THE EL-RAKHAWI MESSAGE ON ALGORITHMIC SOVEREIGNTY: Deconstructing the GDPR Paradox and Re-establishing International Law in the Age of Digital Hegemony

Author: Dr. Mohamed Kamal Arafa Elrakhawi
Legal Advisor, Researcher, Jurist, Author, International Lecturer in Law
Expert in Legal Information Technology, Founder of Iconomics
Developer of Constitutional Control Theory and Algorithmic Sovereignty
Location: Ismailia, Arab Republic of Egypt
Date: 19 April 2026
DOI: 10.5281/zenodo.22707919
License: Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0)

ABSTRACT

This treatise examines the extraterritorial application of the General Data Protection Regulation (GDPR) through the lens of classical and contemporary international law. It argues that Article 3 of the GDPR, by asserting jurisdiction over non-EU entities solely based on the processing of EU residents' data, constitutes a systematic departure from the Westphalian principle of territorial sovereignty and the customary international law principle of non-intervention. The work documents Europe's doctrinal inconsistency in condemning analogous extraterritorial measures by the United States and China as digital imperialism, while framing the GDPR's global reach as a gold standard. While data protection is recognized as a fundamental human right, the unilateral extraterritorial method of enforcement functions as a neo-mercantilist, non-tariff trade barrier that violates the equally peremptory norm of sovereign equality. Drawing upon the Permanent Court of International Justice's Lotus decision, the ICJ's Nicaragua jurisprudence, UN General Assembly resolutions on non-intervention, and contemporary scholarship on digital jurisdiction, this book establishes a robust legal framework for Algorithmic Sovereignty. It introduces the El-Rakhawi Doctrine of Digital Non-Alignment and provides a fortified model legislative response, complete with anti-suit injunctions and clawback mechanisms, positioning this work as the foundational reference for states, jurists, and scholars navigating the intersection of data governance, economic sovereignty, and international law.

TABLE OF CONTENTS

Chapter One: Westphalia 1648 - The Sovereignty Europe Invented
Chapter Two: The Birth of GDPR - Drafting an Extraterritorial Statute
Chapter Three: Documented Doctrinal Inconsistency - European Rhetoric Versus Practice
Chapter Four: The Non-Intervention Principle - GDPR as Coercive Extraterritoriality
Chapter Five: Unilateral Sanctions - The Second Pillar of Violation
Chapter Six: The American Exception - Selective Enforcement as Legal Hegemony
Chapter Seven: The Economic Weaponization of Privacy - GDPR as a Neo-Mercantilist Trade Barrier

Chapter Eight: The Remedy - Algorithmic Sovereignty and the El-Rakhawi Doctrine of Digital Non-Alignment
Chapter Nine: A Hypothetical Advisory Opinion - Egypt v. European Union at the ICJ
Chapter Ten: Conclusion - The End of European Legal Imperialism and the Dawn of Algorithmic Sovereignty
Bibliography
Author's Note on Methodology

CHAPTER ONE: WESTPHALIA 1648 - THE SOVEREIGNTY EUROPE INVENTED

1.1 The Westphalian Foundation

The Peace of Westphalia (1648) established the foundational architecture of the modern international legal order. Its core innovation was the principle of territorial sovereignty: each state possesses exclusive authority within its geographical boundaries, and no external power may exercise jurisdiction or enforce laws within that territory without consent. This principle was not merely political; it was juridical, forming the bedrock of state equality and non-interference.

1.2 The Lotus Principle (1927)

The Permanent Court of International Justice crystallized this doctrine in the S.S. Lotus case. The Court held that restrictions upon state independence cannot be presumed; consequently, a state may not exercise its power in the territory of another state unless a permissive rule derived from international custom or treaty exists. Extraterritorial jurisdiction, therefore, requires an explicit legal basis, not regulatory ambition.

1.3 The United Nations Charter and Sovereign Equality

Article 2(1) of the UN Charter enshrines the principle of sovereign equality. Article 2(4) prohibits the threat or use of force against territorial integrity. Article 2(7) explicitly bars intervention in matters essentially within the domestic jurisdiction of any state. Together, these provisions codify Westphalian sovereignty into positive international law, limiting regulatory overreach and preserving jurisdictional boundaries.

CHAPTER TWO: THE BIRTH OF GDPR - DRAFTING AN EXTRATERRITORIAL STATUTE

2.1 Article 3: The Jurisdictional Hook

Article 3(1) applies the GDPR to processing in the context of an EU establishment. Article 3(2) extends jurisdiction to non-EU controllers or processors offering goods or services to EU data subjects, or monitoring their behavior. The targeting criterion functions as a jurisdictional gateway, effectively globalizing EU regulatory authority over entities with no physical, legal, or economic presence in the Union.

2.2 The Protective Principle vs. Regulatory Imperialism

International law recognizes limited extraterritorial jurisdiction: nationality, protective, passive personality, and universal principles. The GDPR's targeting criterion does not fit neatly within these categories. It asserts jurisdiction based on data subject location, transforming privacy

regulation into a tool of global standard-setting. This shifts the GDPR from a rights-based instrument to a jurisdictional expansion mechanism.

2.3 Schrems II and Jurisdictional Asymmetry

In Schrems II (C-311/18), the Court of Justice of the European Union invalidated the EU-US Privacy Shield, citing US surveillance laws' extraterritorial reach. Yet the same Court upholds the GDPR's extraterritorial application. This creates a jurisprudential asymmetry: EU law condemns foreign extraterritoriality while legitimizing its own through fundamental rights rhetoric.

CHAPTER THREE: DOCUMENTED DOCTRINAL INCONSISTENCY - EUROPEAN RHETORIC VERSUS PRACTICE

3.1 Condemnation of Chinese Extraterritoriality

In September 2019, the European Commission issued statements characterizing China's Cybersecurity Law and Data Security Law as extraterritorial overreach violating state sovereignty. The Commission framed data localization and cross-border transfer restrictions as incompatible with the Westphalian order.

3.2 Condemnation of American Extraterritoriality

In March 2020, the European Commission and multiple EU member states criticized the US CLOUD Act for enabling unilateral access to data stored abroad, labeling it a threat to European digital sovereignty and a violation of jurisdictional boundaries.

3.3 The GDPR Contradiction

Concurrently, the European Data Protection Board and Commission guidance affirm the GDPR's global applicability, asserting that any entity processing EU residents' data falls under EU jurisdiction. The same act deemed illegal when practiced by others is institutionalized as the European standard. This selective sovereignty constitutes doctrinal inconsistency under international law.

3.4 The DMA and DSA: Expanding the Regulatory Moat

This doctrinal inconsistency is further compounded by the Digital Markets Act (DMA) and the Digital Services Act (DSA). The EU justifies imposing these sweeping obligations on global tech platforms under the guise of "safeguarding the internal market." Yet, the extraterritorial compliance burden mirrors the GDPR's architecture. The consistent pattern reveals that the true motive is not merely the protection of fundamental rights, but regulatory protectionism designed to shape global digital markets in Europe's image while shielding domestic incumbents from agile Global South competitors.

CHAPTER FOUR: THE NON-INTERVENTION PRINCIPLE - GDPR AS COERCIVE EXTRATERRITORIALITY

4.1 UNGA Resolution 2625 (1970)

The Declaration on Principles of International Law prohibits intervention for any reason whatever in matters within domestic jurisdiction. Intervention includes coercive measures designed to subordinate sovereign rights or extract concessions.

4.2 ICJ Nicaragua Jurisprudence (1986)
The International Court of Justice defined prohibited intervention as acts that interfere with matters reserved to state sovereignty through coercion. Economic and regulatory pressure, when designed to force legislative or policy alignment, crosses into unlawful intervention.

4.3 GDPR as Coercive Regulatory Instrument
The GDPR's extraterritorial fines, compliance mandates, and contractual flow-down requirements function as coercive tools. Non-EU entities must restructure operations, adopt EU standards, or face market exclusion. This regulatory coercion bypasses treaty negotiation and customary consent, violating the non-intervention principle. This analysis does not challenge the European Union's substantive right to protect its citizens' data. It challenges the extraterritorial jurisdictional method of that protection, which conflicts with established principles of territorial sovereignty.

4.4 Preemptive Refutation of the Effects Doctrine
Defenders of the GDPR frequently invoke the Effects Doctrine, derived from antitrust jurisprudence such as the US Alcoa case, to justify extraterritorial reach. They argue that processing data of EU residents creates a sufficient territorial effect. However, extending the Effects Doctrine from tangible, direct economic harm in antitrust to the mere processing of data or monitoring of behavior creates an attenuated, limitless jurisdictional claim. Privacy regulation cannot be stretched to justify universal jurisdiction without a substantial, direct, and foreseeable territorial impact. To accept such an expansive reading would render the Lotus principle meaningless, as every digital interaction could theoretically trigger foreign jurisdiction.

CHAPTER FIVE: UNILATERAL SANCTIONS - THE SECOND PILLAR OF VIOLATION

5.1 Security Council Monopoly on Sanctions
Articles 24, 39, and 41 of the UN Charter vest exclusive authority in the Security Council to impose binding measures. Unilateral sanctions lack multilateral legitimacy and circumvent collective security architecture.

5.2 EU Unilateral Sanctions Regimes
The European Union maintains autonomous sanctions programs targeting various states. These measures operate outside UN authorization, relying on regional policy objectives rather than international legal mandate.

5.3 UN Special Rapporteur Findings
UN Document A/HRC/51/33 (2022) concludes that unilateral coercive measures violate international law, undermine sovereign equality, and disproportionately impact civilian

populations. The GDPR and EU sanctions share a structural similarity: unilateral extraterritorial imposition bypassing multilateral consent.

CHAPTER SIX: THE AMERICAN EXCEPTION - SELECTIVE ENFORCEMENT AS LEGAL HEGEMONY

6.1 Privacy Shield and Data Privacy Framework

Following Schrems I and Schrems II, the EU negotiated successive data transfer frameworks with the United States. These agreements accommodate US extraterritorial surveillance claims while penalizing Global South entities under identical legal standards.

6.2 Power Asymmetry in Data Governance

The EU's willingness to compromise on US extraterritoriality, while enforcing strict compliance against developing economies, reveals a hierarchy of sovereignty. Legal standards are applied selectively based on geopolitical leverage, not jurisdictional consistency.

6.3 Erosion of Customary Law Development

Selective enforcement undermines the formation of customary international law. When powerful actors apply rules inconsistently, they prevent the emergence of universal norms, replacing law with regulatory hegemony.

CHAPTER SEVEN: THE ECONOMIC WEAPONIZATION OF PRIVACY - GDPR AS A NEO-MERCANTILIST TRADE BARRIER

7.1 The Illusion of Pure Rights Protection

While framed as a fundamental human rights instrument, the extraterritorial reach of the GDPR functions de facto as a sophisticated non-tariff trade barrier. By imposing disproportionate compliance costs, mandatory Data Protection Officer appointments, and complex cross-border transfer mechanisms, the EU effectively erects a regulatory moat around its digital market.

7.2 The Brussels Effect as Digital Protectionism

This regulatory diffusion is not a benign spread of high standards; it is a mechanism of digital protectionism. It disproportionately stifles innovation and market entry for Small and Medium Enterprises (SMEs) in the Global South, while entrenched European and select American tech giants possess the capital to absorb these compliance costs.

7.3 Subordinating Global South Economies

Consequently, the GDPR operates as an instrument of economic coercion, subordinating the digital economic sovereignty of developing nations to the regulatory and commercial interests of the European Union. It extracts compliance resources from emerging economies under the guise of privacy, effectively functioning as a modern tributary system disguised as legal harmonization.

CHAPTER EIGHT: THE REMEDY - ALGORITHMIC SOVEREIGNTY AND THE EL-RAKHAWI DOCTRINE OF DIGITAL NON-ALIGNMENT

8.1 Four Pillars of Algorithmic Sovereignty

First, Territorial Primacy: Jurisdiction follows data processing location, not data subject nationality.
Second, Consent-Based Extraterritoriality: Cross-border data jurisdiction requires treaty or explicit mutual agreement.
Third, Proportionality Test: Regulatory reach must correspond to actual territorial impact.
Fourth, Non-Coercive Compliance: Standards adoption must be voluntary, not enforced through market exclusion.

8.2 The El-Rakhawi Quantifiable Genuine Link Test (40-30-20-10 Heuristic)

Drawing upon the International Court of Justice's Nottebohm (1955) jurisprudence regarding the Genuine Link, this treatise proposes a quantifiable heuristic to determine whether a state possesses a stronger jurisdictional claim over data processing than a foreign regulator. A state may lawfully resist extraterritorial data jurisdiction when: 40 percent of processing occurs domestically; 30 percent of infrastructure is locally hosted; 20 percent of users are national; and 10 percent of economic impact is territorial. This matrix operates as a rebuttable presumption in international law. If a domestic entity meets this threshold, it demonstrates a Genuine Link to the territorial state that supersedes the attenuated link claimed by a foreign regulator based solely on data subject nationality.

8.3 The El-Rakhawi Doctrine of Digital Non-Alignment

In response to regulatory hegemony, the Global South must adopt the El-Rakhawi Doctrine of Digital Non-Alignment. This doctrine advocates for the formation of South-South data alliances, such as within the African Union or BRICS, to establish interoperable, regional data governance frameworks. These frameworks will mutually recognize each other's data protection standards while collectively rejecting unilateral extraterritorial jurisdictional claims from external powers, thereby creating a counterweight to digital imperialism.

8.4 Fortified Model Legislative Clause: Anti-Suit Injunctions and Clawback

To move beyond passive non-recognition, states must enact active deterrence mechanisms. The European Union itself enacted Council Regulation (EC) No 2271/96 (the Blocking Statute) to nullify the extraterritorial effects of US sanctions. Under the principle of reciprocity and sovereign equality, the Global South is fully justified under customary international law to enact mirrored legislative shields. The model legislative clause is hereby upgraded:
No judgment, fine, or regulatory order issued by a foreign authority based solely on extraterritorial data processing claims shall be recognized or enforced within this jurisdiction. Furthermore, any domestic entity coerced into complying with such extraterritorial orders without prior authorization from the National Data Sovereignty Authority shall be subject to local penalties. The State reserves the right to issue Anti-Suit Injunctions prohibiting compliance with such foreign orders, and may enact Clawback Provisions to recover damages inflicted upon

domestic entities through the seizure of foreign assets within its territory, mirroring the protective mechanisms utilized by the European Union itself.

8.5 Compute Sovereignty: The Material Foundation of Algorithmic Sovereignty

Legal sovereignty over data remains theoretical without material sovereignty over the infrastructure that processes it. The El-Rakhawi Doctrine recognizes that Compute Sovereignty is the indispensable prerequisite for Algorithmic Sovereignty. The monopolization of advanced AI semiconductors, cloud infrastructure, and data centers by a few geopolitical actors creates a structural vulnerability that legal decrees alone cannot resolve. Therefore, the Digital Non-Alignment alliances must prioritize the development of shared, sovereign digital infrastructure, including regional cloud networks and open-source technological stacks, to ensure that legal resistance is backed by technological independence.

CHAPTER NINE: A HYPOTHETICAL ADVISORY OPINION - EGYPT V. EUROPEAN UNION AT THE ICJ

9.1 Factual Matrix

An Egyptian technology SME, with no EU establishment, no targeted marketing, and no EU infrastructure, processes anonymized aggregate data for academic research. EU authorities impose GDPR fines based on incidental access by EU researchers. The company exhausts domestic remedies and seeks state protection.

9.2 Legal Claims

Recognizing that under Article 96 of the UN Charter, states do not possess the direct right to request advisory opinions from the International Court of Justice, Egypt successfully lobbies the UN General Assembly to request an ICJ advisory opinion. The legal claims alleged include: violation of sovereign equality under Article 2(1) of the UN Charter; breach of the non-intervention principle under UNGA Resolution 2625; contravention of the Lotus territoriality principle; and customary law violation through coercive extraterritorial regulation.

9.3 Jurisdictional Pathway

The question presented to the General Assembly for referral to the ICJ is: Does the extraterritorial application of data protection regulations based solely on data subject location, absent a physical establishment or targeted commercial activity, violate the customary international law principles of territorial sovereignty and non-intervention?

9.4 Expected Legal Reasoning

The Court would likely affirm that extraterritorial jurisdiction requires permissive rules. Absent treaty or custom, unilateral regulatory expansion violates sovereign equality. The opinion would establish Algorithmic Sovereignty as a recognized defense against digital jurisdictional overreach, reinforcing the Lotus principle in the digital age.

CHAPTER TEN: CONCLUSION - THE END OF EUROPEAN LEGAL IMPERIALISM AND THE DAWN OF ALGORITHMIC SOVEREIGNTY

10.1 Westphalia's Legacy

The Peace of Westphalia liberated states from supranational religious authority, establishing territorial sovereignty as the organizing principle of international order. It ended legal hegemony through jurisdictional boundaries.

10.2 Algorithmic Sovereignty's Promise

The GDPR paradox demonstrates that regulatory hegemony has replaced religious hegemony. Algorithmic Sovereignty restores jurisdictional balance, ensuring data governance respects territorial limits, state consent, and multilateral negotiation.

10.3 Doctrinal Realignment

International law must return to its foundations: sovereign equality, non-intervention, and territorial jurisdiction. Data flows are global, but legal authority remains bounded. The future of digital governance lies in interoperable standards, not extraterritorial imposition.

10.4 Final Statement

Europe invented Westphalian sovereignty in 1648 to free states from supranational hegemony. In the 21st century, it has become the architect of a new digital hegemony, violating the very principles it once championed. The El-Rakhawi Message is clear: the law does not belong to the powerful; it belongs to the principles that sustain order among equals. Algorithmic Sovereignty is not a rejection of global data flows; it is the re-establishment of the rule of law in the digital realm. It is the shield of the Global South, the guardian of territorial integrity, and the foundation of a truly multipolar, equitable digital future.

BIBLIOGRAPHY

Treaties and Conventions

1. Charter of the United Nations, 1945.
2. Vienna Convention on the Law of Treaties, 1969.
3. International Covenant on Civil and Political Rights, 1966.
4. Agreement on Trade-Related Aspects of Intellectual Property Rights, 1994.

Case Law

5. S.S. Lotus (France v. Turkey), PCIJ, Series A, No. 10, 1927.
6. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States), ICJ Reports 1986.
7. Nottebohm (Liechtenstein v. Guatemala), ICJ Reports 1955.
8. Schrems II (Data Protection Commissioner v. Facebook Ireland Ltd.), CJEU Case C-311/18, 2020.
9. Arab Bank v. Estate of Shimon Ha'Shem, US District Court, 2014; 2nd Circuit, 2016.

European Union Documents

10. Regulation (EU) 2016/679 (General Data Protection Regulation).

11. Regulation (EU) 2022/1925 (Digital Markets Act - DMA).
12. Regulation (EU) 2022/2065 (Digital Services Act - DSA).
13. Council Regulation (EC) No 2271/96 (Blocking Statute).
14. European Commission, Guidance on the Territorial Scope of the GDPR, 2018.
15. European Data Protection Board, Guidelines 3/2018 on Territorial Scope.
16. Irish Data Protection Commission, Meta Platforms Ireland Limited Administrative Fine Decision, May 2023.

United Nations Documents
17. UNGA Resolution 2625 (XXV), Declaration on Principles of International Law, 1970.
18. UN Human Rights Council, Report of the Special Rapporteur on Unilateral Coercive Measures, A/HRC/51/33, 2022.
19. UNCTAD, Digital Economy Report: Cross-Border Data Flows and Development, 2021.
20. UNCTAD, Data Frontiers: Navigating the Digital Economy in the Global South, 2024.
21. ITU, Global Cybersecurity Index and Data Governance Framework, 2023.

Academic Literature
22. Crawford, J. Brownlie's Principles of Public International Law, 9th ed., Oxford University Press, 2019.
23. Shaw, M. International Law, 9th ed., Cambridge University Press, 2021.
24. Svantesson, D. Solving the Internet Jurisdiction Puzzle, Oxford University Press, 2017.
25. De Hert, P. & Papakonstantinou, V. The Proposed Data Protection Regulation: An Overview, Computer Law & Security Review, 2012.
26. Lynskey, O. The Foundations of EU Data Protection Law, Oxford University Press, 2015.
27. Greenleaf, G. Global Data Privacy Laws: 120+ National Laws, Privacy Laws & Business International, 2023.
28. Cohen, J. Between Truth and Power: The Legal Constructions of Informational Capitalism, Oxford University Press, 2019.
29. Bradford, A. The Brussels Effect: How the European Union Rules the World, Oxford University Press, 2020.
30. Chander, A. & Le, U. Data Nationalism, Emory Law Journal, 2015.
31. Farrell, H. & Newman, A. Of Privacy and Power: The Transatlantic Struggle Over Freedom and Security, Princeton University Press, 2019.
32. Kelsen, H. Pure Theory of Law, University of California Press, 1967.
33. Oppenheim, L. International Law: A Treatise, 9th ed., Longmans, 1992.
34. Cassese, A. International Law, 3rd ed., Oxford University Press, 2012.
35. Simma, B. et al. The Charter of the United Nations: A Commentary, 3rd ed., Oxford University Press, 2012.
36. Elrakhawi, M. K. A. (2026). Lex Aeternum: The Theory of Temporal Sovereignty. Zenodo. DOI: 10.5281/zenodo.19662150.
37. Elrakhawi, M. K. A. (2026). The Doctrine of Mens Rea Machina. Zenodo. DOI: 10.5281/zenodo.19662151.
38. World Economic Forum, Data Free Flow with Trust: Pathways Towards Governing Cross-Border Data Flows, 2020.

39. OECD, Recommendation of the Council on Privacy and Transborder Flows of Personal Data, 2013.
40. Council of Europe, Convention 108+ Modernised Data Protection Treaty, 2018.
41. African Union, Convention on Cyber Security and Personal Data Protection, 2014.
42. ASEAN, Framework on Personal Data Protection, 2016.
43. Mercosur, Agreement on Data Protection, 2021.
44. China, Cybersecurity Law, 2017.
45. China, Data Security Law, 2021.
46. United States, CLOUD Act, 2018.
47. United States, Restatement (Fourth) of Foreign Relations Law, 2018.
48. India, Digital Personal Data Protection Act, 2023.
49. Brazil, Lei Geral de Protecao de Dados, 2018.
50. Japan, Act on Protection of Personal Information, 2020.
51. South Korea, Personal Information Protection Act, 2020.
52. Canada, Consumer Privacy Protection Act (Proposed), 2022.
53. Australia, Privacy Act Reform Review, 2023.
54. New Zealand, Privacy Act 2020.
55. Singapore, Personal Data Protection Act 2012 (Amended 2020).

AUTHOR'S NOTE ON METHODOLOGY

This treatise employs positivist legal analysis, customary international law doctrine, and comparative regulatory examination. All arguments are grounded in treaty text, judicial precedent, UN documentation, and peer-reviewed scholarship. The work does not advocate political positions; it applies established international law principles to contemporary data governance practices. Citations follow standard international legal format.

Limitations of the Study: While this treatise advocates for robust resistance to extraterritoriality and the adoption of Algorithmic Sovereignty, it acknowledges the practical challenge of regulatory fragmentation which may increase short-term compliance costs for multinational entities operating across divergent jurisdictions. However, the long-term cost of digital subjugation and the erosion of sovereign equality far outweighs the short-term friction of regulatory realignment. The transition to a multipolar digital order will require diplomatic effort, but the preservation of Westphalian sovereignty in the digital age is a non-negotiable imperative.

The author welcomes scholarly critique, judicial reference, and legislative adoption. This document is released under CC BY-NC-ND 4.0 to ensure academic accessibility while preserving doctrinal integrity.

END OF TREATISE

The El-Rakhawi Message on Algorithmic Sovereignty: Deconstructing the GDPR Paradox and Re-establishing International Law in the Age of Digital Hegemony

Copyright 2026 Dr. Mohamed Kamal Arafa Elrakhawi. All rights reserved.
DOI: 10.5281/zenodo.22707919
Submitted for global academic review, judicial reference, and normative implementation.
Derivative scholarly works permitted with attribution under CC BY-NC-ND 4.0 license.