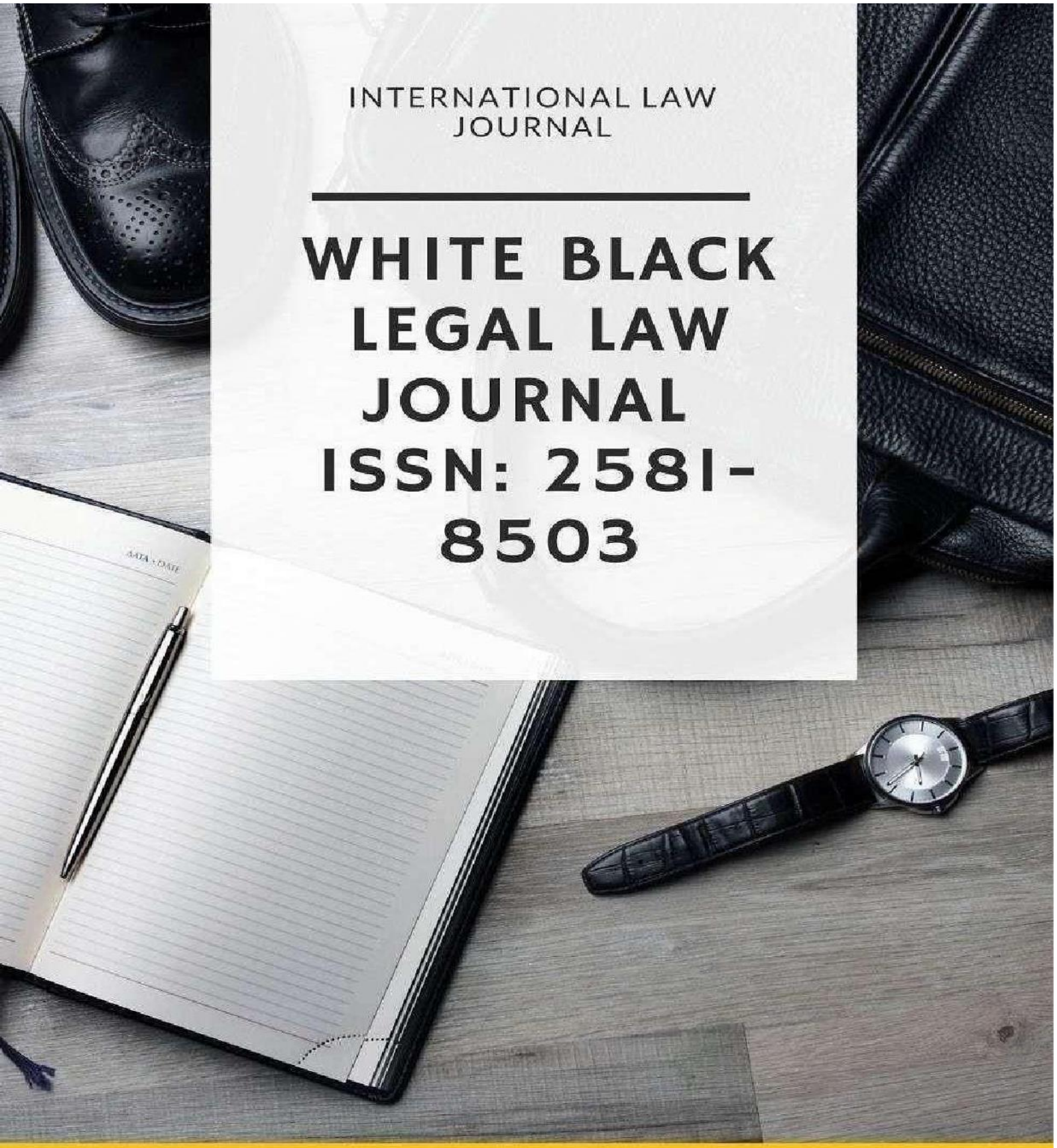

INTERNATIONAL LAW JOURNAL

# WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

## Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

# DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

# ABOUT WHITE BLACK LEGAL

*White Black Legal – The Law Journal* is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

# AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

www.whiteblacklegal.co.in
Volume 3 Issue 7 | June 2026 ISSN: 2581-8503

# TRADE SECRET PROTECTION OF ARTIFICIAL INTELLIGENCE SYSTEMS: CHALLENGES AND OPPORTUNITIES

AUTHORED BY - PRANJAL TAPARIA

## Abstract

Artificial Intelligence has surfaced as one of the most game- changing technologies of the 21st, transforming industries ranging from healthcare and finance to manufacturing and education. As institutions increasingly invest significant resources in developing advanced AI systems, the protection of significant AI related information has become a critical legal and commercial concern. While patent, copyrights and other types of Intellectual property protection provide certain protections, trade secret protection has acquired significant recognition as a preferred mechanism for protecting AI innovations. Compared to patents, trade secret do not require public disclosure and can potentially provide protection for an indefinite duration, making them particularly attractive for preserving proprietary algorithms, source code, training datasets, model architectures, and confidential business process.

Despite these benefits, the application of trade secret law to AI systems presents several challenges. The increasing requirement for transparency and explainability in AI decision-making, risks associated with reverse engineering, cybersecurity threats, employee mobility, and the global nature of AI development develop significant challenges to maintaining secrecy. Furthermore, the absence extensive trade secret legislation in certain jurisdictions, including India, raises issues regarding the sufficiency of legal protection available to AI developers and businesses.

This paper examines the role of trade secret in shielding artificial intelligence systems and analyzes the legal, technological, and commercial challenges associated with such protection. Through doctrinal and analytical method, the study evaluates existing international and national legal approach governing trade secrets and explores evolving prospects for strengthening AI related intellectual property protection. This paper infers that while trade secret protection offers considerable advantages for AI innovation, effective protection requires

robust legal frameworks, improved cybersecurity measures, and a balanced approach that reconciles confidentiality interests with growing regulatory demands for transparency and answerability in artificial intelligence systems.

**Keywords:** Artificial Intelligence, Trade Secrets, Intellectual Property Rights, Confidential Information, AI Governance.

## Introduction

Artificial intelligence (AI) has evolved as one of the influential technological developments of the modern era, reshaping the manner in which businesses, governments, and individuals interact with digital systems, AI technologies are progressively being integrated into diverse sectors, including healthcare, finance, education, transportation, manufacturing, and national security. During the use of machine learning algorithms, neutral networks, and advanced data analytics, AI systems can conduct tasks that traditionally required human intelligence, such as decision- making, patter recognition, language processing, and predictive evaluation. The rapid growth of AI applications has generated significant economic value and heightened competition among organizations seeking to develop innovative and commercially viable AI solutions.[1]

The development of artificial intelligence systems requires significant investments in research, infrastructure, technical expertise, and data acquisition. Institutions often dedicate extensive resources to creating proprietary algorithms, collecting and compiling training datasets, designing model architectures, and refining AI outputs. These elements establish valuable intangible assets that provide a competitive advantage in the marketplace. Consequently, the protection of AI- related innovations has become a critical concern for businesses and policymakers alike. Effective intellectual property protection not only safeguards commercial interests but also encourages novelty by ensuring that creators and investors can derive economic benefits from their attempts.[2]

Traditionally, intellectual property law has relied upon patents, copyrights, trademarks, and

[1]OECD, 'Artificial Intelligence, Machine Learning and Intellectual Property' (2023) OECD AI Policy Observatory <https://oecd.ai/en/> accessed 6 June 2026.
[2] World Intellectual Property Organization, 'Intellectual Property and Artificial Intelligence' WIPO Frontier Technologies Program <https://www.wipo.int/en/web/frontier-technologies/artificial-intelligence/index> accessed 6 June 2026.

industrial designs to protect technological innovations. However, the unique features of AI systems present challenges for traditional forms of intellectual property protection. Patent protection requires public disclosure of the invention, which may expose the valuable technical information to competitors. Copyright law primarily protects the expression of ideas rather than operational concepts, thereby limiting its effectiveness in protecting algorithms and machine learning techniques. As a result, many AI developers have increasingly turned to trade secret protection as an alternative or complementary mechanism for preserving the confidentiality of valuable technological information.[3]

Trade secrets play an important role in the modern knowledge economy because they protect commercially valuable information that derives its value from remaining protected. Unlike patents, trade secrets do not require registration or disclosure to governmental officials. Protection is generally available for information that is secret, possesses commercial value, and is subject to justified measure to maintain its non- disclosure. In the framework of artificial intelligence, trade secrets may include source code, algorithms training datasets, model parameters, deployment strategies, and internal business processes. The flexibility and potentially unascertained duration of trade secret protection make it particularly attractive for AI companies operating in rapidly evolving technological environments.[4]

Despite these benefits, the application of trade secret law to AI systems is accompanied by several legal and practical challenges. The increasing need for transparency and explainability in AI decision making often conflicts with the proprietary nature of trade secrets. Regulatory frameworks around the world are increasingly affirming accountability and transparency in automated decision-making systems, thereby creating tension between public interests and proprietary business interests. Furthermore, AI technologies are vulnerable to reverse engineering, model extraction attacks, cybersecurity breaches, and unauthorized disclosure by employees or business partners. These factors complicate the ability of organizations to maintain the secrecy necessary for legal protection.[5]

The challenges are particularly significant in jurisdictions where trade secret protection is not

[3] Daniel J Gervais, 'The Machine as Author' (2020) 105 Iowa Law Review 2053.
[4] Agreement on Trade-Related Aspects of Intellectual Property Rights' (TRIPS) art 39.
[5] World Economic Forum, 'AI Governance and Regulatory Developments' Artificial Intelligence Governance Alliance <https://initiatives.weforum.org/ai-governance-alliance/home> accessed 6 June 2026.

governed by a detailed statutory framework. In India, for instance, trade secret protection is primarily derived from contractual duties, equitable principles, and judicial recognition of confidential information rather than from dedicated legislation. Although Indian courts have acknowledged the importance of protecting sensitive business information, the absence of a specialized trade secret statute creates lack of certainty regarding the scope and enforcement of protection available to AI developers. By contrast, jurisdictions such as United States and the European Union have adopted more structured legal frameworks that specifically address trade secret misappropriation and enforcement.[6]

The growing importance of artificial intelligence has therefore generated an immediate need to examine whether existing trade secret laws are capable of analyzing the distinctive challenges posed by AI technologies. Such an evaluation is required not only to secure innovation but also to balance competing interests relating to transparency, accountability, competition, and public welfare. As governments continue to formulate AI governance frameworks, trade secret protection is likely to remain a central concern in discussions concerning the regulation and marketization of artificial intelligence systems.

## Research Methodology

The present study adopts a doctrinal, analytical, and comparative research methodology to examine the protection of Artificial Intelligence (AI) systems through trade secret law.[7] The research is doctrinal is nature because it principally relies upon the evaluation and interpretation of legal principles, statutes, judicial precedents, international agreements, policy documents, and scholarly writings relating to intellectual property rights and trade secrets.[8] The analytical aspect of the study involves a detailed appraisal of the adequacy of existing legal regimes in addressing the distinctive challenges posed by AI technologies. Furthermore, a comparative approach has been adopted to analyze the legal frameworks governing trade secret protection in India, The United States, and the European Union.[9]

[6] **India**: VFS Global Services Pvt Ltd v Suprit Roy SCC OnLine Del 1188; **United States**: Defend Trade Secrets Act, 18 USC §§ 1836–1839 (2016); **European Union**: Directive (EU) 2016/943 on the Protection of Trade Secrets <https://eur-lex.europa.eu/eli/dir/2016/943/oj> accessed 6 June 2026.

[7] William Twining and David Miers, *How to Do Things with Rules: A Primer of Interpretation* (5th edn, Cambridge University Press 2010).

[8] World Intellectual Property Organization, 'Artificial Intelligence' WIPO Frontier Technologies Program <https://www.wipo.int/en/web/frontier-technologies/artificial-intelligence> accessed 9 June 2026.

[9] Defend Trade Secrets Act, 18 U.S.C. §§ 1836–1839 (2016) <https://www.congress.gov/bill/114th-congress/senate-bill/1890> accessed 9 June 2026.

The study relies upon secondary sources of data, including international legal instruments such as the TRIPS agreement, legislative enactments such as the Defend Trade Secrets Act of the United States, the European Union Trade Secrets Directive, judicial decisions, reports published by the World Intellectual Property Organization, OECD publications concerning artificial intelligence, and scholarly articles examining the intersection between AI and intellectual property law.[10]

The scope of the study extends to various components of artificial intelligence systems including algorithms, source code, training datasets, model parameters, neutral network architectures, and confidential business strategies.[11] The research evaluates the extent to which these components satisfy the requirements of trade secret protection and examines the practical challenges associated with maintaining confidentiality in an increasingly interconnected technological environment.

## Understanding Trade Secret and Artificial Intelligence

Trade secrets constitute one of the oldest forms of intellectual property protection. Unlike patents, copyrights, or trademarks, trade secret protection does not depend upon registration or notification to a governmental authority. Instead, protection arises from a sensitive nature of information that possesses commercial applicability. Article 39 of the TRIPS Agreement defines protectable undisclosed information as information that is secret, possesses commercial value because it is secret, and has been subjected to reasonable steps to maintain secrecy.[12]

Artificial Intelligence refers to computer systems capable of conducting tasks that ordinarily require human intelligence. Moder Ai systems utilize machine learning algorithms, neutral networks, natural language, processing, and predictive analytics to perform complex operations.[13] The increasing commercialization of AI has transformed data and algorithms into valuable economic assets.[14] Companies invest billions of dollars in formulating AI

[10] World Intellectual Property Organization, 'Artificial Intelligence' WIPO Frontier Technologies Program <https://www.wipo.int/en/web/frontier-technologies/artificial-intelligence> accessed 9 June 2026.
[11] 'Agreement on Trade-Related Aspects of Intellectual Property Rights' (TRIPS) art 39 <https://www.wto.org/english/docs_e/legal_e/27-trips_04d_e.htm> accessed 9 June 2026.
[12] 'Agreement on Trade-Related Aspects of Intellectual Property Rights' (TRIPS) art 39 <https://www.wto.org/english/docs_e/legal_e/27-trips_04d_e.htm> accessed 9 June 2026.
[13] World Intellectual Property Organization, 'Artificial Intelligence' WIPO Frontier Technologies Program <https://www.wipo.int/en/web/frontier-technologies/artificial-intelligence> accessed 9 June 2026.
[14] OECD, 'Artificial Intelligence' OECD AI Policy Observatory <https://oecd.ai/en/> accessed 9 June 2026.

technologies competent of improving productivity, strengthening decision making, and generating innovative products and services.

Unlike conventional software, AI systems derive their effectiveness from a combination of algorithms, training data, computational infrastructure, and continuous learning mechanisms.[15] Consequently, protecting AI innovations involves protecting a wide range of confidential information rather than a single invention. This reality has substantially increased the importance of trade secret protection within the AI sector.

Trade secret law offers several advantages for AI developers. First, it avoids the disclosure requirements associated with patent protection. Second, it provides potentially perpetual protection as long as confidentiality is maintained. Third, it allows businesses to protect information that may not satisfy patentability requirements.[16] These benefits explain why many leading AI corporations depend heavily upon trade secret protection to safeguard their proprietary technologies.

## AI Components Eligible for Trade Secret Protection

- **Algorithms**

  Algorithms constitute the core operational mechanism of AI systems because they determine how data is processed, analyzed, and transformed into outputs.[17] Because algorithms can often be difficult to patent and may require public disclosure under patent law, trade secret protection has become an attractive alternative.[18] Major Technology corporations commonly protect machine learning algorithms as trade secrets rather than claiming patent protection. Maintaining algorithmic secrecy allows companies to safeguard technological benefits while avoiding public revelation.

- **Source Code**

  Source code represents the human- readable instructions that enable software

[15] World Intellectual Property Organization, 'Artificial Intelligence' WIPO Frontier Technologies Program <https://www.wipo.int/en/web/frontier-technologies/artificial-intelligence> accessed 9 June 2026.
[16] 'Agreement on Trade-Related Aspects of Intellectual Property Rights' (TRIPS) art 39 <https://www.wto.org/english/docs_e/legal_e/27-trips_04d_e.htm> accessed 9 June 2026.
[17] World Intellectual Property Organization, 'Trade Secrets' WIPO <https://www.wipo.int/web/tradesecrets> accessed 9 June 2026.
[18] World Intellectual Property Organization, 'Trade Secrets' WIPO <https://www.wipo.int/web/tradesecrets> accessed 9 June 2026.

applications to function.[19] Although copyright law confers protection against unauthorized copying of source code, it does not inevitably prevent competing enterprises from independently developing comparable systems. Trade secret protection supplements copyright protection by safeguarding confidential aspects of software development.[20]

The unauthorized revelation of source code can have severe implication, including the loss of competitive advantage and increased exposure to cyberattacks. Consequently, technology corporations invest significant resources in executing confidentiality measures to protect source code.

- **Training Datasets**

  Training datasets are among the most valuable assets in modern AI systems because the performance of machine learning models depends significantly upon the quality, quantity, and diversity of data used during training.[21] Organizations often expend substantial resources collecting, cleaning, and organizing datasets, making them commercially valuable assets.[22]

  Because datasets frequently hold commercially valuable information that cannot readily be copied, trade secret protection offers an effective means of protecting these assets. The enhancing significance of data- driven innovation has transformed datasets into crucial elements of intellectual property strategies.

- **Model Parameters and Neural Network Architectures**

  AI models often contain millions or even billions of parameters that determine how the system generates outputs.[23] These guidelines represent the accumulated learning acquired during training protocols and are often considered highly significant proprietary assets.

  Similarly, unique neural network architectures may provide significant performance

[19] World Intellectual Property Organization, 'Copyright' WIPO <https://www.wipo.int/copyright> accessed 9 June 2026.
[20] World Intellectual Property Organization, 'Trade Secrets' WIPO <https://www.wipo.int/web/tradesecrets> accessed 9 June 2026.
[21] World Intellectual Property Organization, 'Artificial Intelligence' WIPO Frontier Technologies Program <https://www.wipo.int/en/web/frontier-technologies/artificial-intelligence> accessed 9 June 2026.
[22] OECD, 'Artificial Intelligence' OECD AI Policy Observatory <https://oecd.ai/en/> accessed 9 June 2026.
[23] OECD, 'Artificial Intelligence' OECD <https://www.oecd.org/en/topics/artificial-intelligence.html> accessed 9 June 2026.

advantages and therefore constitute valuable proprietary information.[24] Protecting such information through trade secret law permits businesses to maintain market leadership and technological superiority.

## Challenges in Protecting AI Systems Through Trade Secrets

- **Reverse Engineering**

  One of the most significant challenges associated with AI trade secrets is reverse engineering, whereby competitors analyze publicly available AI products to infer underlying algorithms or replicate model functionality.[25] In contrast to traditional confidential information, AI outputs often demonstrate observations into system design and operational characteristics.

- **Model Extraction Attacks**

  Modern AI systems face risks from model extraction attacks, whereby malicious actors interact with AI systems and use outputs to reconstruct proprietary models.[26] Such attacks jeopardize the confidentiality that forms the basis of trade secret protection.

- **Cybersecurity Threats**

  The increasing digitalization of business operations has exposed AI systems to sophisticated cybersecurity threats that target proprietary algorithms, training, datasets, and source code.[27] Cybersecurity occurrences can result in the damage of trade secret position if confidential information becomes publicly available.

- **Employee Mobility**

  Technology industries experience high levels of employee mobility as skilled engineers frequently move between competing organizations, creating risk that confidential information may be transferred, intentionally or unintentionally, to competitors.[28]

[24] World Intellectual Property Organization, 'Artificial Intelligence' WIPO Frontier Technologies Program <https://www.wipo.int/en/web/frontier-technologies/artificial-intelligence> accessed 9 June 2026.
[25] World Intellectual Property Organization, 'Trade Secrets' WIPO <https://www.wipo.int/web/tradesecrets> accessed 9 June 2026.
[26] OECD, 'Artificial Intelligence' OECD AI Policy Observatory <https://oecd.ai/en/> accessed 9 June 2026.
[27] OECD, 'Digital Security' OECD <https://www.oecd.org/en/topics/digital-security.html> accessed 9 June 2026.
[28] World Intellectual Property Organization, 'Trade Secrets' WIPO <https://www.wipo.int/web/tradesecrets> accessed 9 June 2026.

- **Transparency and Explainability Requirements**

  Recent regulatory developments emphasize transparency and accountability in AI decision- making and these frameworks require organizations to explain how AI systems reach conclusions as these requirements may conflict with the objective of maintaining trade secret protection.[29]

- **Cross- Border Enforcement Issues**

  AI development frequently involves international collaboration and cross- border data transfers, making enforcement of trade secret rights across multiple jurisdictions complex due to differences in national laws and enforcement mechanisms.[30]

## Comparative legal analysis

- **India**

  India lacks dedicated trade secret legislation. Protection is derived primarily from contractual obligations, equitable principles, and judicial recognition of confidential information. In the case of V.F.S Global Services Pvt. Ltd v. Suprit Roy, the court demonstrated judicial willingness to protect confidential commercial information.[31]

- **United States**

  The United States provides comprehensive protection through the Defend Trade Secrets Acts, 2016, which provides federal remedies for trade secret misappropriation and has significantly strengthened enforcement mechanisms.[32]

- **European Union**

  The European Union adopted Directive 2016/943 to harmonize trade secret protection across member state.[33] The legislation offers federal remedies for unauthorized

[29] European Commission, 'Fostering a European approach to Artificial Intelligence' (April 2021) European Commission Digital Strategy <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence> accessed 9 June 2026.
[30] Directive (EU) 2016/943 of the European Parliament and of the Council on the Protection of Trade Secrets <https://eur-lex.europa.eu/eli/dir/2016/943/oj> accessed 9 June 2026.
[31] VFS Global Services Pvt Ltd v Suprit Roy SCC OnLine Bom 1083 <https://indiankanoon.org/doc/1737985/> accessed 9 June 2026.
[32] Defend Trade Secrets Act, 18 U.S.C. §§ 1836–1839 (2016) <https://www.congress.gov/bill/114th-congress/senate-bill/1890> accessed 9 June 2026.
[33] Directive (EU) 2016/943 of the European Parliament and of the Council on the Protection of Trade Secrets <https://eur-lex.europa.eu/eli/dir/2016/943/oj> accessed 9 June 2026.

acquisition of trade secret and has significantly strengthened implementation mechanisms.

The comparative analysis reveals that while India recognizes trade secret rights, greater legislative certainty would enhance protection for AI innovators.[34]

## Trade Secrets Versus Patents: Strategic Considerations

Patents provide exclusive rights in exchange for public disclosure, whereas trade secrets provide confidentiality without disclosure requirements.[35] For AI corporations, disclosure can be economically disadvantageous because competing entities may obtain insights into proprietary technologies.

While patents provide stronger legal monopoly, trade secrets may offer more enduring protection. Consequently, many AI developer incorporate hybrid intellectual property strategies that integrate patents, copyrights, contracts, and trade secret protection.

## Emerging Opportunities for AI Trade Secret Protection

The rise of generative AI, foundation models, and AI-as-a-Service platforms has significantly increased the value of proprietary AI technologies and strengthened the importance of trade secret protection.[36] Organizations frequently rely upon confidential datasets, model architectures, and deployment strategies to differentiate themselves in competitive commercial environments.



As governments continue to develop AI governance structure, opportunities exist to reinforce trade secret protection through specialized legislation, improved cybersecurity standards, and international cooperation. Such measure can promote innovation while safeguarding the confidentiality required for technological advancement.

[34] VFS Global Services Pvt Ltd v Suprit Roy SCC OnLine Bom 1083 <https://indiankanoon.org/doc/1737985/> accessed 10 June 2026.
[35] World Intellectual Property Organization, 'Patents' WIPO <https://www.wipo.int/patents> accessed 10 June 2026.
[36] World Intellectual Property Organization, 'Artificial Intelligence' WIPO Frontier Technologies Program <https://www.wipo.int/en/web/frontier-technologies/artificial-intelligence> accessed 10 June 2026.

## The Growing Tension Between AI Transparency and Trade Secret Protection

One of the most significant legal issues in contemporary artificial intelligence governance is the conflict between transparency obligations and trade secret protection. As AI systems increasingly influence decisions relating to employment, healthcare, credit scoring, law enforcement, and public administration, regulators and policymakers have emphasized the importance of transparency, explainability, and accountability.[37] Transparency enables affected individuals to understand how decisions are made and facilitates the identification of discriminatory or biased outcomes.[38] However, the disclosure of information relating to the functioning of AI systems may undermine the confidentiality that forms the foundation of trade secret protection.

The issue is significantly relevant in the context of machine learning systems, where proprietary algorithms and model restructure constitute valuable commercial assets. Technology companies frequently argue that extensive disclosure requirements may expose sensitive technical information to competitors and diminish incentives for innovation.[39] On the other hand, regulators contend that individuals affected by AI driven decisions should be entitled to clear and meaningful explanations regarding the factors influencing those decisions. The key challenge is to find an appropriate balance between protecting legitimate commercial interests and ensuring public accountability.

Regulatory bodies worldwide have introduced various measures to address the balance between commercial interests and promoting transparency and accountability in AI decision making processes. The European Union's approach to AI governance emphasizes transparency obligations for certain categories of AI systems while simultaneously recognizing the need to protect intellectual property rights and confidential business information.[40] In various regions, similar debates are underway as policy makers are attempting to develop regulatory

[37] European Commission, 'Fostering a European approach to Artificial Intelligence' (April 2021) European Commission Digital Strategy <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence> accessed 10 June 2026.
[38] OECD, 'Artificial Intelligence' OECD <https://www.oecd.org/en/topics/artificial-intelligence.html> accessed 10 June 2026.
[39] World Intellectual Property Organization, 'Trade Secrets' WIPO <https://www.wipo.int/web/tradesecrets> accessed 10 June 2026.
[40] European Commission, 'Fostering a European approach to Artificial Intelligence' (April 2021) European Commission Digital Strategy <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence> accessed 10 June 2026.

frameworks that preserve innovation while safeguarding fundamental rights. The increasing intersection between AI regulation and trade secret law highlights the need for future legal frameworks to thoughtfully balance competing objectives rather than treating transparency and confidentiality as mutually exclusive concepts.

Furthermore, the emergence of explainable artificial intelligence technologies may provide a partial solution to this dilemma. Explainability tools enable organizations to provide understandable explanations regarding AI outcomes without necessarily revealing proprietary algorithms or source code.[41] As a result explainable AI may facilitate compliance with transparency requirements while safeguarding trade secret protection. The ongoing advancement of these technologies is expected to be instrumental in shaping future strategies for AI regulation and the protection of intellectual property.

## Future of Trade Secret Protection in the Artificial Intelligence Era

The increasing reliance upon artificial intelligence across industries suggest that trade secret protection will become even more significant in the coming years.[42] As AI systems become increasingly advanced, organizations are expected to invest substantial resources in developing proprietary models, datasets, and computational methods. These investments generate strong motivation for businesses to pursue legal protections that protect their confidential technological assets from misappropriation.

One emerging trend is the increasing adoption of hybrid intellectual property strategies.[43] Rather than solely depending on patents, copyrights, or trade secrets, organizations are adopting a combination of multiple forms of protection to enhance their overall security and safeguard their innovations more effectively. For example, source code may be protected through copyright law, novel technical inventions through patents, and confidential algorithms or datasets through trade secret protection.[44] Such integrated strategies allow businesses to

[41] OECD, 'Artificial Intelligence' OECD <https://www.oecd.org/en/topics/artificial-intelligence.html> accessed 10 June 2026.
[42] World Intellectual Property Organization, 'Artificial Intelligence' WIPO Frontier Technologies Program <https://www.wipo.int/en/web/frontier-technologies/artificial-intelligence> accessed 11 June 2026.
[43] World Intellectual Property Organization, 'Artificial Intelligence' WIPO Frontier Technologies Program <https://www.wipo.int/en/web/frontier-technologies/artificial-intelligence> accessed 11 June 2026.
[44] World Intellectual Property Organization, 'Copyright' WIPO <https://www.wipo.int/copyright> accessed 11 June 2026; World Intellectual Property Organization, 'Patents' WIPO <https://www.wipo.int/patents> accessed 11 June 2026; World Intellectual Property Organization, 'Trade Secrets' WIPO <https://www.wipo.int/web/tradesecrets> accessed 11 June 2026.

overcome the limitations associated with any single type of intellectual property protection, providing a more comprehensive safeguard for their technological assets.

Another important development concerns the rise of foundation models and generative AI systems.[45] These technologies require extensive investments in data collection, computational infrastructure, and model training.[46] The commercial value associated with these systems has increased the importance of safeguarding training methodologies, model parameters, and deployment strategies to maintain competitive advantage and prevent intellectual property theft. As competition intensifies within the AI industry, trade secret protection is likely to become a primary mechanism for preserving competitive advantages.[47]

At the international level, growing cross border collaboration in AI research and development may encourage greater harmonization of trade secret laws.[48] Differences among national legal systems often lead to uncertainty in enforcement and available remedies, especially is cases involving multinational technology companies, making it challenging to ensure consistent legal outcomes across borders. Increased international cooperation and adoption of common standards may strengthen the effectiveness of trade secret protection while facilitating innovation and technology transfer.[49]

Finally, the future effectiveness of trade secret will rely significantly on organizational practices. Legal rights alone are insufficient if businesses do not establish and maintain appropriate confidentiality measures. Companies must therefore adopt comprehensive strategies involving cybersecurity safeguards, employee training programs, non- disclosure agreements, access controls, and data governance frameworks.[50] Such measures are crucial for meeting the legal requirements of trade secret protection and reducing the risk of unauthorized disclosure, thereby ensuring the confidentiality and integrity of valuable information. As

[45] World Intellectual Property Organization, 'Artificial Intelligence' WIPO Frontier Technologies Program <https://www.wipo.int/en/web/frontier-technologies/artificial-intelligence> accessed 11 June 2026.
[46] OECD, 'Artificial Intelligence' OECD AI Policy Observatory <https://oecd.ai/en/> accessed 11 June 2026.
[47] World Intellectual Property Organization, 'Trade Secrets' WIPO <https://www.wipo.int/web/tradesecrets> accessed 11 June 2026.
[48] 'Agreement on Trade-Related Aspects of Intellectual Property Rights' (TRIPS) art 39 <https://www.wto.org/english/docs_e/legal_e/27-trips_04d_e.htm> accessed 12 June 2026.
[49] World Intellectual Property Organization, 'Trade Secrets' WIPO <https://www.wipo.int/en/web/tradesecrets> accessed 12 June 2026.
[50] OECD, 'Digital Security' OECD <https://www.oecd.org/en/topics/digital-security.html> accessed 12 June 2026.

artificial intelligence continues to evolve, the integration of robust legal protections with effective technological safeguards will remain central to preserving innovation and maintaining competitive advantage in the digital economy.[51]

## Findings

This study shows that trade secret protection has become one of the most important legal methods for preserving artificial intelligence systems. Unlike traditional intellectual property rights, which often require public disclosure of protected information, trade secrets allow organizations to keep their valuable information confidential. This makes trade secrets especially useful for AI technologies, where the worth of proprietary algorithms, training data, source code, model parameters, and business processes depends heavily on keeping them secret. This approach gives companies the ability to protect their most valuable and sensitive information without having to reveal it to the public, which is particularly beneficial in the fast-evolving field of AI.

The study also discovers that many parts of artificial intelligence systems meet the key conditions needed for trade secret protection, which include being kept secret, having commercial value, and having reasonable steps taken to keep the information confidential. AI developers put a lot of money and technical effort into building these innovative systems, and if this information were to be leaked or shared without permission, it could seriously harm their competitive edge. As a result, trade secret laws play a crucial role in encouraging innovation and motivating investments in AI research and development by providing legal protection for their valuable information.

Another important finding is that trade secret protection often has practical benefits over patent protection when it comes to AI technologies. While patents give exclusive rights to an invention, they also require the inventor to publicly disclose details about it and their protection lasts for a limited time. On the other hand, trade secrets can potentially be kept protected forever, as long as the information stays secret. Because AI technology is advancing so quickly, many organizations see trade secrets as a more practical and beneficial way to protect their innovations compared to getting patents.

[51] World Intellectual Property Organization, 'Artificial Intelligence' WIPO Frontier Technologies Program <https://www.wipo.int/en/web/frontier-technologies/artificial-intelligence> accessed 12 June 2026.

The research also highlights a number of challenges that undermine the effectiveness of trade secret protection within the AI ecosystem. Techniques such as reverse engineering, model extraction attacks, cybersecurity breaches, employee turnover, and unauthorized data access all pose significant risks for AI developers and companies. As digital systems become increasingly interconnected and integrated, these vulnerabilities are further amplified, making it even more difficult to maintain the confidentiality of sensitive information. This growing complexity and interconnectedness add layers of difficulty in safeguarding trade secrets, which are essential for protecting innovation in the fast-evolving field of AI.

The study also reveals that new and evolving regulatory rules focusing on transparency, explainability, and accountability in artificial intelligence could potentially clash with the traditional principles of trade secret protection. While being transparent is crucial for building trust and ensuring AI systems do not produce biased or unfair results, demanding too much disclosure can undermine the motivation for companies to innovate by revealing sensitive technological details that they consider proprietary. Finding the right balance between these competing priorities is one of the biggest legal challenges facing AI regulation today. Balancing the need for openness with the need to protect trade secrets requires careful consideration, as too much transparency could stifle innovation, while too little could erode public trust and accountability in AI systems.

A comparative examination of different countries show that the United States and the European Union have quite detailed and robust legal systems specifically designed to protect trade secrets. In contrast, India mainly depends on contracts, fairness principles, and decisions made by courts to safeguard confidential business information. While Indian courts acknowledge the importance of keeping business secrets secure, the lack of specific laws dedicated to trade secrets creates ambiguity about exactly what rights are protected and how they can be enforced. This research underscores the urgent need for India to establish a clearer, more structural legal framework that can effectively address the unique challenges brought about by emerging technologies like artificial intelligence. Such a framework would help clarify rights and provide stronger protection in an increasingly digital and innovative landscape.

Ultimately, the study concludes that the future of safeguarding artificial intelligence will probably rely on a mix of legal measures and technological solutions working together. Relying solely on a trade secret protection may not be enough to tackle all the challenges that come

with AI development and use. Instead, organizations are increasingly turning to a combined approach that integrates various forms intellectual property protections, such as patents and copyrights along with contractual agreements, cybersecurity practices, and trade secret safeguards. This comprehensive, hybrid strategy is likely to offer the most effective way to protect AI innovations as the digital economy continues to evolve and become more complex. By leveraging both legal frameworks and advanced technology, organizations can better ensure their AI advancements are securely protected in a landscape characterized by rapid innovation and increasing interconnectedness.

## Suggestions

In light of the findings of this study, several measures may be adopted to strengthen the protection of artificial intelligence systems through trade secret law.

First and foremost, India needs to think about passing specific legislation focused solely on trade secrets. Such laws should clearly outline what types of confidential information can be protected, set clear standards for what constitutes misappropriation, and offer effective ways to address and remedy cases of unauthorized disclosure. Having a comprehensive legal framework in place would help eliminate the current uncertainty surrounding trade secret protection and would give businesses greater confidence to invest in artificial intelligence technologies. This dedicated legislation would serve as a solid foundation, providing clear guidelines and legal protections that encourage innovation while safeguarding valuable confidential information.

Secondly, companies working on artificial intelligence system need to put strong confidentiality measures in place to meet the legal standards required for trade secret protection. These measures should include a variety of safeguards such as non-disclosure agreements (NDAs), confidentiality clauses embedded within employment contracts, strict access control systems to limit who can view sensitive information, comprehensive cybersecurity protocols to defend against attacks, encryption technologies to protect data, and ongoing training programs for employees to reinforce the importance of secrecy. Maintaining effective internal governance and a culture of confidentiality is crucial for preserving the secrecy that trade secret protections rely on. By implementing these comprehensive measures, organizations can better ensure that their valuable AI innovations remain secure and legally

protected from unauthorized disclosure or misuse.

Third, policymakers need to focus on creating regulatory frameworks that strike a careful balance between the need for transparency and the legitimate interests of AI developers in safeguarding their confidential information. Instead of forcing companies to disclose detailed proprietary algorithms, regulators should promote the adoption of explainable AI techniques. These methods can offer clear and meaningful explanations of how AI systems work without exposing trade secrets. By taking this approach, regulators can help ensure accountability and transparency, which are important for public trust and safety, while still protecting the innovative efforts of AI developers. This balanced strategy would encourage responsible development and deployment of AI technologies, ensuring that essential trade secrets are preserved and that innovation continues to thrive.

Fourth, addressing the complexities of artificial intelligence technologies a more concerted international effort. As AI development often involves collaborations between companies from different countries and significant cross-border data sharing, it's essential to have consistent legal standards and robust enforcement mechanisms in place. This would enable governments to provide more effective protection for confidential information, regardless of where it's being used or shared. By working together, nations can establish a level playing field, prevent the theft of trade secrets, and ensure that companies investing in AI research and development are confident that their intellectual property is secure. This, in turn, will foster greater innovation and collaboration in the AI sector, as companies are more likely to engage in international partnerships when they can trust that their trade secrets will be protected.



Fifth, in order to safeguard their most valuable innovations, organizations should take a multi-faceted approach to intellectual property protection. By combining the use of trade secrets with other forms of intellectual property protection. By combining the use of trade secrets with other forms of intellectual property rights, such patents, copyrights, and contractual agreements, companies can create a comprehensive defense strategy that addresses different types of risks and vulnerabilities. This hybrid approach allows organizations to choose the most suitable forms of protection for each innovation, depending on its unique characteristics and requirements. By leveraging a combination of mechanisms, companies can minimize their reliance on a single method of protection, thus reducing their exposure to potential risks and vulnerabilities. This integrated approach enables organizations to maximize their legal

protection, maintain a competitive edge, and ensure the long-term value of their intellectual property investments.

Sixth, it is important for governments and regulatory bodies to promote the creation of industry-specific guidelines focused on safeguarding trade secrets related to artificial intelligence. These tailored guidelines can serve as valuable resource for businesses, helping them to better identify which information can be protected, establish effective confidentiality protocols, and respond swiftly and appropriately to cybersecurity threats or instances of technological theft. By providing clear and practical standards tailored to the unique challenges faced by different sectors within the AI industry, these guidelines can help organizations strengthen their defenses, prevent unauthorized access, and ensure that their valuable innovations remain secure. Ultimately, fostering such industry-specific best practices will support a more secure and trustworthy environments for AI development and deployment across various sectors.

Finally, more resources and funding should be allocated to strengthening cybersecurity infrastructure and enhancing digital risk management practices. As cyber threats and methods for extracting AI models grow more advanced and complex, implementing robust technological defenses will be vital in maintaining the confidentiality and security of AI systems. Protecting sensitive of AI systems. Protecting sensitive information from cyberattacks and unauthorized access is no longer optional but a critical part of safeguarding trade secrets in today's digital landscape. Therefore, establishing strong cybersecurity measures must be viewed as an integral and essential part of modern strategies for protecting trade secrets, ensuring that organizations can defend their valuable innovations against evolving digital threats effectively.



## Conclusion

Artificial Intelligence has emerged as a transformative technology that is reshaping economic activities, industrial processes, and decision-making mechanisms across the globe.[52] As organizations continue to invest substantial resources in the development of sophisticated AI systems, the protection of valuable technological assets has become an increasingly important legal and commercial concern.[53] This study has explored how trade secret protection can be

[52] World Intellectual Property Organization, 'Artificial Intelligence' WIPO Frontier Technologies Program <https://www.wipo.int/en/web/frontier-technologies/artificial-intelligence> accessed 16 June 2026.
[53] OECD, 'Artificial Intelligence' OECD AI Policy Observatory <https://oecd.ai/en/> accessed 16 June 2026.

used to safeguard artificial intelligence systems, thoroughly analyzing both the potential benefits and the obstacles involved in depending on trade secret law as a means of protecting innovations related to AI. It has looked into how trade secrets can help keep valuable AI technologies secure while also considering the limitations and difficulties that may arise when using legal framework for such advanced and rapidly evolving fields.

The study demonstrates that trade secrets provide significant advantages for AI developers because they protect commercially valuable information without requiring public disclosure.[54] Components such as algorithms, source code, training datasets, model parameters, neural network architectures, and confidential business processes frequently satisfy the requirement of trade secret protection and therefore constitute important intangible assets.[55] Unlike patents, which require disclosure and are limited in duration, trade secrets offer the possibility of indefinite protection provided that confidentiality is maintained.[56] This feature makes trade secret protection especially appealing in the fast-moving world of artificial intelligence, where technological progress often advances faster than traditional forms of intellectual property rights can keep up. In such dynamic environment, relying on trade secrets offers a flexible and immediate way to safeguard innovative AI developments without the delays or limitations that can come with other legal protections.

At the same time, the research highlights several challenges that complicate the effective protection of AI-related trade secrets.[57] Reverse engineering, model extraction attacks, cybersecurity threats, employee mobility, and cross-border enforcement difficulties create substantial risks for organizations seeking to preserve confidential information.[58] Moreover, increasing demands for transparency, explainability, and accountability in AI governance have generated tensions between public interests and the proprietary interests of technology

[54] World Intellectual Property Organization, 'Trade Secrets' WIPO <https://www.wipo.int/web/tradesecrets> accessed 16 June 2026.
[55] 'Agreement on Trade-Related Aspects of Intellectual Property Rights' (TRIPS) art 39 <https://www.wto.org/english/docs_e/legal_e/27-trips_04d_e.htm> accessed 16 June 2026.
[56] World Intellectual Property Organization, 'Patents' WIPO <https://www.wipo.int/patents> accessed 16 June 2026; World Intellectual Property Organization, 'Trade Secrets' WIPO <https://www.wipo.int/web/tradesecrets> accessed 16 June 2026.
[57] OECD, 'Artificial Intelligence' OECD AI Policy Observatory <https://oecd.ai/en/> accessed 16 June 2026.
[58] OECD, 'Digital Security' OECD <https://www.oecd.org/en/topics/digital-security.html> accessed 16 June 2026.

developers.[59] These advancements suggest that conventional methods of protecting trade secrets need to adapt and change in order to address the distinctive feature and complexities of artificial intelligence systems. As AI continues to develop rapidly and exhibit unique traits, traditional approach must evolve to effectively safeguard these innovative technologies.

The comparative analysis undertaken in this study further reveals that while jurisdiction such as the United States and the European Union have established comprehensive legal frameworks for trade secret protection, India continues to rely primarily upon contractual obligations and judicial principles.[60] The absence of dedicated trade secret legislation creates uncertainty regarding the scope of protection available to AI innovators and underscores the need for legislative reform.[61] Strengthening legal frameworks, fostering international cooperation, and promoting the implementation of strong confidentiality measures will be crucial for ensuring effective protection of artificial intelligence innovations in the future. These strategies will help create a more secure and coordinated environment for safeguarding trade secrets across borders and industries.

In conclusion, trade secret protection is a vital and growing mechanism for safeguarding artificial intelligence systems. Its success relies not only legal recognition but also in the adoption of robust organizational, technological, and regulatory safeguards. As artificial intelligence advances and becomes more embedded is society, creating balanced legal frameworks that protect innovation while ensuring accountability will be a key challenge for policymakers, businesses, and legal experts. The future of AI innovation will ultimately depend on the ability of legal systems to adapt to emerging technological realities, while maintaining the incentives essential for ongoing research, development, and economic progress

[59] European Commission, 'Fostering a European approach to Artificial Intelligence' (April 2021) European Commission Digital Strategy <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence> accessed 16 June 2026.
[60] Defend Trade Secrets Act, 18 U.S.C. §§ 1836–1839 (2016) <https://www.congress.gov/bill/114th-congress/senate-bill/1890> accessed 16 June 2026; Directive (EU) 2016/943 of the European Parliament and of the Council on the Protection of Trade Secrets <https://eur-lex.europa.eu/eli/dir/2016/943/oj> accessed 16 June 2026; VFS Global Services Pvt Ltd v Suprit Roy SCC OnLine Bom 1083 <https://indiankanoon.org/doc/1737985/> accessed 16 June 2026.
[61] VFS Global Services Pvt Ltd v Suprit Roy SCC OnLine Bom 1083 <https://indiankanoon.org/doc/1737985/> accessed 16 June 2026.