Fountain University Law Journal Vol. 2 No. 4, 2025

JURISDICTION LIABILITY MODELLING FOR AI- DRIVEN TRADE SECRET MISAPPROPRIATION IN CROSS-BORDER POLICY INTEGRATION UNDER ISLAMIC LAW

By

Ayuba Abdulrasaq Jabaje Ph.D

Abstract

The rapid advancement of Artificial Intelligence (AI) in global commerce has created unprecedented opportunities and risks. Among the most pressing challenges is the misappropriation of trade secrets facilitated by AI systems operating across borders. Traditional legal frameworks struggle to allocate liability when machine learning algorithms extract, generate, or misuse confidential business information. This seminar explores jurisdiction liability modelling for AI-driven trade secret misappropriation in the context of cross-border policy integration, with an added emphasis on compliance with Islamic legal principles. The research proposes a hybrid framework that integrates conventional legal doctrines, international instruments, and the maqāṣid al-sharīʿa (higher objectives of Islamic law) to ensure fairness, accountability, and justice in global digital markets.

Keywords: **Trade Secrecy, Artificial Intelligence, Cross Border Policy, International Instruments, and the Maqāṣid al-Sharīʿa**

1.0 INTRODUCTION

AI technologies are transforming every sector healthcare, finance, manufacturing, and defense. Yet, their application in data analysis often intersects with trade secret law. A trade secret is confidential business information that derives economic value from its secrecy. When AI extracts such information, intentionally or inadvertently, it can trigger misappropriation claims. However, determining jurisdiction and liability in such cases is fraught with difficulties, especially when the AI system is deployed across multiple jurisdictions.[1]

Islamic law (*al-sharīʿa*) provides ethical and legal tools for addressing such dilemmas. The Qur'anic injunction against betrayal of trust (amāna) and the prohibition of unjust enrichment underpin a system of fairness that aligns with modern legal concerns about trade secret protection. This seminar will develop a jurisdictional liability model that draws upon both secular international law and Islamic jurisprudence to address AI-driven trade secret misappropriation.

Lecturer, Islamic Law Department, Al-Hikmah University, Ilorin, Kwara State

[1] Pooley, James. *Trade Secrets: A Practitioner"s Guide*. Law Journal Press, 2021.

2.0 LITERATURE REVIEW

2.1 Trade Secret Misappropriation in the AI Age

Classical trade secret law was not designed to address situations where autonomous AI systems harvest, synthesize, and redistribute data. The *mens rea* (intent) requirement becomes blurred when an algorithm operates without explicit instruction to steal but nonetheless reconstructs proprietary information. In U.S. law, misappropriation involves acquisition by improper means, disclosure without consent, or use of a trade secret. But does algorithmic inference count as improper means‖? Scholars are divided.[2]

The European Union has moved toward harmonization, yet its directive still assumes human agency. Similarly, the TRIPS Agreement obligates member states to protect undisclosed information, but does not account for autonomous computational misappropriation. The lack of clarity has created loopholes exploited by corporations operating transnationally.

2.2 Islamic Legal Perspectives

Under Islamic jurisprudence, information (*maʿlūmāt*) may constitute a protectable asset (*māl*) if it carries utility and economic value. Unauthorized acquisition is considered *ghasb* (usurpation) or *khiyāna* (betrayal of trust), both condemned by the Qur'an and Sunnah. Importantly, liability in Islamic law may attach to both direct and indirect actors, which provides a flexible model for AI-related misconduct: if an AI tool acts under a person's control, the controller remains accountable under the doctrine of *tasabbub* (causation).[3]

2.3 Need for Cross-Border Policy Integration

Globalization and cloud-based AI services mean that trade secret misappropriation often occurs in one country, with harm felt in another, and servers located in yet another. Without cross border policy integration, jurisdictional fragmentation leads to inconsistent remedies. The inclusion of Islamic principles in international frameworks would enrich the discourse with ethical depth, especially in Muslim-majority jurisdictions.

2.2 AI's Unique Capabilities and Trade Secret Risk

Artificial Intelligence today is not merely a passive analytical tool; it has become an active participant in the creation, discovery, and reconstruction of information. With advanced deep learning and reinforcement learning algorithms, AI can detect relationships in datasets that were never explicitly revealed. This becomes problematic when the dataset is partially composed of

[2] TRIPS Agreement, Part II, Section 7, Article 39.
[3] Qur'an 2:188 — *"Do not consume one another"s wealth unjustly or send it [in bribery] to the rulers…"*

public information and partially of sensitive, proprietary information. Through inductive reasoning, AI can reconstruct the proprietary portion with remarkable accuracy, even if the original trade secret database was never directly accessed. Such capability raises a fundamental legal question: can a party be held liable for misappropriation when the AI system, without human intervention at that specific moment, discovers the trade secret? In classical legal doctrine, misappropriation typically requires the act of acquiring by improper means‖ or ―using without consent.[4] But the AI case blurs the lines was the acquisition improper, or was it simply a byproduct of sophisticated computation?

2.3 Gaps in Existing Legal Frameworks

The Uniform Trade Secrets Act (UTSA) in the United States defines ―improper means‖ to include theft, bribery, misrepresentation, breach of a duty to maintain secrecy, or espionage. However, it does not explicitly include algorithmic derivation. Similarly, the EU Trade Secrets Directive recognizes the need to protect against unauthorized use or disclosure but assumes human actors are the agents of harm. Internationally, the TRIPS Agreement (Article 39) requires protection of undisclosed information but leaves implementation details to national laws. This decentralized approach results in significant divergence.[5] When trade secrets are reconstructed by AI in one country and commercially exploited in another, courts must decide which jurisdiction's law applies and whether the AI operator can be held accountable. Current private international law rules, such as the place of harm‖ principle or
place of act‖ principle, often lead to forum-shopping, where parties select favorable jurisdictions to litigate or avoid liability.

3.0 ISLAMIC JURISPRUDENCE AND INFORMATION PROTECTION

In Islamic law, valuable intangible information qualifies as *māl* (property) if it has lawful benefit and is recognized as having economic worth. Misappropriation of such property is considered either *ghasb* (usurpation) or *khiyāna* (betrayal of trust). Both concepts apply whether the act was direct or indirect, intentional or negligent, provided harm occurred. This doctrinal flexibility makes Islamic law capable of addressing AI-related cases without requiring the AI itself to be treated as a legal person.[6]

Furthermore, Islamic law emphasizes the principle of *al-ḍarar yuzāl* harm must be removed which obligates legal systems to prevent or undo harm caused by wrongful acts, even when the wrongful act occurs through novel mechanisms such as autonomous algorithms. The *tasabbub* doctrine (causation by indirect means) assigns liability to individuals or entities whose tools cause harm, whether or not the harm was directly intended. This aligns with modern vicarious liability principles but is grounded in moral accountability.[7]

[4] Al-Dawoody, Ahmed. *The Islamic Law of War and Peace*. Palgrave Macmillan, 2011.
[5] Kamali, Mohammad Hashim. *Principles of Islamic Jurisprudence*. Islamic Texts Society, 2003.
[6] Uniform Trade Secrets Act, §1(2) (1985).
[7] Regulation (EU) 2016/943, Art. 4.

4.0 CROSS-BORDER ENFORCEMENT CHALLENGES

One of the greatest obstacles to enforcing trade secret protections in the AI age is that the harm can be global and instantaneous. An AI model trained in one jurisdiction can be deployed through cloud servers to users worldwide. If misappropriation occurs, the trade secret may be irretrievably exposed across hundreds of jurisdictions before legal proceedings can even begin. Unlike patents or trademarks, trade secret protection is lost once the information becomes public, meaning that speed of enforcement is critical.

Islamic law's emphasis on early intervention to prevent harm (*sadd al-dharāʾiʿ*, blocking the means to harm‖) supports preventive measures such as injunctions or access restrictions before misappropriation occurs. This principle could be incorporated into cross-border AI governance agreements to allow emergency action, even across jurisdictions with different legal traditions.

AI's unique ability to infer sensitive data challenges the existing trade secret framework. Current laws lack explicit provisions for algorithmic derivation, and jurisdictional fragmentation allows offenders to exploit legal loopholes. Islamic legal principles offer adaptable doctrines that can fill these gaps, especially through *tasabbub* liability, the *māl* classification of information, and harm-prevention maxims. However, operationalizing these principles in cross-border contexts will require coordinated policy design and mutual recognition between secular and Islamic legal systems.

5.0 JURISDICTIONAL LIABILITY MODELLING CORE CONCEPTS

5.1 Defining Jurisdiction in AI Contexts

Jurisdiction traditionally refers to a court's authority to hear a case, divided into *territorial jurisdiction* (where acts occur), *personal jurisdiction* (over specific defendants), and *subject-matter jurisdiction* (over the type of case). The challenge is identifying the place of the wrongful act. In traditional tort conflicts, courts often apply either:

i. **Lex loci delicti** — the law of the place where the wrongful act occurred, or
ii. **Lex loci damni** — the law of the place where the harm occurred.

AI cases may trigger multiple loci, which creates overlapping jurisdictional claims. Attribution of Acts to AI Controllers In both secular and Islamic legal frameworks, liability depends on attribution proving that the harmful act can be traced to a responsible party. In secular law, attribution in automated systems often follows the chain of control and foreseeability: Was the harm reasonably foreseeable, and did the defendant have control over the system? In Islamic law, this aligns with the doctrine of *tasabbub* (indirect causation), where someone who uses a tool that causes harm remains liable if they could anticipate the harm.

5.2 Negligence and Intent

Secular systems often distinguish between negligence and intentional wrongdoing. Similarly, Islamic law differentiates between *ʿamd* (intentional acts) and *khaṭaʾ* (mistakes). This matters in liability modelling, as the penalties, restitution, and procedural rules vary. For instance, under

Islamic law, intentional misappropriation of valuable property is more severely punished than negligence, though both require restitution.[8]

5.3 Multi-Tiered Jurisdictional Model Proposal

A robust jurisdictional liability model for AI-driven trade secret misappropriation could operate in three tiers:

1. **Primary Jurisdiction** — where the harm is materially felt (place of the trade secret holder's economic loss).
2. **Secondary Jurisdiction** — where the AI system physically operates or is hosted.
3. **Tertiary Jurisdiction** — where the controller/developer is domiciled.

This layered approach ensures no ―safe harbor‖ for actors seeking to evade liability by exploiting jurisdictional gaps.

5.4 Joint Liability in Cross-Border Cases

Islamic law has long recognized *tadāmun* (joint liability) for cases where multiple actors contribute to harm. In AI contexts, this can mean developers, deployers, and end-users may all share responsibility depending on their role in the chain of causation.

5.5 Integration with Private International Law

While Islamic law provides substantive liability rules, private international law governs conflict of laws — deciding which country's law applies. The model proposed here suggests mutual recognition treaties between jurisdictions (including Islamic states) to honor judgments in AI misappropriation cases, subject to compatibility with *maqāṣid al-sharīʿa* (objectives of Islamic law).

6.0 Challenges in Cross-Border Enforcement

6.1 Inclusion of Islamic Law States

OIC member states differ widely in their integration of trade secret protections. Some, like the UAE, have enacted modern IP laws aligned with TRIPS while still invoking *sharīʿa* principles for certain disputes. Others rely mainly on *fiqh* without detailed statutory codification. For effective integration, agreements must:

1. Recognize judgments reciprocally between secular and Islamic law jurisdictions.
2. Allow the use of *fiqh*-based reasoning alongside statutory norms.
3. Include preventive injunction provisions consistent with *maqāṣid al-sharīʿa*.

[8] Al-Dawoody, Ahmed. *The Islamic Law of War and Peace*. Palgrave Macmillan, 2011.

6.2 Proposed Cross-Border Integration Model
A model treaty could incorporate:

- Uniform definitions for AI-related trade secret misappropriation.
- Minimum standards for damages and injunctions.
- Provisions for urgent ex parte relief in cross-border settings.
- Compatibility clauses ensuring enforcement aligns with each state's public policy and religious norms.

Islamic Law Perspective on AI Trade Secret Misappropriation
Foundations in Qur'an and Sunnah
Islamic law treats protection of property as a fundamental objective (*ḥifẓ al-māl*) within the maqāṣid al-sharīʿa. The Qur'an condemns unjust acquisition of wealth (2:188) and betrayal of trusts (4:58). The Sunnah reinforces these principles; the Prophet Muhammad ﷺ said: *"The property of a Muslim is not lawful to another except by his consent"* (Hadith, Ahmad). These texts apply equally to tangible and intangible property when it holds recognized value.

7.0 THE TASABBUB DOCTRINE AND AI LIABILITY

The Islamic legal doctrine of *tasabbub* liability for causation through indirect means provides a powerful analytical tool for addressing AI-driven trade secret misappropriation in cross-border contexts. In classical *fiqh*, *tasabbub* applies when a person sets in motion a chain of events that foreseeably causes harm, even if they do not commit the harmful act directly. This doctrine evolved in scenarios such as leaving a pit uncovered in a public path, leading to someone's injury. While the AI misappropriation problem appears novel, the underlying moral and legal logic remains the same: the harm results from the defendant's acts or omissions, even if mediated by an autonomous process.

7.1 Applying Tasabbub to AI Systems

In an AI context, the *musabbib* (indirect cause) could be:

- A developer who designs an AI model capable of reconstructing proprietary information.
- A data scientist who feeds the model with datasets containing sensitive patterns.
- A platform provider who knowingly deploys the model without safeguards.

All these actors could be liable if their conduct foreseeably results in trade secret misappropriation, regardless of whether the AI acted ―autonomously‖ at the moment of harm. Islamic law distinguishes between *direct cause* (*mubāshir*) and *indirect cause* (*tasabbub*), assigning liability differently based on foreseeability, negligence, and control. In AI misappropriation, the foreseeability threshold is critical — the more sophisticated the actor, the higher the expectation that they anticipate the potential misuse of their tools.

7.2 Foreseeability in AI Misappropriation Cases

The foreseeability analysis under *tasabbub* closely resembles the ―reasonable foreseeability‖ test in common law negligence. However, Islamic jurisprudence adds an ethical dimension: the actor is morally accountable if they failed to prevent harm when they had the knowledge and means to do so, even if their jurisdiction did not legally prohibit the conduct.

In the AI context, if a cross-border AI model trained on publicly scraped code is known to be capable of reproducing proprietary algorithms, deploying it without proper safeguards could satisfy both the legal and moral thresholds for *tasabbub* liability.

8.0 CONCLUSION

The next decade will likely witness AI systems with even greater capacity to autonomously identify and exploit valuable proprietary information. Without a forward-looking, integrated approach, enforcement gaps will widen, enabling malicious actors to exploit both legal loopholes and technological vulnerabilities. By drawing from Islamic law's moral clarity and blending it with modern policy instruments, we can create a truly harmonized framework that upholds both ethical and commercial justice. In the Qur'an, Allah commands: *"Indeed, Allah commands you to render trusts to whom they are due, and when you judge between people to judge with justice."* (Qur'an 4:58) This verse underpins both the spiritual and legal imperative to protect trade secrets in the AI age. It reminds us that safeguarding knowledge whether ancient or algorithmic is a trust (*amanah*) that transcends borders and epochs. The following are recommended:

1. **Draft Model Cross-Border Agreements** — Incorporating *Shariah*-based liability alongside TRIPS-compliant provisions.
2. **Establish Specialized Arbitration Panels** — Combining Islamic legal scholars and AI technical experts.
3. **Promote Corporate AI Ethics Codes** — Mandating lawful dataset sourcing and internal IP audits.
4. **Adopt Islamic Digital Forensics Standards** — Ensuring *Shariah*-compliant evidence handling in AI cases.
5. **Integrate AI Literacy in Fiqh Councils** — Training jurists on AI's technical and legal implications.