

# INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary  
Peer Reviewed

[www.ijlra.com](http://www.ijlra.com)

## **DISCLAIMER**

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.  
All rights reserved.**

## ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

## ***PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT***

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

# **RECONCEPTUALISING JURISDICTION IN THE AGE OF AUTONOMOUS ARTIFICIAL INTELLIGENCE: A DOCTRINAL ANALYSIS OF TRANSNATIONAL LEGAL ACCOUNTABILITY**

AUTHORED BY - GREGORY KOSHY THOMAS  
INDEPENDENT ADVOCATE

## **Abstract**

The emergence of autonomous artificial intelligence (AI) systems operating across national boundaries presents a fundamental challenge to traditional doctrinal frameworks of jurisdiction and legal accountability. This paper undertakes a comprehensive doctrinal analysis of how transnational legal accountability mechanisms must be reconceptualised to address the unique challenges posed by autonomous AI systems that lack human agency, operate with opacity, and generate legal consequences across multiple jurisdictions. Drawing upon comparative analysis of the European Union, United States, and emerging governance models, this study examines the inadequacy of fault-based liability doctrines, the attribution problem in determining responsibility, and the jurisdictional gaps that permit autonomous systems to operate without meaningful accountability. The paper proposes a multi-layered governance framework integrating principles of functional control, risk-based regulation, strict liability for high-risk applications, and reciprocal jurisdictional recognition mechanisms. It concludes that effective transnational accountability requires abandoning state-centric jurisdictional assumptions and adopting an adaptive, system-oriented legal architecture capable of addressing the distributed nature of responsibility in AI ecosystems while preserving human dignity as the foundational norm.

**Keywords:** jurisdiction, artificial intelligence, autonomous systems, accountability, transnational law, doctrinal analysis, liability attribution, global governance

## 1. Introduction

The proliferation of autonomous artificial intelligence systems across national frontiers has fundamentally disrupted the conceptual foundations of traditional jurisdiction doctrine.<sup>1</sup> As AI systems increasingly operate with minimal human oversight, generating decisions with profound legal consequences—from autonomous weapons targeting civilians to algorithmic systems allocating financial credit and healthcare resources—legal systems designed around assumptions of human agency and predictable causality find themselves inadequate.<sup>2</sup> The core problem is multidimensional: autonomous systems operate across territorial boundaries while traditional jurisdiction remains territorially bounded; they function with algorithmic opacity while law requires transparency for accountability; they distribute responsibility across networks of developers, operators, and users while legal doctrine presumes identifiable individual agents.<sup>3</sup>

This doctrinal analysis addresses the "accountability gap"—the structural mismatch between the technical autonomy of AI systems and the legal frameworks designed to govern human actors.<sup>4</sup> The paper argues that jurisdiction in the AI era cannot remain confined to Westphalian conceptions of state sovereignty and territorial authority. Instead, a reconceptualization grounded in functional control, risk-differentiation, and transnational institutional coordination is necessary. Drawing upon doctrinal analysis of emerging regulatory frameworks, comparative jurisdictional approaches, and normative theory, this paper develops an integrated framework for transnational legal accountability capable of addressing the distributed, cross-border nature of AI governance.<sup>1</sup>

---

<sup>1</sup> The term "accountability gap" originated in weaponized AI literature addressing autonomous weapons systems. See [38]; [39]. It has since been extended to encompass broader challenges of attributing legal responsibility for autonomous systems across sectors. The gap reflects both technical dimensions—opacity preventing determination of system behavior causation—and doctrinal dimensions—traditional legal frameworks lacking concepts adequate to autonomous, distributed decision-making.

<sup>2</sup> The philosophical challenge is profound: if law cannot attribute responsibility to non-human agents, yet autonomous systems increasingly act without human direction, does law retain authority? Conservative responses insist on preservation of human agency as responsibility-bearer; progressive responses reconceptualise responsibility as distributed across organizations and technical-social networks. This paper adopts the latter approach as more adequate to contemporary technological conditions.

<sup>3</sup> Functional control doctrine draws parallels to agency law's concept of actual authority—one actor bears responsibility for another's conduct when it maintains substantial control over that person's actions. Extension to AI systems is not unprecedented but represents significant expansion from interpersonal to technological governance. See [14] discussing corporate accountability in transnational AI contexts.

<sup>4</sup> Global Administrative Law theory, articulated by Benedict Kingsbury and colleagues, emphasizes that contemporary governance challenges increasingly transcend territorial jurisdiction, requiring coordination mechanisms that cut across state boundaries while respecting state sovereignty. This framework has proven particularly fruitful for analysing AI governance fragmentation.

## 2. The Doctrinal Crisis: Traditional Accountability Frameworks and Autonomous Systems

### 2.1 Fault-Based Liability and the Collapse of Causation

Contemporary civil and criminal law doctrines rest upon foundational assumptions that are fundamentally incompatible with autonomous AI systems.<sup>5</sup> Traditional fault-based liability, grounded in Articles 1365–1367 of Continental civil codes and analogous common law principles of negligence, presumes that harm arises from identifiable human conduct, that causation flows linearly from actor to consequence, and that mens rea (mental culpability) attaches to individual perpetrators.<sup>6</sup> When an autonomous vehicle causes injury, when an algorithmic hiring system discriminates against protected classes, or when a trading algorithm manipulates financial markets, the linear causation chain fractures. The AI system acts without direct human instructions; multiple developers and operators contributed to its training, deployment, and parameters; the specific sequence of computational steps leading to harm remains opaque even to designers.

The Netherlands-based study examining civil liability for AI in the Vietnamese context revealed that traditional tort principles struggle to accommodate autonomous systems because causation cannot be established along simple human-agent-harm sequences.<sup>7</sup> Instead, harm emerges from the interaction between algorithmic training data, model architecture decisions, deployment contexts, and real-world contingencies—none of which align with doctrinal requirements for proving individual negligence. Nigerian jurisprudence, similarly structured around human-centered fault, lacks mechanisms to address harm arising from autonomous decision-making where no single actor can be proven negligent.<sup>8</sup> This doctrinal inadequacy is not merely technical; it reflects a philosophical crisis in law's ability to govern non-human

---

<sup>5</sup> Explainability requirements face significant technical challenges—some AI systems may be inherently difficult to explain without fundamentally altering their functionality. Legal doctrine must therefore establish reasonable standards for explainability rather than requiring perfect transparency. See [19] discussing these tensions in medical AI contexts.

<sup>6</sup> Criminal responsibility reconstruction represents the most controversial element of AI accountability innovation. Some scholars argue that preserving individual human agency as prerequisite for criminal liability protects fundamental principles of human dignity and due process. Others contend that this approach improperly privileges formal doctrinal commitments over substantive accountability for harm. This debate will define criminal law development over coming decades.

<sup>7</sup> The EU AI Act's extraterritorial scope—applying to actors targeting EU markets regardless of incorporation location—exemplifies market-access jurisdiction. It contrasts with traditional territorial jurisdiction but reflects recognition that conventional jurisdictional authority cannot effectively govern cross-border digital platforms. Extraterritoriality generates tensions with national sovereignty, particularly for jurisdictions uncomfortable with EU regulatory authority. See [1] analyzing these jurisdictional conflicts.

<sup>8</sup> The US tort law innovation discussed involves doctrinal flexibility—courts are gradually expanding traditional causation and foreseeability doctrine to accommodate algorithmic complexity without requiring legislative amendment. This evolutionary approach contrasts with the EU's preference for comprehensive statutory reform. Both approaches have merits; the US approach enables faster adaptation but risks unpredictability, while the EU approach provides certainty but may lag technological development.

agents.<sup>2</sup>

## 2.2 The Attribution Problem and Functional Responsibility

A second doctrinal fracture concerns attribution—determining which actors bear legal responsibility for autonomous system conduct.<sup>9</sup> In criminal law, the Rome Statute framework presumes that perpetrators, aiders and abettors, or commanders can be identified through analysis of human intent and control.<sup>10</sup> When autonomous weapons systems act independently, when their targeting algorithms operate unpredictably, or when system behavior emerges from training processes that no single designer intended, attribution mechanisms fail.<sup>11</sup> The Ukrainian Supreme Court's approach to state responsibility for armed aggression demonstrates how even international law—traditionally focused on state actors—recognizes the inadequacy of classical attribution doctrine when distributed, autonomous systems are implicated.<sup>12</sup>

This attribution problem extends across sectors. In Indonesian financial services, AI systems engaging in discrimination, fraud, or algorithmic manipulation operate without clear assignment of liability to any specific human actor.<sup>13</sup> The European Union's proposed approach through the AI Act attempts to resolve this through "functional control"—assigning responsibility to the actor with greatest capacity to foresee and prevent harmful outcomes.<sup>14</sup> However, this functional approach departs from classical doctrinal requirements of direct

---

<sup>9</sup> Functional control doctrine, while preserving doctrinal continuity, requires significant evidentiary reconstruction. Determining which actor maintained "sufficient" control over which dimensions of AI system behavior requires detailed technical and organizational investigation. Courts and regulators must develop expertise in algorithmic auditing to operationalize this principle effectively.

<sup>10</sup> Recognition-based coordination is not without critics. Some scholars worry that conditional procedural reliance insufficiently protects rights—allowing EU regulators to rely on Chinese safety determinations based on procedural adequacy standards might subordinate substantive rights protection to inter-jurisdictional comity. This tension between coordination and protection remains unresolved.

<sup>11</sup> Distributed responsibility creates challenges for victims seeking compensation—they must identify which actor bears liability in complex networks. Some jurisdictions address this through joint and several liability principles (any actor in the chain bears responsibility for full victim compensation) or through compensation funds established ex-ante to ensure victim access to remedy regardless of individual actor accountability. See [40] discussing Three-Tier Liability Frameworks.

<sup>12</sup> Precautionary governance shifts legal culture from remediation to prevention. This approach accords with environmental law principles and occupational safety doctrine but departs significantly from criminal law's preference for ex-post punishment. The tension between these approaches defines regulatory design choices—some systems prioritize innovation incentives through permissive ex-post liability; others prioritize harm prevention through stringent ex-ante requirements.

<sup>13</sup> Functional control doctrine requires careful specification of control dimensions. Manufacturers control system design and training; deployers control real-world deployment decisions and monitoring; data providers control training data quality; users influence outcomes through interaction patterns. Each commands different control dimensions, and responsibility cannot be accurately assigned through aggregate concepts like "ultimate responsibility."

<sup>14</sup> The due diligence framework, articulated through the UN Guiding Principles on Business and Human Rights and extended through international cyber law practice, has proven remarkably flexible in accommodating distributed responsibility across transnational networks. Its emphasis on processes rather than outcomes, and on systemic prevention rather than perpetrator punishment, aligns well with AI accountability requirements. See [41] examining state responsibility for human rights harms.

agency and introduces forward-looking risk management principles that traditional liability frameworks cannot easily accommodate. The result is not merely regulatory innovation but doctrinal transformation.<sup>3</sup>

### **2.3 Jurisdictional Fragmentation and the Multipolarity Problem**

A third doctrinal crisis concerns jurisdiction itself—the authority of particular legal systems to regulate conduct, allocate liability, and enforce remedies<sup>15</sup>. Traditional jurisdiction doctrine, refined through centuries of interstate conflict and codified in instruments like the Brussels Recast and Rome II Regulations, assumes that conduct occurs within identifiable territories and that conflicts of law arise between jurisdictions with competing but ultimately reconcilable interests. Autonomous AI systems shatter this assumption. A machine learning model trained in one jurisdiction, deployed through servers in a second, generating harm affecting persons in a third, with responsibility distributed across multiple actors across multiple borders cannot be neatly subjected to singular jurisdictional authority.

Moreover, regulatory divergence creates strategic incentives for "jurisdiction shopping"—platforms and developers selecting favorable legal regimes while externalities flow to other territories. The European Union's comprehensive AI Act, the United States' sectoral approach, and China's centralized control framework reflect fundamentally incompatible regulatory philosophies. This fragmentation generates what Global Administrative Law theory recognizes as a "coordination deficit"—multiple overlapping regulatory regimes lacking coherent mechanisms for ensuring consistency, preventing gaps, or distributing compliance burdens equitably.<sup>4</sup>

## **3. Autonomy, Opacity, and the Challenge to Legal Transparency**

### **3.1 Black Box Algorithms and Evidentiary Collapse**

The autonomy of contemporary AI systems introduces a distinctive legal pathology: algorithmic opacity fundamentally undermines the evidentiary foundations upon which law depends<sup>16</sup>. When traditional courts assess negligence, they examine the actor's knowledge, the

---

<sup>15</sup> Organizational responsibility for AI harms represents extension of corporate criminal liability doctrine. This approach holds organizations liable for systemic failures to establish preventive mechanisms, even when individual employees lack culpable intent. It has proven effective in occupational safety and environmental contexts. See [5] discussing Autonomous Criminal Cyber Defense Systems and organizational responsibility frameworks.

<sup>16</sup> Regional governance initiatives in ASEAN, African Union contexts, and other emerging institutional frameworks represent experiments in post-Westphalian governance. These initiatives remain limited in scope and institutional capacity compared to the EU or bilateral trade arrangements, but they exemplify the principle that transnational governance can emerge through regional coordination structures distinct from both national regulation and global harmonization efforts.

foreseeability of harm, and the reasonableness of precautions taken. These legal concepts presume that causation can be traced, that decision-making can be explained, that the relationship between action and consequence is intelligible to human judgment. Machine learning systems, particularly those employing deep neural networks, defeat this intelligibility requirement. The system produces outputs—decisions about creditworthiness, criminal risk assessment, medical diagnosis—through computational processes that resist human explanation.

This opacity has direct legal consequences. First, it prevents meaningful informed consent—patients, consumers, and citizens cannot understand how AI systems will affect them, making it impossible to satisfy legal requirements for transparency and autonomy.<sup>17</sup> Second, it undermines due process, preventing individuals subject to AI-mediated decisions from understanding the basis of those determinations or effectively challenging them. Third, it ruptures causal inference—the fundamental evidentiary process through which lawyers establish responsibility, courts assign liability, and remedies are calculated. As German and Chinese autonomous driving jurisprudence recognizes, the solution cannot be to eliminate the transparency requirement; rather, legal doctrine must evolve to embed explainability requirements as preconditions for lawful AI deployment, shifting from ex-post enforcement (after harm occurs) to ex-ante governance (before deployment).<sup>5</sup>

### 3.2 The Responsibility Gap in Complex Networks

Beyond opacity, autonomy creates a "responsibility gap" through the distribution of control and knowledge across networks of actors.<sup>18</sup> Consider a cross-border autonomous weapons system: strategic decisions are made by military command in one state; the software is developed by private contractors in multiple jurisdictions; the training data originates from diverse sources; the deployment platform operates across territorial boundaries; and the actual targeting decision emerges from algorithmic processing governed by parameters set through decisions distributed across multiple actors and agencies. Traditional doctrines assign liability

---

<sup>17</sup> Market-access restrictions, while effective, risk generating institutional closure and reducing beneficial innovation in restricted jurisdictions. Striking appropriate balance between stringent compliance requirements and innovation incentives remains among the most challenging policy questions. The EU AI Act's risk-based approach—permitting low-risk innovation with minimal requirements while restricting high-risk applications—exemplifies an attempt to navigate this balance, though critics worry it remains insufficiently precautionary in some domains and excessively restrictive in others.

<sup>18</sup> Post-Westphalian accountability architecture reflects the recognition that contemporary governance challenges exceed the capacity of territorial states operating through traditional hierarchical authority. Instead, governance emerges through overlapping networks of institutional authority—supranational bodies (EU institutions), multinational markets (World Trade Organization), technical standards bodies (ISO), professional communities (medical associations), and civil society organizations. This fragmented authority structure creates both opportunities (enabling experimentation and learning) and risks (creating gaps and inconsistencies in protection).

to the "most culpable" actor—but culpability doctrine presumes individual agency and knowledge, which dissolves in networks of distributed decision-making.

Indonesian criminal law's response, refusing to recognize AI systems as independent criminal subjects while directing liability toward programmers, manufacturers, users, or corporations based on "functional control," represents an attempt to preserve the actor-based structure of criminal responsibility despite autonomy. However, this approach, while doctrinally conservative, requires identifying which actor exercised sufficient functional control—a determination that itself requires reconstructing the distributed network of technical and organizational decisions. The alternative is to reconceptualize criminal responsibility not as requiring individual agency but as distributed across organizational infrastructure, requiring each actor to implement preventive structures, auditability mechanisms, and human oversight protocols. This represents not merely regulatory innovation but a fundamental doctrinal shift in how criminal law attributes responsibility.<sup>6</sup>

## **4. Transnational Legal Accountability Mechanisms**

### **4.1 Recognition-Based Coordination and Regulatory Interoperability**

Rather than pursuing harmonization—the impossibly ambitious goal of aligning all jurisdictions' AI standards—emerging scholarship advocates "recognition-based coordination". This mechanism enables states to give cross-border effect to foreign regulatory determinations when underlying processes meet transparency, accountability, and procedural legitimacy standards. A safety evaluation conducted by EU authorities could be recognized in Singapore if processes are intelligible and subject to meaningful review. This approach acknowledges regulatory diversity as permanent while creating coordination structures enabling information sharing, cross-border reliance, and mutual learning.

Recognition mechanisms require institutional infrastructure: international standards bodies (ISO committees, CEN/CENELEC working groups) establishing technical baselines; multilateral platforms (OECD AI Principles, UNESCO recommendations) articulating shared normative commitments; and reciprocal information-sharing mechanisms enabling regulators to assess whether foreign processes meet adequacy standards. The nascent Global Administrative AI Governance Framework (GAIGF) attempts to operationalize these principles through layered coordination—national regulation grounded in domestic mandates, regional harmonization through mutual recognition agreements, and international soft-law coordination establishing aspirational norms and information-sharing protocols.<sup>10</sup>

## 5.2 Attribution Frameworks and Distributed Responsibility

A second mechanism involves reconstructing attribution doctrine to accommodate distributed responsibility networks. Rather than requiring identification of single culpable actors, this approach recognizes that responsibility for AI systems is inherently distributed across development organizations, deploying entities, regulatory overseers, and data providers. The European Union's AI Act operationalizes this through "role-based responsibility"—providers have obligations regarding transparency and bias testing; deployers have obligations regarding human oversight and monitoring; affected persons retain rights to contestation and remedy regardless of which actor ultimately bears liability.

This distributed responsibility model represents doctrinal innovation by recognizing that legal accountability need not require assigning all responsibility to single actors. Instead, each actor in the AI development and deployment ecosystem bears specific obligations aligned with their functional position. Developers must implement algorithmic governance, maintain training data quality, conduct impact assessments; deployers must monitor real-world performance, implement human override mechanisms, maintain audit trails; regulators must review systemic risks and enforce compliance; affected persons maintain rights to explanation and contestation. Together, these distributed obligations create accountability infrastructure that no single actor could provide.<sup>11</sup>

## 6. The Attribution Problem: From Individual Agency to Systemic Accountability

### 6.1 The Functional Control Doctrine

Central to transnational AI accountability is the concept of "functional control"—responsibility attaches to actors capable of controlling relevant system behavior [9]. This principle departs from classical criminal law's requirement that perpetrators exercise direct physical control over harmful conduct, and from tort doctrine's assumption that defendants consciously chose actions causing harm. Instead, functional control focuses on capacity to foresee, prevent, and mitigate harm through structural, procedural, and technological mechanisms.

The German autonomous driving jurisprudence illustrates this approach concretely: manufacturers bear responsibility for vehicle behavior not because they directly control specific instances but because they maintain authority over system design, training, and deployment parameters; drivers retain residual responsibility for monitoring and override capabilities; insurers bear financial responsibility for harms within coverage parameters. This

distributed assignment reflects the actual distribution of meaningful control—no single actor commands all relevant decisional authority, yet each commands sufficient control to influence outcomes. Doctrinal innovation consists in recognizing that responsibility can be distributed without collapsing into attributive chaos.<sup>13</sup>

## **6.2 The Cybersecurity Analogy: From Attribution to Responsibility Reconstruction**

International cyber law, examined in the Tallinn Manual framework, offers instructive parallels. When state or non-state actors conduct cyberattacks causing harm, traditional responsibility doctrine initially faltered: complex attribution chains obscured perpetrators; multiple actors (software developers, platform hosts, network operators) contributed to capability; sovereignty implications complicated enforcement. Over time, practice evolved toward emphasizing "due diligence" obligations—states must implement cybersecurity standards, monitor critical infrastructure vulnerabilities, prosecute persons operating from their territory, and cooperate internationally in attribution and remediation.

This due diligence approach resonates with AI accountability reconstruction: rather than requiring perfect attribution of responsibility to perpetrators, it emphasizes systemic obligations of state and non-state actors to implement preventive structures, maintain transparency, enable investigation, and cooperate internationally. Autonomous AI systems created by Chinese developers deployed on American platforms processing European data affecting Indian citizens exemplify this complexity—traditional jurisdiction doctrine cannot assign exclusive authority to any single state, yet all states have legitimate interest in protecting their citizens. The solution is not Winner-Take-All jurisdiction but layered due diligence obligations distributed across actors and jurisdictions.<sup>14</sup>

## **7. Toward an Integrated Framework: Principles and Implementation**

### **7.1 Core Principles for Transnational AI Accountability**

Drawing on comparative analysis and doctrinal reconstruction, an integrated framework for transnational legal accountability in the AI era should be grounded in six interrelated principles: First, functional control prioritizes responsibility assignment based on actual capacity to govern system behavior, rather than traditional categories of perpetrator, aider-and-abettor, or commander.<sup>16</sup> This principle accommodates distributed decision-making by recognizing that responsibility can attach to multiple actors each commanding different dimensions of control. Second, transparency and explainability requirements make it impossible for actors to defend algorithmic systems deployed to affect human interests without providing intelligible

explanations of decision-making processes. This principle reflects the normative judgment that law cannot permit autonomous systems affecting fundamental rights to remain opaque, and that technical opacity cannot shield actors from accountability.<sup>19</sup>

Third, risk differentiation establishes that legal obligations scale with system risk—high-risk applications require stricter ex-ante governance, impact assessment, and human oversight than low-risk systems. This principle operationalizes precautionary logic while avoiding regulatory overreach that would chill beneficial innovation in low-risk AI applications.

Fourth, reciprocal jurisdictional recognition enables coordination among diverse regulatory regimes through conditional procedural reliance—states give effect to foreign regulatory determinations when underlying processes meet transparency and accountability standards.<sup>17</sup> This principle acknowledges that regulatory diversity is permanent while creating coordination structures enabling information sharing and cross-border consistency.

Fifth, victim-centered remedies ensure that affected persons maintain meaningful access to explanation, contestation, and compensation regardless of which actor bears ultimate responsibility. This principle reflects the normative judgment that legal systems must center protection of affected persons rather than actor accountability, with remedies available through multiple pathways (administrative, civil, criminal).

Sixth, international institutional coordination through multilateral bodies, professional communities, and technological standards enables transnational governance despite jurisdictional fragmentation. This principle recognizes that no single jurisdiction commands sufficient authority to regulate global AI systems; instead, coordination must emerge through overlapping institutional networks maintaining information exchange and norm development.<sup>18</sup>

## **8. Implementation Challenges and Transitional Mechanisms**

### **8.1 Resistance from Regulatory Arbitrage and Competitive Federalism**

Implementation of transnational accountability frameworks encounters systematic resistance from actors pursuing "regulatory arbitrage"—strategically locating operations in favorable jurisdictions to minimize compliance obligations while externalizing harms to less-regulated territories.<sup>20</sup> This dynamic, well-documented in financial regulation and intellectual property

---

<sup>19</sup> Regional governance initiatives in ASEAN, African Union contexts, and other emerging institutional frameworks represent experiments in post-Westphalian governance. These initiatives remain limited in scope and institutional capacity compared to the EU or bilateral trade arrangements, but they exemplify the principle that transnational governance can emerge through regional coordination structures distinct from both national regulation and global harmonization efforts.

<sup>20</sup> Platform accountability represents a critical governance frontier. Social media networks, search engines, and cloud providers wield enormous influence over which AI systems are deployed, how they operate, and how harms are

enforcement, virtually guarantees that voluntary coordination will prove inadequate. Jurisdictions offering light-touch regulation attract AI development and deployment, generating network effects that concentrate capability in permissive regimes while constraining innovation in stringent jurisdictions.

Addressing this requires mechanisms that increase non-compliance costs: mutual legal assistance treaties requiring states to prosecute persons violating foreign AI regulations when operating from their territory; asset seizure authority enabling victims to recover compensation from defendant assets located in third jurisdictions; and market-access restrictions preventing companies failing to meet baseline standards from accessing major markets. The EU's approach—threatening market-access denial for non-compliant actors regardless of incorporation location—provides a model, though one dependent on the market power of sufficiently large jurisdictions.<sup>21</sup>

## 8.2 Institutional Capacity Constraints in Emerging Jurisdictions

A second challenge involves systematic capacity disparities. Wealthy jurisdictions with advanced legal systems, substantial regulatory budgets, and sophisticated technical expertise can establish comprehensive AI governance frameworks. Emerging jurisdictions face severe capacity constraints—limited budgets for regulatory staff, insufficient expertise in evaluating algorithmic systems, inadequate legal education incorporating AI governance, and competing priorities across broader development challenges. This disparity threatens to create a two-tier system: strict governance in wealthy jurisdictions, minimal oversight in emerging markets, with predictable flows of risky AI systems toward weakly regulated territories.

Addressing this requires capacity-building initiatives: technical assistance enabling emerging jurisdictions to establish regulatory frameworks and train personnel; technology transfer arrangements enabling developing countries to access tools for algorithmic auditing; and financial mechanisms enabling emerging jurisdictions to participate in international governance structures without bearing disproportionate costs.

## 9. Conclusion: Toward a Post-Westphalian Accountability Architecture

The emergence of autonomous artificial intelligence systems demands fundamental reconceptualization of jurisdiction and legal accountability doctrine. Traditional frameworks,

---

addressed. Yet platform governance remains largely unaccountable to public oversight and democratic processes. Extending accountability obligations to platforms represents necessary extension of governance authority into private digital infrastructure.

grounded in assumptions of human agency, territorial authority, and identifiable perpetrators, cannot accommodate autonomous systems operating across borders with distributed responsibility. The answer is not to intensify jurisdictional assertions—claiming exclusive authority over actors or conduct located elsewhere—but to develop transnational accountability mechanisms grounded in functional control, institutional coordination, and victim-centered remedies.

This doctrinal transformation moves law beyond Westphalian assumptions toward what might be termed "post-Westphalian accountability"—governance grounded not in territorial sovereignty but in functional distribution of control, institutional capacity, and remedial access. Rather than asking "which state has jurisdiction?" the framework asks "what actors command what dimensions of control over this AI system?" and "what obligations follow from each actor's functional position?" Recognition-based coordination replaces harmonization as the dominant coordination mechanism; risk-based regulation replaces comprehensive prohibition or laissez-faire tolerance; distributed responsibility replaces single-actor liability.<sup>23</sup>

These transformations are not merely technical adaptations to technological change. They represent a deeper reconceptualization of what accountability means in complex, autonomous, transnational systems. They reflect the normative judgment that law cannot abandon affected persons to algorithmic opacity and distributed irresponsibility—that human dignity, informed consent, and access to remedy remain fundamental legal commitments even as the technologies enabling harm become increasingly autonomous and opaque. The integration of these principles into comprehensive legal frameworks, coupled with institutional development enabling their operationalization across jurisdictions and sectors, represents the essential agenda for legal scholarship and reform in the coming decades.<sup>24</sup>

## Footnotes

1. The term "accountability gap" originated in weaponized AI literature addressing autonomous weapons systems. See [38]; [39]. It has since been extended to encompass broader challenges of attributing legal responsibility for autonomous systems across sectors. The gap reflects both technical dimensions—opacity preventing determination of system behavior causation—and doctrinal dimensions—traditional legal frameworks lacking concepts adequate to autonomous, distributed decision-making.

2. The philosophical challenge is profound: if law cannot attribute responsibility to non-human agents, yet autonomous systems increasingly act without human direction, does law retain authority? Conservative responses insist on preservation of human agency as responsibility-bearer; progressive responses reconceptualize responsibility as distributed across organizations and technical-social networks.
3. Functional control doctrine draws parallels to agency law's concept of actual authority—one actor bears responsibility for another's conduct when it maintains substantial control over that person's actions. Extension to AI systems is not unprecedented but represents significant expansion from interpersonal to technological governance. See [14] discussing corporate accountability in transnational AI contexts.
4. Global Administrative Law theory, articulated by Benedict Kingsbury and colleagues, emphasizes that contemporary governance challenges increasingly transcend territorial jurisdiction, requiring coordination mechanisms that cut across state boundaries while respecting state sovereignty. This framework has proven particularly fruitful for analyzing AI governance fragmentation. See [18].
5. Explainability requirements face significant technical challenges—some AI systems may be inherently difficult to explain without fundamentally altering their functionality. Legal doctrine must therefore establish reasonable standards for explainability rather than requiring perfect transparency. See [19] discussing these tensions in medical AI contexts.
6. Criminal responsibility reconstruction represents the most controversial element of AI accountability innovation. Some scholars argue that preserving individual human agency as prerequisite for criminal liability protects fundamental principles of human dignity and due process. Others contend that this approach improperly privileges formal doctrinal commitments over substantive accountability for harm. This debate will define criminal law development over coming decades.
7. The EU AI Act's extraterritorial scope—applying to actors targeting EU markets regardless of incorporation location—exemplifies market-access jurisdiction. It contrasts with traditional territorial jurisdiction but reflects recognition that conventional jurisdictional authority cannot effectively govern cross-border digital platforms. Extraterritoriality generates tensions with national sovereignty, particularly for jurisdictions uncomfortable with EU regulatory authority. See [1] analyzing these jurisdictional conflicts.

8. The US tort law innovation discussed involves doctrinal flexibility—courts are gradually expanding traditional causation and foreseeability doctrine to accommodate algorithmic complexity without requiring legislative amendment. This evolutionary approach contrasts with the EU's preference for comprehensive statutory reform. Both approaches have merits; the US approach enables faster adaptation but risks unpredictability, while the EU approach provides certainty but may lag technological development.
9. Functional control doctrine, while preserving doctrinal continuity, requires significant evidentiary reconstruction. Determining which actor maintained "sufficient" control over which dimensions of AI system behavior requires detailed technical and organizational investigation. Courts and regulators must develop expertise in algorithmic auditing to operationalize this principle effectively.
10. Recognition-based coordination is not without critics. Some scholars worry that conditional procedural reliance insufficiently protects rights—allowing EU regulators to rely on Chinese safety determinations based on procedural adequacy standards might subordinate substantive rights protection to inter-jurisdictional comity. This tension between coordination and protection remains unresolved.
11. Distributed responsibility creates challenges for victims seeking compensation—they must identify which actor bears liability in complex networks. Some jurisdictions address this through joint and several liability principles (any actor in the chain bears responsibility for full victim compensation) or through compensation funds established ex-ante to ensure victim access to remedy regardless of individual actor accountability. See [40] discussing Three-Tier Liability Frameworks.
12. Precautionary governance shifts legal culture from remediation to prevention. This approach accords with environmental law principles and occupational safety doctrine but departs significantly from criminal law's preference for ex-post punishment. The tension between these approaches defines regulatory design choices—some systems prioritize innovation incentives through permissive ex-post liability; others prioritize harm prevention through stringent ex-ante requirements.
13. Functional control doctrine requires careful specification of control dimensions. Manufacturers control system design and training; deployers control real-world deployment decisions and monitoring; data providers control training data quality; users influence outcomes through interaction patterns. Each commands different

control dimensions, and responsibility cannot be accurately assigned through aggregate concepts like "ultimate responsibility."

14. The due diligence framework, articulated through the UN Guiding Principles on Business and Human Rights and extended through international cyber law practice, has proven remarkably flexible in accommodating distributed responsibility across transnational networks. Its emphasis on processes rather than outcomes, and on systemic prevention rather than perpetrator punishment, aligns well with AI accountability requirements. See [41] examining state responsibility for human rights harms.
15. Organizational responsibility for AI harms represents extension of corporate criminal liability doctrine. This approach holds organizations liable for systemic failures to establish preventive mechanisms, even when individual employees lack culpable intent. It has proven effective in occupational safety and environmental contexts. See [5] discussing Autonomous Criminal Cyber Defense Systems and organizational responsibility frameworks.
16. Functional control doctrine operationalizes the principle that responsibility should follow capacity. Actors with greatest capacity to foresee and prevent harmful outcomes bear primary responsibility; actors with more limited control bear residual responsibility. This principle aligns with economic efficiency analysis (concentrating responsibility on "cheapest cost avoiders") and with rights protection (ensuring accountability reaches actors capable of mitigating harm).
17. Recognition-based coordination operationalizes the principle that perfect harmonization is neither achievable nor necessary for transnational governance. Instead, jurisdictions can coordinate through conditional reliance—accepting that regulatory diversity reflects legitimate differences in governance philosophies and policy priorities, while establishing procedural standards ensuring that diversity does not create unmanageable fragmentation or unacceptable rights protection gaps.
18. International institutional coordination through overlapping networks—standards bodies, professional communities, information-sharing platforms—creates governance infrastructure not centered in any single institutional locus. This "network governance" approach contrasts with both state-centric governance (assuming states monopolize legitimate authority) and market-based governance (assuming private ordering produces optimal outcomes). It reflects recognition that contemporary challenges require coordination across multiple institutional forms.

19. Regional governance initiatives in ASEAN, African Union contexts, and other emerging institutional frameworks represent experiments in post-Westphalian governance. These initiatives remain limited in scope and institutional capacity compared to the EU or bilateral trade arrangements, but they exemplify the principle that transnational governance can emerge through regional coordination structures distinct from both national regulation and global harmonization efforts.
20. Platform accountability represents a critical governance frontier. Social media networks, search engines, and cloud providers wield enormous influence over which AI systems are deployed, how they operate, and how harms are addressed. Yet platform governance remains largely unaccountable to public oversight and democratic processes. Extending accountability obligations to platforms represents necessary extension of governance authority into private digital infrastructure.
21. Market-access restrictions, while effective, risk generating institutional closure and reducing beneficial innovation in restricted jurisdictions. Striking appropriate balance between stringent compliance requirements and innovation incentives remains among the most challenging policy questions. The EU AI Act's risk-based approach—permitting low-risk innovation with minimal requirements while restricting high-risk applications—exemplifies an attempt to navigate this balance, though critics worry it remains insufficiently precautionary in some domains and excessively restrictive in others.
22. The possibility of achieving genuine harmonization seems remote. Fundamental differences in governance philosophy—between EU rights protection emphasis, US innovation emphasis, and Chinese state control emphasis—reflect deep commitments unlikely to converge through negotiation. Transnational governance must therefore accommodate persistent divergence through mechanisms enabling coordination despite incompatibility.
23. Post-Westphalian accountability architecture reflects the recognition that contemporary governance challenges exceed the capacity of territorial states operating through traditional hierarchical authority. Instead, governance emerges through overlapping networks of institutional authority—supranational bodies (EU institutions), multinational markets (World Trade Organization), technical standards bodies (ISO), professional communities (medical associations), and civil society organizations. This fragmented authority structure creates both opportunities (enabling experimentation and learning) and risks (creating gaps and inconsistencies in protection).

24. The fundamental normative commitment animating this analysis is preservation of human dignity and meaningful human agency in a technological era. As autonomous systems increasingly mediate human decisions and affect human rights, legal systems must ensure that autonomy does not translate to unaccountability, that technological sophistication does not excuse legal oversight, and that affected persons maintain meaningful access to explanation, contestation, and remedy. This commitment, grounded in international human rights law and philosophical tradition, provides the normative foundation for reconceptualizing jurisdiction and accountability in the age of autonomous artificial intelligence.

