
PROTECTING AI ALGORITHMS: PATENTS, TRADE SECRETS, AND LICENSING: A COMPARATIVE LEGAL REVIEW

Pankaj Singh Karki, Chanakya National Law University

Kavya Malik, Gujarat National Law University, Gandhinagar

ABSTRACT

Today, artificial intelligence is developing rapidly, and the existing Intellectual property frameworks are turning out to be insufficient to protect these AI innovations. Section 3k of The Indian Patent Act 1970 does not grant patents to ai related innovations, Copyright under The Copyright Act 1957 remains restricted due to its human authorship requirements, and there is no law on trade secrets that rely on common law and contractual principles, While previous research has highlighted these problems they do not provide any effective policy solution.

This paper aims to propose a Hybrid IP Protection method integrating elements from trade secrets, patents, licensing, and copyrights. This study explores the best IP protection methods by assessing case studies from different jurisdictions including the USA, UK, EU, and Australia, presenting a hybrid model – offering patents for AI innovations, Trade secrets for proprietary algorithms, and licensing for controlled commercialization for effective legal protection.

In India, the development of Artificial Intelligence is facing a fragmented legal landscape. This paper introduces a structured IP method that promotes innovation while protecting ownership, The study concludes with recommendations for the Indian legislature to implement a HYBRID AI strategy that can promote innovation and encourage fair market competition while protecting the ownership of AI assets

This study contributes to the AI-IPR debate by presenting a more versatile and structured IP Framework ensuring a balanced and enforceable protection of AI-driven advancements.

Keywords: Artificial intelligence, Intellectual property, patents, trade secrets, India's AI policy and legal reforms.

INTRODUCTION

The term Artificial Intelligence was coined by John McCarthy as a vast discipline of computer science that deals with developing systems that can operate autonomously and intelligently.¹ Subsequently, Stuart Russell and Peter Norvig characterized AI as a system that is able to execute tasks typically necessitating human intelligence, such as recognition, decision-making, creation, learning, evolving, and communication.² Today, Artificial Intelligence is powering everything from autonomous cars to search engines, and the existing IP tools are failing to protect them.

AI can be subdivided into four main aspects: “1. Data inputs, which should contain the suspected signals and features that provide the essential information to address the proposed question; 2. The learning algorithm, 3. The operating model in use, and 4. The intended output.”³ The second aspect, the learning algorithm, will be the point of discussion in this literature. Algorithms are like a decision-making engine of AI, an integration of artificial neural networks (ANN) and machine learning (ML), determining how it behaves and how it learns. It can be defined as “a set of instructions to be followed in calculation or other operations.”⁴

They are proprietary assets requiring considerable investment in research, data collection, and model training, and it becomes crucial to protect them legally to maintain a competitive edge.⁵ Protecting these algorithms can be complicated. In India, the patentability of AI Algorithms is subject to the exclusions given in section 3k of the Patents Act,⁶ whereas in the USA, the Alice Doctrine makes it difficult to patent abstract ideas like algorithms.⁷ Copyright laws do not cover algorithms because they are not seen as expressive works. Trade secrets can be an alternative, but they rely on maintaining secrecy and cannot be enforced if the information is leaked or the algorithm is reverse-engineered⁸. Licensing agreements, though widely used, fail to address

¹ John McCarthy et al., *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence* (1955), <https://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf>.

² Stuart Russell & Peter Norvig, *Artificial Intelligence: A Modern Approach* 1–2 (4th ed. 2020)

³ Kevin M. Pasquinelli, *Adapt Your IP Strategy for Artificial Intelligence*, 2 J. Robotics, Artif. Intell. & L. 389 (Nov.–Dec. 2019).

⁴ *What Are AI Algorithms?*, Tableau, <https://www.tableau.com/data-insights/ai/algorithms> (last visited June 13, 2025).

⁵ Cassandra Jones Harvard, *Digital Footprints: Technology, Race, and Justice*, 45 CARDOZO L. REV. 1177 (April 2024).

⁶ The Patents Act, No. 39 of 1970, § 3(k), India Code (1970).

⁷ *Alice Corp. v. CLS Bank Int'l*, 573 U.S. 208 (2014).

⁸ See 18 U.S.C. § 1839(3)–(6) (2016); David S. Almeling, *Four Reasons to Enforce Trade Secret Laws*, 19 Fordham Intell. Prop. Media & Ent. L.J. 769, 778 (2009)

the technical and ethical risk, and do not provide long-term exclusivity, while newer licensing models like Open & Responsible AI Licenses (RAIL) impose user restrictions; the standardization and enforcement across jurisdictions with weaker enforcement mechanisms remains difficult⁹. The scarcity of clear legal precedents regarding AI algorithms' ownership makes algorithm protection challenging for developers, and the cross-border enforcement becomes difficult.

As a result, companies often adopt a combination of strategies such as patent applications, maintaining secrecy, and licensing agreements to manage and protect their algorithms. For example, OpenAI distributes the ChatGPT platform using licensing agreements with a strict confidentiality clause to protect its core algorithms, showing reliance more on trade secrets than traditional IP models. Meanwhile, IBM acquires patents for AI-driven data analysis and uses trade secrets to keep its Watson AI proprietary.¹⁰ While the existing literature mainly deals with IP protection of the input data used to train AI models, the output, and ownership rights. This paper specifically focuses on proprietary algorithms- arguably the most commercially sensitive component. This paper examines how Patents, Trade secrets, and licensing models are used in different legal systems, India, the U.S., and the EU for the protection of AI algorithms, and what lessons India could draw to improve. It further argues that currently, no single IP model is sufficient for algorithmic protection. It highlights the need to recognize a hybrid protection framework—one that pragmatically combines patent law (for technical innovations), trade secret law (for confidential operational models), and licensing (for usage control and commercial deployment). The paper suggests India should formally acknowledge this practice in official policy documents, issue sector-specific guidelines that would ensure enforceability, consistency, and incentivize AI innovations.

AI Algorithms and Patent Law

Patents are IP models that give exclusive rights to the developers, which preclude others from exploiting their inventions; usually, for 20 years, they can be filed as product, method, or use claims.¹¹ Under the Indian law, there are three essentials for the grant of patents: 1-novelty,

⁹ *The Turing Way Community, Licensing Machine Learning Models, The Turing Way* (Aug. 2022), <https://the-turing-way.netlify.app/reproducible-research/licensing/licensing-ml.html>.

¹⁰ Ryan Heath, IBM Outpaces Rivals in AI Patent Race, *Axios* (Feb. 5, 2024), <https://www.axios.com/2024/02/05/patent-applications-generative-ai-ibm-list>.

¹¹ European Patent Convention (EPC), as amended (2016), cited in Katarina Foss-Solbrekk, *Three Routes to Protecting AI Systems and Their Algorithms Under IP Law: The Good, the Bad and the Ugly*, 16 J. Intell. Prop. L. & Prac. 231, 234 (2021)

which means it should be unavailable globally before patent filing, 2-inventive step, it should not be obvious to anyone skilled in that field of art, 3-industrial applicability, it should have a practical use. Patents can be used as a crucial tool for the protection of technological innovations as they offer legal exclusivity in exchange for public disclosure, thereby promoting innovation and transparency.¹²

Patents are one of the strongest forms of IP protection for computer software, including AI algorithms, which serve as the core of many innovative systems. Algorithms can be framed as “method” and “process,” and in some cases, patentable subject matter¹³ However, their application to these algorithms is limited and complex. Across jurisdictions, the US, EU, and India, algorithms often fall under the exclusions of mathematical method and “abstract idea and get rejected by patent offices.¹⁴ Algorithms can still be granted patents if they can be proved to have a “technical application” or are embedded in a broader system having a “technical effect”.¹⁵ These limitations create a significant uncertainty for the developers of the algorithms seeking to protect their innovation. As a result, developers cannot depend only on patents and often use additional tools such as trade secrets and licenses to safeguard valuable algorithmic components.

The treatment of AI Algorithms under the Patent laws of different jurisdictions can vary. A closer study of the approaches followed by the USA, the EU, and India will help to illustrate what practical and doctrinal challenges are faced when developers try to secure patent protection for these innovations. This also reinforces the central argument of the paper- that in the face of uncertain patent standards, a hybrid approach becomes necessary to provide holistic protection to AI algorithms.

USA

The eligibility of AI algorithms as a subject matter under the US patent laws has been a considerable debate. Historically, algorithms, when expressed as mathematical formulae and

¹² World Intellectual Prop. Org., *What Is a Patent?*, <https://www.wipo.int/patents/en/> (last visited June 13, 2025)

¹³ European Patent Convention art. 52(2), as amended (2016), cited in Katarina Foss-Solbrekk, *Three Routes to Protecting AI Systems and Their Algorithms Under IP Law: The Good, the Bad and the Ugly*, 16 J. Intell. Prop. L. & Prac. 231, 233–34 (2021).

¹⁴ *Alice Corp. Pty Ltd. v. CLS Bank Int'l*, 573 U.S. 208 (2014)

¹⁵ Katarina Foss-Solbrekk, *Three Routes to Protecting AI Systems and Their Algorithms Under IP Law: The Good, the Bad and the Ugly*, 16 J. Intell. Prop. L. & Prac. 231 (2021).

abstract ideas, were not perceived as original and unworthy of protection.¹⁶ This position was reaffirmed in the US Supreme Court case of *Gottschalk v. Benson*, where the court was unconvinced by the argument that a computer-made thought process of creating an algorithm was more original or concrete.¹⁷ According to the court, the algorithm-based inventions were eligible for patentability only if they were “new and useful.”¹⁸ This case showcased the court's struggle in determining whether a computer can create an original thought.

At present, the patentability of algorithms is mainly governed by the Alice doctrine laid out in the case of *Alice Corp. Proprietary Ltd. V. CLS Bank International*, where the Supreme Court revoked a software patent, holding that proprietary technologies of computerized algorithms are abstract and thus are not patent eligible.¹⁹ Unless it could demonstrate that the method produced is unique, novel, nonobvious, and has a practical use.²⁰ The application of this doctrine by the Federal US courts and, U.S. Patent and Trademark Office. (UPTSO) has been inconsistent, creating uncertainty for the developer regarding which of their innovations are eligible for patent protection. To address this ambiguity, the UPTSO released a revised subject matter eligibility guidance²¹ on December 18, 2020, which clarified that AI/ML inventions are patentable as long as they are novel, non-obvious, and have practical application.²² Following the issuance of these guidelines, the UPTSO allowance rate grew from 15 percent to 38 percent, which also correlates to an increase in training of examiners in January 2019. The World Intellectual Property Organization (WIPO) has also recognized this in its technology trends study, concluding AI/ML innovation is booming, shifting from theory to commercial application.²³

While these policy improvements reflect a maturing approach, they also show the limits of a standalone patent regime. Today, AI algorithms may be patentable in the U.S. if they are

¹⁶ 35 U.S.C. § 101 (2018)

¹⁷ *Gottschalk v. Benson*, 409 U.S. 63, 67 (1972)

¹⁸ *Gottschalk v. Benson*, 409 U.S. 63, 69–70 (1972) (quoting *Cochrane v. Deener*, 94 U.S. 780, 780 (1876)), cited in Cassandra Jones Havard, *Digital Footprints: Technology, Race, and Justice*, 45 Cardozo L. Rev. 1177, 1188 (2024).

¹⁹ Cassandra Jones, Harvard, *Digital Footprints: Technology, Race, and Justice*, 45 CARDOZO L. REV. 1177 (April 2024).

²⁰ *Id.*

²¹ U.S. Patent & Trademark Off., *2019 Revised Patent Subject Matter Eligibility Guidance*, 84 Fed. Reg. 50 (Jan. 7, 2019)

²² *Id.*

²³ *WIPO Technology Trends 2019: Artificial Intelligence* (World Intellectual Prop. Org. 2019), quoted in Kevin M. Pasquinelli, *Adapt Your IP Strategy for Artificial Intelligence*, 2 J. Robotics, Artificial Intelligence & L. 389, 388 (Nov.–Dec. 2019)

framed with sufficient specificity, demonstrate a practical application, and satisfy the traditional requirements of novelty and non-obviousness. However, specificity and disclosure may not always be desirable, especially in the context of commercially sensitive algorithms; thus, a multi-pronged strategy becomes useful to navigate post-Alice uncertainty.

EUROPEAN UNION

Patents in Europe are governed by the European Patent Convention (EPC), which does not explicitly exclude algorithms; it generally treats them as excluded subject matter unless they demonstrate a technical effect beyond a mere mathematical method or abstract idea.²⁴

The Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement, specifically Article 27(1), permits patent protection for a wide array of technological subjects, including inventions, products, or processes.²⁵ However, ARTICLE 52 (2) of the EPC presents a challenge by excluding computer programmes and mathematical (defined under EPC as claims referring to ‘a sequence of computer-executable instructions’ that specify a ‘method rather than the method itself’²⁶ From patent protection. Algorithms—especially those based on machine learning—are often dismissed for lacking the “concrete technical character. If it can be demonstrated that the method involves the application of a technical means, such as a computing system, and the subject matter as a whole has a technical character, it can be patentable.²⁷ Ultimately, it is the “technical character” and the type of underlying algorithm of a computer programme that determines the likelihood of its patentability under EPC²⁸.

The European Patent Office (EPO) provides guidance on AI/ML, directing a close scrutiny of terms such as "reasoning engine" and "neural network" to determine whether the patent claim has a technical or an abstract character²⁹. For example, the use of neural networks to detect irregular heartbeats can be said to have a technical application. Similarly, classifying low-quality pixel data or signal patterns into images, speech, or videos may be patent-eligible when

²⁴ Emma Johansen, *Inventions without Inventors: The Challenge of Applying Patent Law Objectives to AI-Generated Inventions*, Lund University, 2022, pp. 10–11, 21–25

²⁵ Agreement on Trade-Related Aspects of Intellectual Property Rights art. 21, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299.

²⁶ Katarina Foss-Solbrekk, *Three Routes to Protecting AI Systems and Their Algorithms Under IP Law: The Good, the Bad and the Ugly*, 16 J. Intell. Prop. L. & Prac. 231 (2021).

²⁷ *Id.*

²⁸ *Id.*

²⁹ “Kevin M. Pasquinelli, Adapt Your IP Strategy for Artificial Intelligence, 2 THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (FASTCASE) 389 (November-December 2019).” (Pasquinelli, p. 388)

it improves a technical process.³⁰ However, classifying text documents purely based on linguistic content is generally not considered a technical purpose and may be excluded.³¹ The guidance acknowledges that a technical character can be attributed to an invention based on processes for training and classifying data³², especially when a novel method or architecture is involved. As such, patent protection under the EPC is often available for inventions that go beyond applying known models, offering inventive and practical technical improvements.

Since most of the contracting states of EPC are also TRIPS signatories, different jurisdictions can make different interpretations of the patentability of computer programmes. The Courts in the UK have allowed patents to computer programs, while Finnish and Italian patent offices do not categorically exclude patents for AI-related computer programs, though such applications are commonly filed as computer-implemented inventions (CIIs).³³ In contrast, the patent offices of Germany, Spain, Ireland, and the Czech Republic have expressly barred patents to computer programmes, in line with Article 52(c) of EPC.

EPC framework appears consistent, but its practical application to AI algorithms remains jurisdictionally fragmented. The “technical character” requirement remains central, but its interpretation varies depending on how national offices approach computer-implemented inventions. For developers, this means that while protection is possible, it often depends on how the algorithm is framed and where the patent is filed, making strategic drafting and jurisdictional awareness essential in Europe. In such a scenario where there is no clarity on “technical character,” a hybrid model combining different IP tools can serve as a necessary fallback.

INDIA

In India, the Indian Patent Office (IPO) classifies and treats AI systems as Computer-Related inventions (CRIs) if they incorporate a complex system of mathematical methods and/or algorithms.³⁴ The Indian Patent Act of 1970 governs patent applications in India. AI-related

³⁰ *Id.*

³¹ *Id.*

³² *Id.*

³³ Katarina Foss-Solbrekk, *Three Routes to Protecting AI Systems and Their Algorithms Under IP Law: The Good, the Bad and the Ugly*, 16 J. Intell. Prop. L. & Prac. 231 (2021).

³⁴ Office of the Controller General of Patents, Designs and Trade Marks, *Guidelines for Examination of Computer Related Inventions (CRIs)* (Feb. 19, 2016), https://ipindia.gov.in/writereaddata/Portal/Images/pdf/CRI_Guidelines_21_02_2016.pdf.

inventions are assessed against the subject matter exclusions mentioned in section (3k) of the act.³⁵ Which defines the phrase “mathematical methods, business models, computer programmes as such, and algorithms”³⁶. Since the algorithms are often structured as mathematical models or software, they fall within this exclusion, presenting a significant legal constraint in the patentability of AI Algorithms.

Indian Courts and Patent Office assess AI-related patent applications under the Guidelines for Examination of Computer-Related Innovations (CRIs), issued by the IPO in 2017. As per these guidelines, CRIs, like any other invention, must fulfil the requirements of “novelty”, ‘Inventive step’, “industrial application”, and “sufficiency of disclosure” for patent protection³⁷. However, they can be eligible for patent protection if they can demonstrate a “technical effect” or “technical contribution” and should be inextricably linked with hardware.³⁸ Indicating a stance similar to one adopted by the United Kingdom and the European Union.³⁹

A significant development in the Indian position came through the Delhi High Court’s ruling in *Ferid Allani v. Union of India and Ors.*⁴⁰ Acknowledged that AI and Blockchain technologies should not be excluded from patent protection, only because them being computer programmes, highlighting the importance of AI-related technologies in future innovations.⁴¹ The judgement emphasised the determination of “technical effect” or “technical contribution” of CRIs to decide their patentability. While the judgement itself doesn’t define the term, it states, “the meaning of ‘technical effect’ is no longer in dispute owing to the development of judicial precedents and patent office practices internationally and in India”.⁴²

Although statutory exclusions in Section 3(k) present challenges, the changing interpretation seen in the CRI Guidelines and court rulings such as *Ferid Allani* suggest a more lenient

³⁵ Kumari, Riddhi. *The Role of Patent in an AI Driven World*, 4 Indian Journal of Law and Legal Research 1 (2022), pp. 11–12

³⁶ *Id.*

³⁷ Neha Arora & Joyita Deb, *The Viewpoint: A Future-Proof Indian Patent Office? Patenting AI Inventions in India, Bar & Bench* (Feb. 23, 2022), <https://www.barandbench.com/columns/a-future-proof-indian-patent-office-patenting-ai-inventions-in-india>.

³⁸ Kumari, Riddhi. *The Role of Patent in an AI Driven World*, 4 Indian Journal of Law and Legal Research 1 (2022), pp. 11–12

³⁹ Neha Arora & Joyita Deb, *The Viewpoint: A Future-Proof Indian Patent Office? Patenting AI Inventions in India, Bar & Bench* (Feb. 23, 2022), <https://www.barandbench.com/columns/a-future-proof-indian-patent-office-patenting-ai-inventions-in-india>.

⁴⁰ *Ferid Allani v. Union of India & Ors.*, W.P. (C) No. 7 of 2014 (Delhi High Court Dec. 12, 2019).

⁴¹ Neha Arora & Joyita Deb, *The Viewpoint: A Future-Proof Indian Patent Office? Patenting AI Inventions in India, Bar & Bench* (Feb. 23, 2022), <https://www.barandbench.com/columns/a-future-proof-indian-patent-office-patenting-ai-inventions-in-india>.

⁴² *Id.*

approach to the patentability of AI algorithms, as long as the invention shows “technical effect,” they have a “technical contribution”. Developers continue to face uncertainty due to the absence of consistent statutory clarity on algorithm-specific languages, reinforcing the need to support patent claims with other IP tools for layered protection.

AI Algorithms and Trade Secrets

A trade secret is confidential business or technical information that “drives an independent economic value” from “not being publicly known”, and “is protected through reasonable efforts to maintain its secrecy”.⁴³ Unlike patents or copyrights, trade secrets do not confer exclusive rights to the information itself; rather, they protect against unauthorized acquisition, use, or disclosure⁴⁴. Trade secrets were first formally defined in the Restatement (First) of Torts, which stressed that secrecy is their central element, stating “the subject matter of a trade secret must be secret.”⁴⁵. Later the USA's Uniform Trade secrets acts(UTSA) defined what constitutes as trade secret- “A formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy”⁴⁶.

Since algorithms are mathematical methods and abstract ideas, and are not creative expressions, protecting them using copyright and patents can be challenging. Trade secrets offer a valuable alternative, providing indefinite protection. Moreover, AI systems are generally anonymous and have a commercial value; thus, they become eligible for trade secret protection. They are particularly useful for protecting proprietary 'know-how,' which, unlike patents, need not be novel or disclosed.⁴⁷ According to WIPO, trade secret protection is automatic if the owner takes certain steps to protect the secret and derives commercial value from keeping the secret.⁴⁸

⁴³ 18 U.S.C. § 1839(3) (2016)

⁴⁴ *Id.*

⁴⁵ Restatement (First) of Torts § 757 (Am. L. Inst. 1939)

⁴⁶ Unif. Trade Secrets Act § 1(4) (Unif. L. Comm'n 1985)

⁴⁷ Kevin M. Pasquinelli, Adapt Your IP Strategy for Artificial Intelligence, 2 THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (FASTCASE) 389 (November-December 2019)

⁴⁸ World Intellectual Prop. Org., *Trade Secrets*, <https://www.wipo.int/tradesecrets/en/> (last visited June 13, 2025)

Protecting AI algorithms using Trade secrets has its downsides; it only lasts as long as the information is kept secret and offers no protection if the information is independently discovered or reverse-engineered (which is legal), making it inherently fragile. This fragility underscores the core argument of this paper—that AI algorithm protection often demands a hybrid model combining trade secrets with patent claims and licensing agreements to balance secrecy, control, and enforceability.

The United States provides one of the most developed legal regimes for trade secret protection, particularly after the passage of the Defend Trade Secrets Act (DTSA) of 2016, which federalized trade secret enforcement. The next section explores this framework in greater depth.

USA

In the USA, trade secret protection is governed by the DTSA at the federal level and the Uniform Trade Secrets Act (UTSA) at the state level, with different states adopting their own variation of UTSA.⁴⁹ Under 18 U.S.C. § 1839(3), trade secrets can include “a formula, pattern, compilation, program, device, method, technique, or process”⁵⁰ That is “not generally known” and “drives an independent economic value” from secrecy, and is subject to reasonable measures to maintain its secrecy.⁵¹ This expansive definition allows AI algorithms -including learning methods, model architectures, and optimization techniques to be protected by trade secrets provided the confidentiality is preserved.

The precedent set in *Alice Corp. v. CLS Bank Int'l*, with its stringent subject matter eligibility requirements, makes it difficult for AI algorithms to get patent protection.⁵² Thus, developers often resort to trade secrets, which include not only the code itself but also model weights, datasets, and training processes that power complex machine learning systems.

Notably, DTSA expressly permits reverse engineering, under its U.S.C. § 1839(6)(B), which states that acquiring a trade secret through reverse engineering does not constitute “Improper

⁴⁹ See 18 U.S.C. §§ 1836–1839 (2018); Unif. Trade Secrets Act §§ 1–14 (Unif. L. Comm'n 1985), <https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=01f85cbf-4aaf-fd2d-51fd-71a65793ae1e>.

⁵⁰ 18 U.S.C. § 1839(3) (2018) (“a formula, pattern, compilation, program, device, method, technique, or process”)

⁵¹ *Id.*

⁵² *Alice Corp. v. CLS Bank Int'l*, 573 U.S. 208 (2014).

means”.⁵³ As a result, AI firms often resort to contract law by including confidentiality and anti-reverse-engineering provisions in license agreements to supplement trade secret protections, and courts often enforce these clauses.⁵⁴ For example, OpenAI’s ChatGPT is distributed under licensing terms that prohibit reverse engineering or model probing.⁵⁵

The application of trade secret law to AI was prominently demonstrated in *Waymo LLC v. Uber Technologies, Inc.*, where Waymo alleged misappropriation of confidential LiDAR algorithms used in autonomous vehicles. The case, brought under the DTSA, was settled for \$245 million and reaffirmed that AI-related algorithms can be protected as trade secrets under U.S. law.⁵⁶

In summary, the USA provides trade secrets mechanisms for protection with the DTSA and the UTSA, along with relying on contract law and judicial enforcement. However, these federal and state laws still do not address the issue of reverse engineering; thus, pairing trade secrets with careful licensing and anti-reverse engineering clauses becomes essential for the protection of AI innovations. The next section will provide a similar examination of trade secret protection to AI algorithms in the EU.

European Union

In the European Union, trade secret legislation is relatively novel compared to the USA, and is governed by European Trade Secret Directives (EUTSD). It sets minimum standards of protection across member states, aligning with Article 39 of the TRIPS, which requires the signatories to ensure protection of ‘undisclosed information from disclosure’.⁵⁷ Although TRIPS does not explicitly define trade secrets, Recitals 1, 2, and 14 of the EUTSD clarify that they include “know-how”, along with “business and technological information”, as well as

⁵³ 18 U.S.C. § 1839(6)(B) (2016).

⁵⁴ Camilla A. Hrdy, *Keeping ChatGPT a Trade Secret While Selling It Too*, 40 Berkeley Tech. L.J. 75, 84–85 (2025).

⁵⁵ *Id.*

⁵⁶ Complaint, *Waymo LLC v. Uber Techs., Inc.*, No. 3:17-cv-00939 (N.D. Cal. Feb. 23, 2017); see also Daisuke Wakabayashi, *Uber Settles With Waymo Over Trade Secrets*, N.Y. Times (Feb. 9, 2018), <https://www.nytimes.com/2018/02/09/technology/uber-waymo-lawsuit-settlement.html>.

⁵⁷ Agreement on Trade-Related Aspects of Intellectual Property Rights art. 39, Apr. 15, 1994, 1869 U.N.T.S. 299.

“commercial data related to customers”.⁵⁸

While trade secret protection is not classified as a form of intellectual property in the EU, it plays a growing role in protecting commercially sensitive AI algorithms from disclosure.⁵⁹ Since algorithms have a proprietary nature and a commercial value, they are eligible to be protected as a trade secret under EUSTD. Nonetheless, the collaborative aspect of AI algorithms necessitates information sharing among various parties, making it challenging to maintain confidentiality. Bashir observes that even with harmonization, effectively enforcing these agreements is tough when collaboration and information exchange are central to AI development.⁶⁰

There has been an increasing concern in the European Union about the reliance on trade secrets to protect AI algorithms. This concern mainly stems from the lack of transparency in the working of these systems, which obstructs accountability and public scrutiny, affecting high-stakes sectors like health care and criminal justice.⁶¹ For instance, the UK’s Visa scoring algorithms were found to have discriminatory effects based on race, yet trade secret protections blocked further legal examination.⁶² Another major issue that makes the Trade Secret a poor solution for AI in the EU is that EUSTD explicitly states that trade secrets are not intellectual property rights.⁶³ Unlike patents and copyrights, trade secrets do not confer an exclusive right to information.⁶⁴ These concerns have highlighted the need for stronger trade secret laws that could balance innovation incentives with transparency with accountability.

INDIA

In India, trade secret protection is comparatively less developed than in the USA and the EU.

⁵⁸ Directive 2016/943 of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure, 2016 O.J. (L 157) 1.

⁵⁹ Katarina Foss-Solbrekk, *Three Routes to Protecting AI Systems and Their Algorithms Under IP Law: The Good, the Bad and the Ugly*, 16 J. Intell. Prop. L. & Prac. (3) 2021.

⁶⁰ Anna Bashir, *Prospects and Challenges of Artificial Intelligence Protection in Indian IPR Regime vis-à-vis EU, China and the US*, 30 J. Intell. Prop. Rts. 65 (2025).

⁶¹ Katarina Foss-Solbrekk, *Three Routes to Protecting AI Systems and Their Algorithms Under IP Law: The Good, the Bad and the Ugly*, 16 J. Intell. Prop. L. & Prac. (3) 2021.

⁶² Joint Council for the Welfare of Immigrants, *Home Office Scraps Racist Visa Algorithm After Legal Challenge* (Aug. 4, 2020), <https://www.jcwi.org.uk/News/home-office-scraps-racist-visa-algorithm-after-legal-challenge>.

⁶³ Directive 2016/943 of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure, 2016 O.J. (L 157) 1.

⁶⁴ *Id.*

Currently, there is no single legislation in India that defines trade secrets. The National Information Bill (NIB) 2008 mentions trade secrets in its preamble, but is silent on what constitutes a trade secret.⁶⁵ India, as a signatory of the TRIPS agreement, is obligated to protect “confidential information,” but it still lacks any dedicated statute to combat misappropriation of trade secrets.

In Practice, the “confidential information,” including AI algorithms, in India can be protected through a combination of common law, contract law, and the Information Technology Act 2000⁶⁶, and mainly judge-made law⁶⁷. Since Judges in India often rely on the Trade secrets definition given in Black's Law Dictionary⁶⁸, which can include “methods”, “programme”, and “techniques”, terms broad enough to include AI Algorithms.⁶⁹ The enforcement of trade secrets in India primarily relies on confidentiality agreements and non-disclosure clauses under the Indian Contract Act, 1872.⁷⁰ The Delhi High Court, in the case of *American Express Bank Ltd. v. Priya Puri*, acknowledged that trade secrets may encompass “set formulae for the manufacture of products.”⁷¹ This perspective illustrates how Indian courts perform a fact-specific analysis, emphasizing whether the contract included confidentiality obligations and how the subject matter was safeguarded.

The NIB in its chapter IV, from section 8 to 14, also provides remedies for the protection of confidential information,” while strictly obligating third parties to receive information from authorized channels only. The bill explicitly allows for independent creation as an exception to misappropriation, but remains silent on the issue of reverse engineering, which is seen as a fair practice in other jurisdictions.⁷² Unfortunately, this bill, which could have provided a robust framework for trade secret protection, was never enacted. Later Parliamentary Standing Committee on Commerce, in its 161st report in 2021, highlighted the need for dedicated legislation for trade secrets. The committee emphasised that protecting data and ensuring its

⁶⁵ See *The National Innovation Bill, 2008* (India) (unpublished draft), <https://prsindia.org/billtrack/the-national-innovation-bill-2008>.

⁶⁶

⁶⁷ Law Comm'n of India, *Report No. 289: Trade Secrets and Economic Espionage* (Mar. 17, 2024).

⁶⁸ *Id.*

⁶⁹ *Trade Secret*, *Black's Law Dictionary* (11th ed. 2019).

⁷⁰ Law Comm'n of India, *Report No. 289: Trade Secrets and Economic Espionage* (Mar. 17, 2024).

⁷¹ See *American Express Bank Ltd. v. Priya Puri*, 2006 SCC OnLine Del 19.

⁷² See *The National Innovation Bill, 2008* (India) (unpublished draft), <https://prsindia.org/billtrack/the-national-innovation-bill-2008>.

confidentiality in business and trade is crucial for companies that hold “secret formulas, business strategies, algorithms, etc”.⁷³

In the absence of a dedicated statute, trade secrets are protected under the broader umbrella term of “confidential information,” and contractual safeguards remain the most reliable protection for AI algorithms in India. Developers must ensure robust NDAs, internal controls, and documentation of economic value to build enforceable claims under Indian law.

Licensing as a Complementary Tool for Algorithm Protection

Licensing, which is traditionally a contractual mechanism that allows the use of Intellectual properties under specified terms, has seen a growing use in filling the gaps left by patents, trade secrets, and copyright, especially in the context of AI algorithms. Licensing, which has traditionally been a contractual tool to allow the use of intellectual property under specified conditions, is increasingly utilized to address the legal and practical voids left by patents and trade secrets, particularly in the context of AI algorithms.⁷⁴ Unlike statutory intellectual property protections, licensing does not confer ownership rights. Instead, it governs the manner, location, and individuals permitted to access, utilize, and distribute an AI artifact.⁷⁵ As AI systems become more powerful and accessible, licenses act both as a shield and leash: they restrict harmful or unauthorized usage while permitting valuable use cases.⁷⁶

Why licensing fills the gaps in AI Protection

While patents offer exclusivity, they are difficult to obtain due to algorithmic abstraction and the legislative exclusions, like section 3k of the Patents Act in India, or the Alice doctrine in the USA. Trade secrets laws provide protection through confidentiality, but are vulnerable to reverse engineering and are still underdeveloped. Licensing as a complementary tool fills these gaps by binding users through enforceable terms, offering flexibility without requiring disclosure, and enabling cross-border enforceability via contract law. Licensing covers not just

⁷³ Dep’t-Related Parl. Standing Comm. on Com., *161st Report on the Review of the Intellectual Property Rights Regime in India*, Rajya Sabha (Jul. 2021), https://rajyasabha.nic.in/rsnew/Committee_site/Committee_File/ReportFile/13/143/161_2021_7_15.pdf.

⁷⁴ Kevin M. Pasquinelli, *Adapt Your IP Strategy for Artificial Intelligence*, 2 THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (FASTCASE) 389 (November-December 2019).

⁷⁵ Montreal AI Ethics Institute, *Responsible AI Licenses: Social Vehicles Toward Decentralized Control of AI*, MONTREAL AI ETHICS INST. (July 18, 2023), <https://montrealaiethics.ai/responsible-ai-licenses-social-vehicles-toward-decentralized-control-of-ai/>.

⁷⁶ Kevin M. Pasquinelli, *Adapt Your IP Strategy for Artificial Intelligence*, *supra* note 72, at 10.

the code but the trained model weights, APIs, interfaces, and use cases,⁷⁷ especially when it's difficult to classify AI Algorithms under traditional IP categories.

Three Types of Licensing Paradigms

1. Open source licenses—valuable but vulnerable

Licenses like Apache 2.0 or MIT have traditionally fostered collaborative software development and attracted many ML developers due to their simplicity.⁷⁸

However, these licenses were not intended for the nuanced functionality, opacity, and dual-use potential of AI algorithms. They allow unrestricted copying, usage, and modification of code or models, which can lead to misuse in areas such as surveillance, disinformation, and discriminatory profiling.⁷⁹ Although open-source code is protected by copyright, the underlying algorithm, as an idea or method, is not.⁸⁰ Thus, once the model weights or logic are publicly shared under an open license, they may be irreversibly exposed without recourse for the licensor.

2. Enterprise Licenses – Trade Secret + Contractual Control

Under the enterprise licenses, the AI Model usage is limited within a particular enterprise⁸¹. Open AI best exemplifies this kind of licensing by incorporating highly specific terms of use, including confidentiality provisions, non-compete clauses, and anti-reverse engineering clauses.⁸² An example of enforcing these terms is seen in the U.S. case, *Triage Logic Mgmt. & Consulting, LLC v. Innovative Triage Services*. Here, a North Carolina court upheld a licensing clause banning reverse engineering, showing that courts might accept such contractual terms as valid even beyond typical intellectual property contexts.⁸³ Conversely, courts in some areas,

⁷⁷ The Turing Way Community, *Licensing Machine Learning Models*, in *The Turing Way: A Guide to Reproducible Research* (Alan Turing Institute 2024), <https://book.the-turing-way.org/reproducible-research/licensing/licensing-ml>.

⁷⁸ Montreal AI Ethics Institute, *Responsible AI Licenses: Social Vehicles Toward Decentralized Control of AI*, MONTREAL AI ETHICS INST. (July 18, 2023), <https://montrealethics.ai/responsible-ai-licenses-social-vehicles-toward-decentralized-control-of-ai/>.

⁷⁹ *Id.*

⁸⁰ *The Turing Way*, *supra* note 75, at Licensing Machine Learning Models.

⁸¹ Kevin M. Pasquinelli, Adapt Your IP Strategy for Artificial Intelligence, 2 THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (FASTCASE) 389 (November-December 2019).

⁸² Camilla A. Hrdy, *Keeping ChatGPT a Trade Secret While Selling It Too*, 40 Berkeley Tech. L.J. 75, 84–85 (2025).

⁸³ *Triage Logic Mgmt. & Consulting, LLC v. Innovative Triage Servs.*, No. 22 CVS 8132, 2023 WL 4531206 (N.C. Super. Ct. June 15, 2023).

like California, have deemed perpetual non-compete clauses as unenforceable due to being unreasonable restraints on trade.⁸⁴ In the case of OpenAI, the business terms are designed to protect trade secrets while allowing extensive use, illustrating how licenses can uphold proprietary advantages without revealing the underlying algorithm.⁸⁵ Users who misuse the license or exceed its limits risk violations of both contract and trade secret laws.

3. Responsible AI Licenses (RAIL) – Ethical and Legal Innovation

Rail and OpenRAIL licenses have brought an evolution in the licensing of AI models. They balance openness and responsibility by incorporating use-based restrictions, for example, banning use for surveillance, health insurance scoring, or automated criminal profiling, into the license itself.⁸⁶ While open-source licenses provide a similar treatment to AI models and software code⁸⁷, RAIL licenses treat them distinctly and incorporate clauses on model weights, training data, and interface restrictions.⁸⁸ The use restrictions are passed from user to user and thereby creating a chain of responsible use down the line.⁸⁹ These obligations can travel along with the AI artifact, regardless of jurisdiction, helping cross-border enforcement. According to the Montreal AI Ethics Institute, the “community norms” set by these licenses provide not just moral suggestions but also legal enforceability to ethical use of AI.⁹⁰

Licensing as a Strategic Complement

Licensing does not replace patents or trade secrets; it enhances them. When patents are unavailable or enforcing trade secrets is difficult, licensing offers a contractual mechanism for safeguarding and managing rights. Through enterprise-level agreements and community-based licenses like RAIL, licensing enables developers to enforce responsible and jurisdiction-

⁸⁴ Hrdy, *supra* note 81, at 84–85.

⁸⁵ *Id.*

⁸⁶ Kevin M. Pasquinelli, *Adapt Your IP Strategy for Artificial Intelligence*, *supra* note 80, at 11.

⁸⁷ Montreal AI Ethics Institute, *Responsible AI Licenses: Social Vehicles Toward Decentralized Control of AI*, MONTREAL AI ETHICS INST. (July 18, 2023), <https://montrealetics.ai/responsible-ai-licenses-social-vehicles-toward-decentralized-control-of-ai/>.

⁸⁸ *Id.*

⁸⁹ The Turing Way Community, *Licensing Machine Learning Models*, in *The Turing Way: A Guide to Reproducible Research* (Alan Turing Institute 2024), <https://book.the-turing-way.org/reproducible-research/licensing/licensing-ml>.

⁹⁰ Montreal AI Ethics Institute, *Responsible AI Licenses: Social Vehicles Toward Decentralized Control of AI*, MONTREAL AI ETHICS INST. (July 18, 2023), <https://montrealetics.ai/responsible-ai-licenses-social-vehicles-toward-decentralized-control-of-ai/>.

⁹⁰ *Id.*

independent controls over AI system access and use.

In India, the patentability of AI algorithms is limited by section 3(k),⁹¹ And there is no statute on trade secret law.⁹² licensing can become an effective interim strategy. Although India doesn't have a developed licensing framework for algorithms, the standards followed by the US firms can be encouraged, particularly the anti-reverse engineering, ethical use, and nondisclosure provisions. This can help to close the protection gap until India develops a robust IP regime. Thus, licensing can serve as an important cornerstone in India's journey towards a hybrid protection system for AI.

Policy suggestions for India

Reforming Indian Patent Law for Algorithmic Innovation

India should retain its existing CRI framework, but should provide more clarity on terms like "algorithms", "technical effect," and "technical contribution" through statutory definitions to reduce ambiguity in interpretation. Section 3k of the patent act, which through its exclusion of "mathematical methods, algorithms, and computer programs per se"⁹³ Impose a blanket rejection on AI-based innovations needs to be amended. It should be narrowed or clarified to ensure that AI algorithms offering genuine technical advancements are not inadvertently excluded. Sector-specific guidelines need to be issued on when machine learning techniques can amount to a "technical contribution". Case-by-case assessment focusing on novelty, industrial application, and technical effect rather than rigid exclusions needs to be encouraged.

Strengthening Trade Secret Protection in India

A formal statute or guidance providing a clear definition of trade secret and what constitutes a trade secret is needed, which should align with global norms like Article 39 of the TRIPS agreement⁹⁴ And EU Trade Secrets Directive (2016/943).⁹⁵ Since trade secrets are automatically protected, a statute on registration may not be needed, but remedies such as

⁹¹ Ferid Allani v. Union of India, 2019 SCC OnLine Del 11867

⁹² Law Comm'n of India, *Report No. 289: Trade Secrets and Economic Espionage* (Mar. 17, 2024).

⁹³ Agreement on Trade-Related Aspects of Intellectual Property Rights art. 39, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299.

⁹⁴ Directive 2016/943 of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure, 2016 O.J. (L 157) 1.

⁹⁵ The Patents Act, No. 39 of 1970, § 3(k), India Code (1970).

injunctions, damages, and evidentiary safeguards need to be codified to address misappropriation. It should include exceptions for disclosure on grounds like public interest, regulatory compliance, or whistleblowing, to address genuine transparency concerns. A recognition-based framework would improve legal certainty and promote innovation in algorithm-centric sectors like AI, where confidentiality is crucial for protection.

Encouraging Licensing Standards for Algorithmic Protection

Licensing of algorithms is mainly an industry-led area, where new licenses like RAIL and MIT are developed by industry stakeholders with little or no involvement of the government. Government, in collaboration with industry and academia, can help develop new licensing templates that keep up with the complexities of AI systems. Government bodies like DPIIT and MeitY can still issue non-binding model guidelines recognising licensing as a complementary tool to protect algorithms. Recommendation of baseline standards, such as scope of use, sublicensing limits, and termination clauses, can help promote consistency and enforceability. Recognising licensing as a practice in the official policy framework would improve certainty when statutory patent and trade secret protections for algorithms remain limited.

Recognizing Hybrid IP Protection as a Policy Norm

In addition to reforms in individual IP regimes, policymakers should acknowledge the reality of hybrid protection models in AI innovation. Government bodies like DPIIT or MeitY can issue non-binding guidelines that recognize layered protection, e.g., where trade secrets, patent claims, and licensing terms operate together. Such recognition would help the patent offices and courts to approach these algorithmic assessments more comprehensively. While a formal statute may not yet be feasible, recognising hybrid protection in policy papers can promote doctrinal clarity, prevent fragmented adjudication, and provide legal certainty to developers and rights holders navigating India's evolving AI ecosystem.

Practical guidance for developers

1. Use the Right IP Tool for the Right AI Component

Developers should align each part of their AI system with the most appropriate IP strategy:

- Source code: Register under copyright (as a literary work).
- Trained model weights, architecture, and fine-tuned outputs: Protect as trade secrets, using internal controls, limited access, and NDAs.
- Novel algorithmic innovations: If they demonstrate technical effect, have an industrial use, or are linked to external hardware, patents should be explored.
- Non-patentable but commercially valuable AI systems: Protect using enterprise licensing agreements, focusing on usage control and confidentiality.

This approach ensures layered and flexible legal protection, which is enforceable while being component-sensitive.

2. Adopt Strong Licensing and Trade Secret Practices

Until India has a stronger IP framework, developers should reinforce protection through contract clauses and licensing.

- Use enterprise-level licenses with:
 - Usage limits
 - Anti-reverse engineering clauses
 - Anti-redistribution terms
 - Clear IP ownership over improvements and outputs
- Maintain confidentiality via:
 - Strong NDAs
 - Access control systems
 - Model/API obfuscation in cloud-hosted deployments
- Keep logs and documentation to prove independent development, which would help in

proving originality or trade secret misuse.

Conclusion

The objective of this paper was to examine how the existing frameworks for the protection of AI Algorithms in India, the US, and the EU are inconsistent and fragmented. By a comparative analysis, it has been shown that while Patent trade secrets and licensing models provide partial protection, they are insufficient to address the legal, technical, and ethical challenges posed by algorithmic systems. The Indian laws particularly suffer from the definitional ambiguity under Section 3(k), lack of statutory recognition of Trade secrets, and absence of official policy frameworks for licensing AI artifacts. The analysis shows that industry actors are already informally using hybrid models, relying on trade secrets to protect secrecy, licensing for access and control, and patents when there is a technical contribution. Still, the formal legal doctrines and policy haven't recognised this practice, creating an ambiguity in enforcement and investment. This paper therefore advocates that India should adopt a protection strategy that (a) reforms existing statutory exclusions, (b) establishes a recognition-based framework for trade secrets, and (c) issues guidelines for model licensing that support responsible use. However, these stand-alone legal reforms are not enough. More research is needed to explore the criteria under which algorithms should qualify for protection, particularly in determining what constitutes sufficient novelty, industrial application, or technical contribution. These standards must be able to balance the responsible use and transparency concerns with incentivizing and protecting genuine innovation. As India navigates this critical phase of AI policy development, a hybrid, flexible, and context-aware IP framework will not only ensure alignment with international practices but also create a legally secure environment for algorithmic innovation to thrive.