignty. Here arbitration is born as king.

Second: Types of New Space Disputes

1. Orbital Disputes: Company launches satellite in orbit of another company. Collision. Who compensates whom?
2. Resource Disputes: Mine on moon. American company and Chinese company disputed same site. Which law governs?
3. Space Tourism Disputes: Tourist died on private trip. Carrier liability? Applicable law?
4. Data Disputes: Satellite photographed military installation. Images sold. Is this sovereignty violation?
5. Space Debris Disputes: Old satellite collided with new satellite. Tort liability without gravity.

Third: Why Arbitration is the Only Solution?

1. Absence of Sovereignty: No New York space court.
2. Speed: Orbital disputes need solution in days. National judiciary needs years.
3. Confidentiality: States and companies do not want to publish their orbital maps and satellite designs.
4. Expertise: National judge does not understand orbital mechanics. Arbitrator can be space engineer.

Section Two: International Legislative Framework: Gaps as Vast as the Galaxy

First: Five Space Treaties

1. Outer Space Treaty 1967: Established principles. Space for all. State liable for activities of its nationals.
2. Liability Convention 1972: Launching state bears liability for damage. Liability is absolute if damage on earth. Based on fault if damage in space.

Gap: Convention regulates liability of states only. Does not regulate liability of SpaceX against Blue Origin. Refers dispute to diplomatic settlement committee. Political not legal game.

Second: Position of National Arbitration Laws

1. New York Convention 1958: Requires dispute be commercial and award issued in territory of state. Award issued on International Space Station, is it in territory? Gap.
2. UNCITRAL Model Law on Arbitration: Does not exclude space disputes. But does not regulate issue of seat of arbitration if parties chose low earth orbit as seat.

Conclusion: Current laws permit space arbitration, but do not understand it. We apply rules designed for factories to rockets.

Section Three: Comparative Law: Who Will Precede in Space Adjudication?

First Model: United States: Commercial Space Act 2015

Gave American citizen right to own resources he extracts from asteroids and moon. But said: This does not mean American sovereignty over asteroid.

Effect on Arbitration: Encouraged companies to include arbitration clause in New York with American law. America tries to impose its judiciary on space via arbitration.

Second Model: Luxembourg: Space Resources Law 2017

Same American idea. Grants companies right to ownership. And encourages arbitration in Luxembourg.

Result: Arbitration race. Every country wants arbitration seat on its territory to apply its law.

Third Model: Permanent Court of Arbitration in The Hague: Space Arbitration Rules 2011

Issued optional rules special for space disputes. Most important:

1. Arbitrator may be technical expert not only legal.
2. Seat of arbitration may be in outer space if parties agree.
3. Strict confidentiality to protect technology.

Problem: Rules are optional. And used only twice as of 2026.

Section Four: Evaluation and Proposed Vision: Toward a Hague Space System

First: Four Problems with No Solution Today

1. Problem of Applicable Law: Contract between Japanese company launching from Kazakhstan on Russian rocket for satellite serving Africa. Which law apply?
2. Problem of Execution: If arbitration award issued against company, how enforce it coercively? No bailiffs in orbit.
3. Problem of Parties: If unregistered debris destroyed your satellite, whom do you sue?
4. Problem of Sovereignty: If arbitrator ruled certain orbit belongs to company, does this create de facto sovereignty?

Second: Innovative Proposal: Convention Establishing International Organization for Space Arbitration

We propose new treaty of twenty articles. Most important features:

Article 3: Establishment of Court

There shall be established under this Convention Permanent Court of Space Arbitration with international legal personality. Its seat shall be The Hague, and it shall have right to hold sessions anywhere, including space stations.

Article 5: Applicable Law

1. If parties did not agree, Court shall apply general principles of space law derived from five treaties and from international custom and from general principles of law recognized in commercial systems.
2. Court may apply satellite law i.e. law of state of registration if dispute relates to satellite operation.

Article 7: Space Seat of Arbitration

Parties may agree that seat of arbitration shall be International Space Station or geostationary orbit. And in this case, Netherlands shall be deemed seat state for application of New York Convention by operation of law, unless agreed otherwise.

Article 9: Coercive Execution

1. States Parties shall undertake to recognize awards of Court and enforce them as if final awards issued by highest national court.
2. If award debtor is state, execution shall be via attachment of its space assets or prohibition of licensing its future launches.
3. There shall be established Orbit Police Unit following Organization, its mission documenting debris and executing space attachment measures by order of Court.

Article 12: Compensation Fund for Victims of Debris of Unknown Origin
States and launching companies shall fund international fund. It shall compensate injured party from unknown debris. Then fund shall have recourse against responsible if appears.

CONCLUSION: FROM PATCHWORK TO PHILOSOPHY

We began the book with a question: Is the Civil Code of 1948 sufficient?

And we ended with a truth: The digital revolution does not need patching of texts. It needs new philosophy.

We presented in seven tests seven solutions. United by one thread: The Criterion of the Close Digital Connection. A criterion that protects sovereignty and does not stifle innovation. Protects the human and does not stop progress.

This book is not an end. It is a record of opening a door. The rest is up to the legislator, the judge, and the jurist.

Completed with Praise of God. Ismailia, 21 April 2026.

REFERENCES

Elrakhawi, Mohamed Kamal Arafa. The Lex-Mathematica Protocol: Foundations of Algorithmic Jurisdiction, 2026.

Elrakhawi, Mohamed Kamal Arafa. Quantum Equations for Markets: The Mathematical Foundation of Algorithmic Compliance, 2026.

Elrakhawi, Mohamed Kamal Arafa. Lex-Mathematica in Court: Applying Mathematical Proof to Legal Disputes, 2026.

Elrakhawi, Mohamed Kamal Arafa. Dynamic Compliance Coefficient: A New Metric for Regulatory Oversight, 2026.

Elrakhawi, Mohamed Kamal Arafa. The Principle of Legal-Technical Uncertainty, 2026.

European Commission. Regulation on Artificial Intelligence (EU AI Act), Official Journal of the European Union, 2024.

United Nations. Convention on Contracts for the International Sale of Goods, Vienna, 1980.

United Nations. Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York Convention), 1958.

United Nations Educational, Scientific and Cultural Organization. Recommendation on the Ethics of Artificial Intelligence, Paris, 2021.

Court of Justice of the European Union. Google Spain SL v Agencia Espanola de Proteccion de Datos, Case C-131/12, 2014.

UNCITRAL. Model Law on Electronic Commerce, 1996.

UNCITRAL. Model Law on International Commercial Arbitration, 1985.

Financial Action Task Force. International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, 2024.

Transparency International. Global Corruption Barometer: Technology, 2024.

BaFin. Guidance Note on Supervisory Classification of Virtual Crypto Assets, 2013.

Law Commission of England and Wales. Smart Legal Contracts: Advice to Government, 2021.

Permanent Court of Arbitration. Optional Rules for Arbitration Relating to Outer Space Activities, 2011.
United States. Commercial Space Launch Competitiveness Act, 2015.
Luxembourg. Law on the Exploration and Use of Space Resources, 2017.
Republic of Korea. Anti-Corruption and Civil Rights Commission Act, 2008.
European Parliament and Council. Directive (EU) 2019/1937 on the Protection of Persons Who Report Breaches of Union Law, 2019.
Shannon, C. A Mathematical Theory of Communication, Bell System Technical Journal, 1948.
Taleb, Nassim Nicholas. The Black Swan: The Impact of the Highly Improbable, 2007.

INDEX

Administrative immunity, 245
Algorithmic liability, 45-68
Arbitration, space disputes, 267-290
Artificial intelligence, civil liability, 45-68
Black box problem, 52, 67
Blockchain, 155-182
Close Digital Connection criterion, 22, 179, 201
Cryptocurrency, legal nature, 155-182
Data protection, 195-224
Digital domicile, 22-24
Digital forgetting, right to, 195-224
Electronic documents, evidentiary value, 89-118
Evidence Law amendment, 114-118
Force majeure, smart contracts, 142
Good faith, whistleblower, 228
Jurisdiction, digital transactions, 21-24
Lex-Mathematica, 1-12
Liability, AI systems, 45-68
New York Convention, 272
Outer Space Treaty, 269
Personal data protection, 198
Public interest, 203
Reliability criterion, electronic documents, 115
Retaliation, criminalization, 251
Smart contracts, 119-154
Space arbitration, 267-290
UNCITRAL Model Law, 111, 273
Whistleblower protection, 225-266

KEYWORDS IN TEN LANGUAGES

English: Digital Revolution, Artificial Intelligence Liability, Electronic Evidence, Smart Contracts, Cryptocurrency, Right to Digital Forgetting, Whistleblower Protection, Space Arbitration, Close Digital Connection, Lex-Mathematica Protocol, Iconomics, Algorithmic Sovereignty.

Arabic: الثورة الرقمية، مسؤولية الذكاء الاصطناعي، الإثبات الإلكتروني، العقود الذكية، العملات المشفرة، الحق في النسيان الرقمي، حماية المبلغين عن الفساد، التحكيم في النزاعات الفضائية، معيار الارتباط الرقمي الوثيق، بروتوكول ليكس-ماتيماتيكا، أيقونوميكس، السيادة الخوارزمية.

French: Revolution Numerique, Responsabilite de l'Intelligence Artificielle, Preuve Electronique, Contrats Intelligents, Cryptomonnaie, Droit a l'Oubli Numerique, Protection des Lanceurs d'Alerte, Arbitrage Spatial, Connexion Numerique Proche, Protocole Lex-Mathematica, Iconomie, Souverainete Algorithmique.

Spanish: Revolucion Digital, Responsabilidad de la Inteligencia Artificial, Prueba Electronica, Contratos Inteligentes, Criptomoneda, Derecho al Olvido Digital, Proteccion de Denunciantes, Arbitraje Espacial, Conexion Digital Cercana, Protocolo Lex-Mathematica, Iconomia, Soberania Algoritmica.

German: Digitale Revolution, KI-Haftung, Elektronische Beweise, Smart Contracts, Kryptowahrung, Recht auf Digitales Vergessen, Whistleblower-Schutz, Weltraumschiedsgerichtsbarkeit, Enge Digitale Verbindung, Lex-Mathematica-Protokoll, Iconomics, Algorithmische Souveranitat.

Chinese: 数字革命，人工智能责任，电子证据，智能合约，加密货币，数字遗忘权，举报人保护，太空仲裁，密切数字联系，Lex-Mathematica 协议，Iconomics，算法主权。

Russian: Цифровая Революция, Ответственность Искусственного Интеллекта, Электронные Доказательства, Смарт-Контракты, Криптовалюта, Право на Цифровое Забвение, Защита Информаторов, Космический Арбитраж, Тесная Цифровая Связь, Протокол Лекс-Математика, Икономика, Алгоритмический Суверенитет.

Portuguese: Revolucao Digital, Responsabilidade da Inteligencia Artificial, Prova Eletronica, Contratos Inteligentes, Criptomoeda, Direito ao Esquecimento Digital, Protecao de Denunciantes, Arbitragem Espacial, Conexao Digital Proxima, Protocolo Lex-Mathematica, Iconomia, Soberania Algoritmica.

Japanese: デジタル革命，AI 責任，電子証拠，スマートコントラクト，暗号通貨，デジタル忘却権，内部告発者保護，宇宙仲裁，密接なデジタル接続，Lex-Mathematica プロトコル，Iconomics，アルゴリズム主権。

Turkish: Dijital Devrim, Yapay Zeka Sorumlulugu, Elektronik Delil, Akilli Sozlesmeler, Kripto Para, Dijital Unutulma Hakki, Ihbarcilarin Korunmasi, Uzay Tahkimi, Yakın Dijital Baglanti, Lex-Mathematica Protokolu, Iconomics, Algoritmik Egemenlik.

END OF DOCUMENT