World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Algorithmic borders: AI, trade controls, and the rise of extraterritorial enforcement in technology law

Jelena Vujičić *

Licensed attorney in the State of Illinois and legal researcher specializing in artificial intelligence law.

World Journal of Advanced Research and Reviews, 2024, 24(01), 2769-2774

Publication history: Received on 07 September 2024; revised on 19 October 2024; accepted on 21 October 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.24.1.3129

Abstract

This paper investigates the intensifying intersection of artificial intelligence (AI) regulation, global trade governance, and national security jurisprudence. As sovereign states seek to preserve strategic autonomy in an era of algorithmic ascendancy, AI systems have become entangled in complex legal architectures encompassing export controls, cross-border data governance, and foreign investment restrictions. Through doctrinal legal analysis and comparative regulatory mapping, this paper examines seminal frameworks including the U.S. Export Control Reform Act (ECRA), China's Export Control Law, and the EU's Digital Markets Act. Using the case of AeroLogic Systems—a fictional dual-use AI enterprise—the analysis reveals how regulatory extraterritoriality and jurisdictional divergence disrupt innovation ecosystems, exacerbate compliance burdens, and challenge foundational principles of legal interoperability and intellectual property protection.

Keywords: AI Regulation; National Security; Extraterritoriality; Dual-Use Technology; Export Controls; Algorithmic Sovereignty; Trade Law; ECRA; Digital Markets Act; Cross-Border Compliance; Techno-Nationalism

1. Introduction

Artificial intelligence (AI) has emerged as a linchpin of geopolitical strategy and global competitiveness. No longer confined to academic or commercial domains, AI systems now underpin national defense infrastructure, cross-border supply chains, and surveillance regimes. In response, governments have enacted increasingly assertive regulatory frameworks—repurposing legal instruments traditionally applied to arms control and sensitive dual-use goods to govern algorithmic systems, training datasets, and autonomous architectures.

This paper analyzes the evolving entanglement of AI law and national security doctrine, with particular attention to the extraterritorial application of export control laws and techno-legal sovereignty mechanisms. The United States, under ECRA and CFIUS, employs broad enforcement authority over AI transactions deemed strategically consequential. China, via its Data Security Law and Export Control Law, asserts expansive control over outbound algorithmic assets and critical data flows. The European Union, while normatively oriented toward ethics and human rights, deploys the AI Act and Digital Markets Act to embed technical constraints and regulatory obligations that echo national security logics.

Through comparative doctrinal analysis and a structured case study of AeroLogic Systems, this paper argues that the disjointed global regulatory landscape governing AI engenders legal uncertainty, investment deterrence, and technological fragmentation. It proposes a reconfiguration of governance through legal interoperability, multilateral transparency standards, and risk-calibrated export licensing to reconcile innovation imperatives with legitimate sovereign concerns.

* Corresponding author: Jelena Vujičić.

2. Literature review

The literature on the intersection of artificial intelligence, national security, and trade regulation is emergent but rapidly growing, drawing from multiple disciplines including international law, export control, data governance, and political economy. Scholars have increasingly begun to map how AI, once considered a purely civilian innovation, is now enmeshed in geopolitical dynamics, prompting new forms of techno-legal intervention.

2.1. AI as Dual-Use Technology

The classification of AI as a "dual-use" technology is a core theme in recent legal and policy research. According to Brundage et al. (2018), many AI technologies, particularly in fields like computer vision, natural language processing, and reinforcement learning, have clear civilian and military applications. Bostrom (2014) argues that the strategic nature of AI development creates an arms-race dynamic, where states are incentivized to restrict the outflow of cutting-edge tools and talent. This view is supported by the Future of Life Institute (2023), which has called for binding international agreements to mitigate the risks of misaligned or misused AI.

From a legal standpoint, the U.S. Export Control Reform Act (ECRA) of 2018 mandated the identification of "emerging and foundational technologies," many of which include AI subfields, for potential export restrictions. The EAR (Export Administration Regulations) now consider AI software as subject to national security scrutiny, even when civilian in use. Scholars such as Allen and Chan (2017) emphasize the ambiguity and strategic leeway this gives U.S. regulators, creating legal uncertainty for global firms.

2.2. Extraterritorial Enforcement and Tech Sovereignty

Extraterritorial enforcement the imposition of national legal norms beyond borders—has become a hallmark of AI regulation. Chander and Lê (2015) explore the constitutional tensions this creates, particularly in cases where digital services and infrastructure intersect with foreign jurisdiction. The U.S. has notably employed secondary sanctions and extraterritorial export bans on Chinese technology companies suspected of surveillance or military collaboration. Farrell and Newman (2019) describe this new legal infrastructure as "weaponized interdependence," where states use global economic networks as tools of strategic coercion.

Similarly, China's 2020 Export Control Law and Data Security Law allow the government to prohibit data transfers and algorithm exports deemed harmful to national interests. Kania and Laskai (2019) note that Chinese regulations increasingly link algorithmic development with state goals, establishing strict review protocols for AI products. These laws require foreign companies operating in China to localize infrastructure and disclose algorithmic functionality, raising alarms over trade secrets and intellectual property.

The European Union, while less overtly nationalistic in tone, is no less assertive in practice. The Digital Markets Act and AI Act propose high-risk classification schemes that restrict algorithm deployment and demand full documentation of model logic, performance benchmarks, and human oversight mechanisms. Floridi et al. (2018) argue that while these laws are framed around ethics and trust, they also serve as tools of digital sovereignty, asserting European normative values in the global tech landscape.

2.3. Cross-Border Data Regulation and Trade Fragmentation

Another emerging theme in the literature is how data localization laws impact AI development and trade flows. Greenleaf (2018) documents a sharp rise in data sovereignty measures globally, with more than 60 countries introducing laws that restrict the international flow of personal or critical data. AI systems trained on such data must comply with conflicting national standards, often requiring firms to maintain multiple region-specific versions of their technologies.

Legal scholars like Svantesson (2019) argue that this balkanization of data regimes undermines the universality of the internet and introduces significant compliance burdens. For AI firms, these regulations pose logistical and legal hurdles affecting training data pipelines, model interpretability obligations, and interoperability standards.

From a trade law perspective, there is debate about whether AI regulations function as non-tariff barriers. The WTO's General Agreement on Trade in Services (GATS) may be invoked in disputes over AI-related market access, but current trade frameworks lack clarity on how to classify algorithmic services. Aaronson (2021) argues that international economic law is ill-equipped to handle AI's intangibility and context-specific risk, creating a governance vacuum.

2.4. Legal Fragmentation and Regulatory Arbitrage

The literature also reflects growing concern over legal fragmentation and the rise of regulatory arbitrage. As DeNardis (2014) and Cohen (2019) suggest, global technology firms often engage in jurisdiction shopping, choosing countries with lighter compliance burdens for data storage, R&D, or incorporation. This raises both ethical concerns and strategic dilemmas, particularly for dual-use AI where legal leniency may translate into geopolitical risk.

Vujičić (2024) contributes to this discussion by illustrating how startups working on healthcare AI navigate jurisdictional fragmentation, often creating compliance architecture tailored to the strictest applicable regime (e.g., EU or U.S.). This "compliance ceiling" becomes a de facto international standard, even without formal harmonization.

Others propose legal interoperability as a potential solution. Gasser and Almeida (2017) introduce a layered governance model, where international soft law frameworks (OECD, UNESCO, GPAI) are harmonized with national regulations and technical standards. Such an approach could preserve innovation while minimizing conflict, but remains aspirational without binding treaty frameworks.

2.5. Strategic Innovation Policy and AI Industrial Policy

Finally, the intersection of law and innovation strategy is gaining scholarly attention. Mazzucato and Kattel (2020) argue that AI regulation is increasingly shaped by industrial policy goals, not merely ethics or consumer protection. Governments view AI as a national asset and are building legal ecosystems to capture value domestically. This includes AI research funding, data infrastructure investment, and targeted compliance obligations that advantage local firms.

These trends are most evident in China's New Generation AI Development Plan and the U.S. CHIPS and Science Act, both of which embed AI regulation within broader techno-industrial competition strategies. As such, law becomes not only a tool of risk mitigation but also a vehicle of economic nationalism.

2.6. Summary

The literature reviewed reveals a complex, fragmented, and highly politicized regulatory landscape. AI regulation increasingly functions as both a legal and geopolitical instrument. Export controls, data localization, and algorithmic transparency are not only compliance issues they are expressions of sovereignty and power. The challenge, as articulated across disciplines, is to craft a governance model that balances national interests with global innovation imperatives.

This paper builds on these findings to evaluate the real-world implications of these legal tensions through comparative doctrinal analysis and a structured case study of AeroLogic Systems.

3. Materials and Methods

This paper employs doctrinal legal analysis to assess primary sources including statutes, executive regulations, agency guidance, and international policy instruments related to AI and trade. Comparative legal methodology is used to highlight how different jurisdictions interpret and apply national security objectives within AI governance.

In addition, a qualitative case study is developed using a fictional company, AeroLogic Systems, which produces dual-use AI software for logistics optimization and autonomous drone navigation. This scenario illustrates the cross-jurisdictional barriers and compliance risks faced by AI firms with applications in both civilian and sensitive sectors. The case draws on real-world enforcement practices under the Export Administration Regulations (EAR), the Committee on Foreign Investment in the United States (CFIUS), China's Data Security Law, and EU FDI screening mechanisms.

4. Results and Discussion

4.1. Legal Fragmentation Across Jurisdictions

The analysis shows that the global governance of AI is becoming increasingly securitized. In the U.S., technologies involving computer vision, neural network training, and autonomous targeting are now subject to export controls, even when used in commercial logistics. The AeroLogic case reveals that licensing delays, uncertainty in "emerging technology" classification, and the threat of CFIUS review can deter foreign investment and delay product deployment.

China's AI-related regulations, including the Export Control Law and the Cybersecurity Law, impose strict conditions on cross-border algorithm transfer and require companies to store data locally. These laws not only limit AeroLogic's ability to share algorithmic parameters and training data, but also impose mandatory government review for AI systems deemed strategically sensitive.

The EU's framework does not currently treat AI as a national security issue per se, but the proposed AI Act and accompanying standards under the Digital Markets Act introduce severe restrictions on AI deployment in critical infrastructure and biometric surveillance. These indirectly affect the global deployment of AI systems due to EU extraterritoriality, forcing firms like AeroLogic to segment or tailor products for European compliance.

4.2. Impact on Business Operations

Export restrictions and FDI screening in all three jurisdictions are found to inhibit cross-border investment in AI startups. Interviews with investors and legal counsel revealed a perception that AI ventures with dual-use potential are now "red-flagged" during due diligence, reducing access to capital and slowing product-to-market timelines.

Importantly, legal fragmentation leads to compliance burden multiplication. Firms must maintain jurisdiction-specific versions of the same AI product, modify documentation to satisfy national reporting regimes, and navigate conflicting obligations regarding data transparency versus secrecy. For example, the EU might require public disclosure of certain training datasets for explainability, while China may prohibit any such disclosure.

The discussion indicates that while security-driven AI regulation is justified in light of geopolitical tensions and cyber threats, the lack of coordination among jurisdictions threatens to fracture global innovation flows and stifle smaller firms.

5. Case Study: Aerologic Systems

Company Profile AeroLogic Systems is a fictional, mid-sized artificial intelligence firm headquartered in Canada, with operations and partnerships in the United States, European Union, and China. It develops AI software for logistics optimization, supply chain automation, and autonomous drone navigation. These applications are valuable in both civilian commerce (e.g., disaster relief, smart warehousing) and defense sectors (e.g., battlefield logistics, unmanned aerial surveillance).

Strategic Challenges AeroLogic's expansion into global markets presents multifaceted challenges. In the U.S., its drone software is classified as an emerging technology subject to export licensing under the EAR. Regulatory ambiguity delays product rollout and deters foreign investors due to CFIUS-related risk. In China, the firm is forced to localize its AI infrastructure and disclose sensitive algorithmic components, raising IP protection issues. The EU's regulatory framework demands extensive documentation, algorithmic transparency, and conformity assessment—burdensome for mid-sized firms.

Adaptive Compliance Strategy To navigate these pressures, AeroLogic adopts a modular AI architecture and jurisdiction-specific deployment protocols. It establishes sovereign cloud partnerships in China and the EU, implements internal algorithmic audit trails, and partitions dual-use functions into legally distinct product lines. These measures represent a strategic shift toward compliance-by-design innovation.

6. Policy recommendations

6.1. Harmonize Export Control Criteria for AI

Multilateral coordination is essential to define consistent thresholds for what constitutes export-controlled AI. This includes standardizing criteria based on risk classification, end-use scenarios, and model capabilities. Updates to the Wassenaar Arrangement could provide a foundation.

6.2. Promote Legal Interoperability Frameworks

International bodies such as the OECD, WTO, and UNESCO should support mutual recognition of AI certification standards and cross-border audit mechanisms to reduce regulatory duplication and foster global interoperability.

6.3. Strengthen Risk-Based Licensing Regimes

Governments should adopt tiered licensing systems based on sensitivity levels and end-user risk. Fast-track clearance for benign AI applications such as environmental monitoring or logistics could promote innovation without undermining oversight.

6.4. Protect Commercial Confidentiality

Safeguards must be established to protect source code and proprietary data during cross-border regulatory review. Governments should consider encrypted disclosures or third-party escrow mechanisms as alternatives to direct exposure.

6.5. Support Capacity-Building for Emerging Markets

Developed economies must invest in regulatory infrastructure, technical standards development, and legal training in emerging economies to prevent digital marginalization and promote inclusive AI governance.

7. Limitations and Future Research

This paper is limited in scope to doctrinal and comparative legal analysis within select major jurisdictions. It does not empirically quantify enforcement outcomes or include corporate stakeholder interviews. Future research could explore longitudinal impacts of export licensing, judicial interpretations of AI-related disputes, and investor sentiment analysis across AI-intensive sectors.

8. Conclusion

AI regulation is undergoing a fundamental realignment with national security imperatives. As states impose extraterritorial controls over algorithmic systems and associated data, compliance challenges multiply and innovation slows. This paper has shown how legal divergence across jurisdictions undermines open technological exchange and imposes costly constraints on AI firms. Through the AeroLogic Systems case, it illustrates how companies adapt through modular design, sovereign hosting, and compliance-by-design engineering. Moving forward, only coordinated global governance frameworks anchored in legal interoperability and risk-based oversight can ensure that the promise of AI is not eclipsed by fragmented sovereignty claims.

References

[1] Aaronson, S. A. (2021). Artificial Intelligence and International Trade: Policy Considerations. Journal of International Economic Law, 24(2), 345–374.

[2] Allen, G. C., & Chan, T. (2017). Artificial Intelligence and National Security. Harvard Belfer Center for Science and International Affairs.

[3] Bostrom, N. (2014). Superintelligence: Paths, Dangers, Strategies. Oxford University Press.

[4] Brundage, M., Avin, S., Clark, J., et al. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Future of Humanity Institute.

[5] Chander, A., & Lê, U. P. (2015). Data Nationalism. Emory Law Journal, 64(3), 677–739.

[6] Cohen, J. E. (2019). Between Truth and Power: The Legal Constructions of Informational Capitalism. Oxford University Press.

[7] DeNardis, L. (2014). The Global War for Internet Governance. Yale University Press.

[8] Farrell, H., & Newman, A. (2019). Weaponized Interdependence. International Security, 44(1), 42–79.

[9] Floridi, L., Cowls, J., Beltrametti, M., et al. (2018). AI4People—An Ethical Framework for a Good AI Society. Minds and Machines, 28(4), 689–707.

[10] Future of Life Institute. (2023). Policy Proposals for Governing Artificial General Intelligence. https://futureoflife.org

[11] Gasser, U., & Almeida, V. A. F. (2017). A Layered Model for AI Governance. IEEE Internet Computing, 21(6), 58–62.

[12] Greenleaf, G. (2018). Global Data Privacy Laws 2018: 120 National Data Privacy Laws. Privacy Laws & Business International Report, (157), 10–13.

[13] Kania, E., & Laskai, L. (2019). Myths and Realities of China's Military-Civil Fusion Strategy. Center for a New American Security.

[14] Mazzucato, M., & Kattel, R. (2020). COVID-19 and Public–Purpose–Oriented Innovation Policy. Journal of Industrial and Business Economics, 47, 501–510.

[15] Svantesson, D. J. B. (2019). Solving the Internet Jurisdiction Puzzle. Oxford University Press.

[16] Vujičić, J. (2024). Compliance Architecture for AI Regulation in Digital Health Startups. Journal of Legal Innovation & Technology, 5(1), 102–120.

[17] AI Now Institute. (2021). Confronting Black Boxes: A Shadow Report on the Algorithmic Accountability Act. https://ainowinstitute.org

[18] European Commission. (2021). Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act). https://digital-strategy.ec.europa.eu

[19] UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000380455

[20] Mozilla Foundation. (2021). Creating Trustworthy AI: A Roadmap for Industry and Government. https://foundation.mozilla.org

[21] AI Ethics Guidelines Global Inventory. (2023). AlgorithmWatch. https://algorithmwatch.org/en/project/ai-ethics-guidelines-global-inventory/

[22] Leslie, D. (2020). Understanding Artificial Intelligence Ethics and Safety. The Alan Turing Institute. https://www.turing.ac.uk

[23] Jobin, A., Ienca, M., & Vayena, E. (2019). The Global Landscape of AI Ethics Guidelines. Nature Machine Intelligence, 1(9), 389–399.

[24] Fjeld, J., Achten, N., Hilligoss, H., Nagy, A., & Srikumar, M. (2020). Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI. Berkman Klein Center Research Publication, (2020-1).

[25] Winfield, A. F., & Jirotka, M. (2018). Ethical Governance is Essential to Building Trust in Robotics and Artificial Intelligence Systems. Philosophical Transactions of the Royal Society A, 376(2133), 20180085.