# TRADE SECRETS IN THE AGE OF GENERATIVE AI: RETHINKING CONFIDENTIALITY, CONTROL, AND COMPETITIVE ADVANTAGE

Arghyadip Choudhury, Presidency University, Bangalore

**ABSTRACT**

Such ever-increasing integration of commercial and industrial ecosystems with accelerating and advancing generative artificial intelligence (AI) has greatly upset the traditional intellectual property paradigm particularly the doctrine of trade secrets. Trade secrets, unlike patent or copyright, have their legal protection based on secrecy and the reasonable efforts used to maintain such secrecy. Nonetheless, systems of generative AI, which are characterised by the ingestion of large quantities of data, probabilistic inference, and autonomous generation of output present previously unseen challenges to this doctrine. These systems augment the threat of unintentional disclosure, leak of information as well as algorithmic reproduction of confidential information, thus undermining the impact of traditional safeguards.

The paper critically assesses the effect of generative artificial intelligence on the protection of trade secrets focusing on the absorption of secrecy and the poor fit of the current legal frameworks and the negative outcome of the development of new forms of misappropriation, such as indirect and data-driven extraction of proprietary information. Through an analysis of statutory frameworks like the Defend Trade Secrets Act (DTSA), the EU Trade Secrets Directive, and the Indian legal position, the paper identifies important doctrinal gaps in strategies to help overcome AI-related risks, especially concerning the attribution of liability, the challenges of proving, and cross-border data flows.

The research also stresses the necessity of modifying, based on changing technology actualities, key legal concepts like, but not limited to reasonable measures; and: misappropriation. It advocates a re-conceptualization of trade secret law, which incorporates technological protective measures (e.g. secure AI architectures), organizational governance (e.g. internal AI policies), and being able to adaptively adjust regulation. Finally, the paper ends by concluding that trade secret protection needs to change into a hybrid legal-technological frame, which would guarantee the protection of confidential business information, as well as the ongoing promotion of innovation in the AI-driven economy.

**Keywords:** Generative Artificial Intelligence; Trade Secrets; Intellectual Property Law; Confidential information; Misappropriation; Data leakage; Reasonable measures; AI Regulation; Legal Frameworks; Defend Trade Secrets Act; EU Trade Secrets Directive; Indian Law; Information Governance; Technological Safeguards; Hybrid Legal Model.

## 1. Introduction

Traditionally, the theory of trade secrets has been based on a very consistent conception of control and secrecy. Digital and industrial economies alike have succeeded in being effective when using this method. However, with the emergence of generative AI, this balance was disrupted because a number of new means of processing, delivering and inferring information have been introduced[1].

Examples of generative AI systems that are, in effect, data-driven include large language model and neural networks. Large datasets, frequently from both public and private sectors, must be ingested and processed in order for them to function.[2]Trade secret law, which depends on limiting access to information, is structurally at odds with this[3]. When used in entering personal information into AI systems, either intentionally or accidentally, the information will be processed, stored, and it may also be duplicated, which will compromise the confidentiality thereof.

This is not only a theoretic issue. Recent reports have contributed to significant legal concerns[4], because the information of the trade secrets shared with other parties through trade secret AI tools could be concealed and lost protection.

The overall research question of this paper is thus the following: Can trade secret law, as it currently stands, do a good job in protecting confidential information in the era of generative AI?

## 2. Conceptual Foundations of Trade Secret Law

Trade secret law occupies special place in the environment of the intellectual property law. Trade secrets protect knowledge because, unlike patents, trade secrets are kept confidential,

[1]Sheppard Mullin, The AI Knows Too Much (2026)
[2]Deloitte, Generative AI Legal Issues (2024).
[3]Id.
[4]Reuters, Trade Secret Litigation Surges (2026).

without requiring any disclosure as a prerequisite to the exclusivity. This creates a contradiction: the usefulness of a trade secret must be its inaccessibility.

In the Defend Trade Secrets Act (DTSA)[5], a trade secret is defined as information that (1) has an independent economic value that it would not have in the absence of its secrecy (i.e. it is notgenerally known or easily discoverable) and (2) is the subject of a reasonable effort to keep it confidential (i.e. it is not generally known or easily discovered)[6].

Courts have stressed the point that it is not necessary that absolute secrecy was being taken steps to which it is a focus to discover whether they have undertaken steps that were reasonable under the circumstances[7].

The development of generative AI, however, provokes a challenge to this norm. And in an environment where data can be immediately transmitted to AI systems over which the owner has no control, what does it mean by light Speed when referring to reasonable efforts? This question is the focus of the current doctrinal challenge[8].

### 3. Generative AI and the Erosion of Secrecy

Generative AI alters the definition of secrecy immensely by introducing tools that enable the indirect disclosure/reconstruction of sensitive information. Unlike other traditional databases, AI systems do not simply store data, but also analyze the patterns and generate outputs that can reveal underlying data structures.

This presents a very grave risk whereby any personal information typed into an AI platform might be recreated in a type of feedback of outputs that other individuals can access as well. Research has shown that, in some circumstances, machine learning models are capable of memorizing and repeating training data.[9]

It also compromises the privacy of personal information because effectively the latter is made a part of a bigger dataset.

[5]18 U.S.C. § 1839(3).
[6]18 U.S.C. § 1839(3) (Defend Trade Secrets Act).
[7]Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1974)
[8]Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174 (7th Cir. 1991).
[9]Nicholas Carlini et al., Extracting Training Data from Large Language Models (2021).

Courts begin to realize and admit this hazard. Legal commentary would interpolate entering trade secrets into an AI system, where protective measures are insufficient, as a theft of confidentiality and the loss of protection[10].

**4. Inadvertent Disclosure and Employee Liability**

Unintentional disclosure is one of the largest issues that are related to generative AI. AI tools are widely used by employees to increase productivity, usually without considering the legal ramifications of their activities.

The debugging and optimization of an AI system are an example of this. An example is an employee typing proprietary code[11]. Although such could appear as innocuous, it actually provides a third party with access to confidential information.

Historically, the courts have adjudicated that the protection of trade secrets is lost once the information is disclosed to a third party without confidentiality considerations.[12]Since many AI systems do not come with strong guarantees of confidence, this principle presupposes new importance in AI.

The employers can also be liable to neglect the proper safety measures[13]. This is encompassed not just in technological actions but also in organizational policies and training programs.

**5. Reverse Engineering and AI Inference**

As long as it doesn't include unethical behavior, reverse engineering has been acknowledged as a legitimate way to obtain information.[14] On the other hand, reverse engineering proprietary processes is much improved by generative AI[15].

The protection of trade secrets on the basis of the inability to identify the information is negated by this.

There are significant legal ramifications. Trade secret protection can severely be reduced in

[10]Jones Day, Trade Secrets and Generative AI (2023).
[11]Sheppard Mullin (2026).
[12]Ruckelshaus v. Monsanto Co., 467 U.S. 986 (1984).
[13]Winston & Strawn LLP, Best Practices for Trade Secret Protection (2025).
[14]Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141 (1989).
[15]Greenberg Traurig (2025).

case the AI can replicate the patented procedures without having to access the confidential information.

**6. Redefining "Reasonable Measures" in the Age of Generative AI**

Companies should now adopt the state of the art such as:

- AI-specific confidentiality policies
- Ultimate regulations on how AI public platforms are used.
- Implementation of safe, enterprise-level AI instruments.
- Data flows constant monitoring[16].

The inability to implement such actions can lead to the loss of the trade secret protection.

Any measures that can be deemed as reasonable with regards to the trade secret law (confidentiality agreements, limited access and simple cyber protection) have been becoming increasingly insufficient in the context with generative AI. The AI systems bring about novel data processing, storage, and dissemination forms, which are greatly increasing the exposure to unintentional disclosure. As a result, the legal standards of what is to be regarded as reasonable efforts is becoming more technology-based, risk-sensitive and thus taking a different reform line.

Firms are now forced to deal with AI specific security that extends beyond the common practice. Firstly, AI-related confidentiality policies need to be created. These policies should clearly regulate employee use of generative AI-related applications, including prohibiting the submission of trade secrets to third-party/unverified systems. In the absence of such policies, organizations are likely to be considered as having poor control of their confidential information.

Second, stringent limitations of the public AI platforms use have to be in place. Many generative AI providers process user data in a way that may transfer or store sensitive data, which can further trade secrets. This means that companies will either ban such use of sensitive

[16]Winston & Strawn LLP, Best Practices for Trade Secret Protection (2025).

information or put in place control access measures.

Third, organizations ought to invest in safe and enterprise level AI systems. The systems may be designed to have the built-on security measures in terms of information isolation; encryption; and controlled training environments, thus the chances of information leakage are minimized.

Fourth, data flow monitoring and auditing has become a crucial need. This involves monitoring data utilization in AI training, identifying abnormal data access patterns, and ensuring that any outputs do not unintentionally reveal confidential data. This kind of monitoring Not only is proactive risk management, but is also effective in reinforcing reasonable protection claims.

## 7. Misappropriation in the AI Context

Generative AI has given rise to new forms of trade secret misappropriation that cannot be easily defined by the strict terms and forms found in the more traditional provisions of the law. One of them is the automated data scraping [17]where AI-based systems gather a lot of publicly available information, which may unintentionally include confidential or proprietary information. Self-scraping may be legal in some situations but when applied in training models that may in turn replicate or utilize sensitive information, it raises serious questions on matters of legality.

The other new form is the illegal use of the results that are generated by AI using hidden inputs. Even with proprietary business data (e.g. the outputs of the system fed with the proprietary data) may still constitute trade secrets. This poses a legal dilemma of whether such outputs are a derivative misuse or disclosure especially when done to make a commercial gain.

Secondly, there has been a high vulnerability of leakage through training datasets. Confidential data may be used in the models trained with mixed or under-vetted data, and can be then recovered by making use of prompts or reverse-engineering. This disputes the traditional aspect of demonstrating direct copying or deliberate misappropriation.

By subjecting the technologically complex cases to the application of the established legal principles, mainly those, which relate to breach of confidence and improper means, courts have

[17]HiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985 (9th Cir. 2019).

begun tackling the issues. The fact that the legal approach to cases remains largely case-focused demonstrates that the lack of specific, AI-centered legal norms.

## 8. Comparative Legal Frameworks

Generative AI: laws of jurisdictions vary in the treatment of trade secrets, due to differences in statutory treatment, judicial interpretation and regulatory objectives. Though the majority of those systems have a similar goal - securing trade secrets - the results vary by the system. Although convergence on core tenets between the United States, the European Union and India is found; there is a discrepancy on regulatory sophistication[18].

Nonetheless, India does not have a special trade secret law, so there is a risk of uncertainty when it comes to AI.

### 8.1 United States: Statutory Strength with Emerging Gaps

Protects the trade secrets of businesses, the Defend Trade Secrets Act (DTSA) the United States. This is a civil lawsuit under which a trade secret can be misappropriated in a federal court. The DTSA supplements the state laws against the misappropriation of the trade secrets that have been modelled mostly on the Uniform Trade Secrets Act (UTSA). Under this Act there are remedies available with the main remedies being an injunction over further use and a further disclosure of the trade that is covered by this Act.

The U.S. framework has generally been regarded as strong because it clearly defines a trade secret, lays emphasis on the concept of reasonable measures needed to keep a trade secret confidential, and has a well-developed jurisprudence. Nonetheless, generative AI reveals a number of shortcomings:

- Various rulings of the DTSA show that the owner of a trade secret who fails to establish how he or she acquired or used the information will be deprived of a misappropriation claim. The legislation offers relief on possession, use or knowledge by a party.

- It may be challenging to demonstrate that it was misappropriated in the case of a trade secret such as AI models and algorithms. This is because AI systems are used as a black

[18]Directive (EU) 2016/943.

box, and it is difficult to demonstrate that an AI.

- Accompanied is the utilization of off-the-shelf generative AI tools: The adoption of all the outside generative AI phase has been further extended. Even though they may be used by organizations during the review processes, it remains unknown whether it is appropriate to transmit confidential and sensitive information to such sites.

There are indeed some gaps in the U.S.A but one should never underrate the ability of American judge to suit the doctrine to the current case. The Courts have often not refused to apply a current law on the ground that the new challenge being technologically driven with the refusal to do so.

### 8.2 European Union: Harmonization with a Focus on Lawful Acquisition

The EU directive on trade secrets also brings in the legislation on trade secrets in the entire European Union. According to the EU Directive a trade secret is the information that possesses the following characteristics: it is secret; it has commercial value because it is secret; and the person over whom that information is maintained takes.

The importance of lawful possession and use is noteworthy in the EU context. The Directive authorizes some legitimate activities like reverse engineering, independent discovery and public observation. The implications as to generative AI are important:

- Training on publicly accessible data: AI developers in the EU can take into consideration the principle of legal acquirement to justify training models on publicly accessible data, even when such information indirectly contains sensitive information[19].

- Making trade waistful, both innovative and protective: The EU policy reflects a larger policy agenda of both achieving innovation and providing protections to proprietary interest and especially within the digital economy.

- Interaction with data protection law: The General Data Protection Regulation, creates highly stricted requirements on the usage of personal data in AI systems. This puts in

[19]HiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180 (9th Cir. 2022).

place a stratified compliance model in which the protection of trade secrets needs to coexist with the privacy requirements.

Unlike the U.S., however, the EU framework has not yet fully considered the risks related to AI, including but not restricted to model memorization or algorithmic leakage. The lack of specific provisions to such issues makes forming an interpretation a challenge, though the current policy efforts (like the EU artificial intelligence regulation efforts) can potentially help fill such a gap.

### 8.3 India: Fragmented Protection and Regulatory Uncertainty

Unlike U.S. and EU, India lacks a specific trade secret law. A combination of the contract law, the equitable principles, and the common law doctrines, especially those that deal with breach of confidence[20], furnish protection. Trade secrets have been regarded by the courts as confidential information and have provided relief in such cases where there is unauthorized disclosure or misuse.

The lack of a codified framework gives rise to certain challenges:

- The absence of a uniform definition of a trade secret and standard remedies: Varied judicial results: unlike in the DTSA or EU Directive, no uniform definition of a trade secret and standardized remedies exist in India, leading to inconsistent judicial decisions.

- Relying on contractual processes: Protection can be based on non-disclosure agreements (NDAs), employment agreements, and confidentiality clauses, which might not be adequate in more sophisticated AI setting.

- Insufficient jurisprudence on AI-related cases: The Indian judiciary has not yet established a significant mass of judicial cases addressing the overlap of trade secrets and generative AI, leading to legal uncertainty among business.

Such uncertainty is especially problematic in an AI context, where data ownership, data flows across territories, and accountability of algorithms are in the limelight. Although larger

[20]Saltman Eng'g Co. v. Campbell Eng'g Co. (1948).

regulatory frameworks, including the Information Technology Act 2000, offer some protection against data anonymity and some trade secret misappropriation in AI systems, they do not directly address any of the three issues of data anonymity, trade secret misappropriation, and cybersecurity oversight in AI systems.

However, legal system in India provides a certain flexibility as it is based on fair principles. Courts can also restrain to existing doctrines to find solutions to new challenges of technology, but this would not have the predictability and coherence of a specific statute. An increasing number of calls have been made to regulate the laws to bring in a comprehensive law on trade secrets in line with international standards.

### 8.4 Comparative Insights and Emerging Convergence

Comparative evaluation shows that there is a number of important things to be known:

- Unification of principal principles: In all three jurisdictions, the basic core of OTS is convergence in fundamental principles.

- Difference in regulatory specificity: The United States and Europe have well-structured forms of statutory regulation, whereas India uses a fragmented and case-specific approach to regulation.

- Common challenge in AI adaptation:Not a single jurisdiction has completely worked out the legal implications or generative AI, specifically, the legal issues of data training, model outputs, and indirect misappropriation.

Moving ahead, the necessity to harmonize internationally and provide legal advice for AI purposes grows. As AI systems interact at the international level, national differences in policies may lead to a regulatory arbitrage, enforcement challenges, and weakening incentives to innovate. An international strategy, possibly through international bodies or model laws, may contribute to developing clearer principles of the protection of trade secrets in the AI era.

## 9. Corporate Governance and Risk Management in the Age of Generative AI

The present AI economy has serious implications for protection and enforcement of trade secrets. The protection of trade secrets is no longer merely a compliance issue; rather, it is now

a fundamental corporate governance and enterprise risk management function. Generative AI systems create new possibilities and risks, especially with the processing of a lot of data and the outcome they generate. Firms will have to implement integrated multi-layered governance frameworks with strong legal, technological and organizational controls which secure confidential business information throughout its life-cycle.

This includes developing AI usage policies, implementing secure AI systems, and conducting regular audits.[21]

### 9.1 Governance as a Strategic Imperative

Within the AI context, corporate governance reaches further than old ways of watching over things because corporate governance must include careful looking at information possessions, mathematical sets of rules, and electronic task sequences. Groups of governing directors and high ranking leadership individuals are now called upon to take a working position where AI-related risks are watched by them. Experts claim that these AI-related risks involve things like revealing secret business knowledge, digital attacks, and failing to follow the laws. Such a movement shows a bigger change where people see information and AI models as very important company riches because protecting these AI models is needed for a company to keep its superior market standing.

A well-designed governance structure typically includes:

- **Board-level accountability** for AI and data governance,
- Designation of specialized roles such as Chief Information Security Officers (CISOs) or AI compliance officers,
- Integration of trade secret protection into enterprise risk management (ERM) frameworks.

### 9.2 Legal and Policy Frameworks within Organizations

At the organizational level, corporations need to create effective and implementable internal

[21]Deloitte, Generative AI Legal Issues (2024).

policies to regulate the use of generative AI. Such policies must deal with:

- **Permissible and prohibited uses of AI tools**, particularly restrictions on inputting confidential or proprietary information into external platforms,
- **Data classification protocols**, distinguishing between public, internal, confidential, and trade secret information,
- **Contractual protections, such as non-disclosure agreements (NDAs), confidentiality clauses in employee contracts, and vendor agreements between AI service providers and their clients,**
- **Governance alignment with the relevant legislations in place in the country such as the law related to Information Technology e.g. The Information Technology Act 2000.**

These policies should be dynamic and periodically reviewed to accommodate changing technological abilities and regulatory changes.

### 9.3 Technological Safeguards and Secure AI Systems

The mitigation strategy of the threat of generative AI mainly relies on technological interventions. Companies need to ensure the use of state-of-the-art security controls to prevent unauthorized access, misuse or leakage of trade secrets. Key safeguards include:

- **Access control mechanisms** (role-based access, multi-factor authentication),
- **Encryption of data at rest, in transit, and in use**,
- **Secure AI development environments**, ensuring that training data and models are protected from external intrusion,
- **Privacy-preserving techniques** such as differential privacy and federated learning,
- **Output monitoring systems** to detect and prevent unintended disclosure of sensitive information.

Importantly, these measures are increasingly being considered part of the **"reasonable efforts"**

**requirement** under trade secret law, meaning that failure to implement them could weaken legal protection.

### 9.4 Risk Assessment and Audit Mechanisms

One of the most important aspects of corporate governance is the creation of ongoing risk evaluation and audit program. Organizations should actively determine vulnerabilities on their AI systems and data management practices. This includes:

- **Regular internal audits** of AI systems and data flows,
- **Third-party risk assessments**, particularly when relying on external AI vendors or cloud service providers,
- **Impact assessments** to evaluate the potential exposure of trade secrets during AI training and deployment,
- **Incident response planning**, ensuring that organizations can quickly respond to breaches or suspected misappropriation.

Audits should not be limited to technical systems but should also evaluate **employee behavior, policy compliance, and organizational culture**, as human factors remain a source of risk.

### 9.5 Employee Training and Organizational Culture

Human error remains among the greatest of trade secret leak of all, especially in the application of generative AI tools. By typing in confidential data into AI applications without knowledge of what involves risks, the employees may happen to disclose confidential data. In an attempt to respond to this, organizations have to invest in:

- **Comprehensive training programs** on AI usage and data protection,
- Clear communication of policies and consequences for non-compliance,
- Development of a **culture of confidentiality and security awareness**.

Such initiatives not only reduce risk but also strengthen the organization’s ability to demonstrate that it has taken reasonable steps to protect its trade secrets.

### 9.6 Integration with Enterprise Risk Management (ERM)

Trade secret protection in the AI era must be embedded within broader **enterprise risk management frameworks**. This involves:

- Identifying AI-related risks as a distinct category within ERM,
- Quantifying potential financial and reputational impacts of trade secret breaches,
- Aligning risk mitigation strategies with overall business objectives.

By integrating AI governance into ERM, organizations can move from a reactive to a **proactive risk management approach**, anticipating threats before they materialize.

### 9.7 Toward a Holistic Governance Model

In the end, AI-based corporate governance needs to be interdisciplinary and holistic. Legal compliance, technological security and organizational practices are no longer independent but they have to work together. Businesses that effectively combine them will be in a better place to keep their trade secrets safe and might take advantage of the benefits of generative AI.

## 10. Emerging Trends and Litigation

According to the new trends[22], courts seek to determine the appropriateness of security measures, in part, due to the shift to remote work and the use of AI.

One of the major occurrences within the current law context is that the number of trade secret cases which involve the theft of digital assets illicitly has risen considerably[23]. According to legal experts, the juridical institutions are frequently shown with legal contradictions of ownership to the proprietary datasets, training models, or algorithmic architecture. It is thought that the particular models were accessed or copied by other systems using AI in an inappropriate way. Such trade secret litigation actions usually occur due to using of some information without consent by rival enterprises[24]. These AI legal suits are unlike theft in history since historical theft typically included physical pieces of paper or facts that can be

[22]Legal AI Beat (2026).
[23]Reuters, Trade Secret Litigation Surges (2026).
[24]E.I. duPont de Nemours & Co. v. Kolon Industries, Inc., 637 F.3d 435 (4th Cir. 2011).

easily viewed. Since AI conflict involves non-physical and probability-based things, the principles of demonstrating the truth in court are becoming more challenging and highly controversial. It can be noted that the intricacy of such cases becomes more complicated by virtue of the fact that the character of information is challenging to determine. The law is frequently perceived to be less reliable as compared to the physical evidence, and so the legal consequences of these AI cases are often viewed as less definitely followed in court than the physical evidence.

The law is taking a new turn in terms of juridical questioning of what ought to be done, in reasonable manner, to protect trade secrets by organizations. In the context of AI, the legal community assert that this standard experiences transformation since now reasonable measures involve a set of basic access control tools such as non-disclosure agreements and access restrictions with a complex array of potentially sophisticated technical procedures. These advanced technical lifecycle comprises encryption protocols, secure data pipelines, audit logs, and model governance frameworks. It is also noted that judicial authorities are unwilling to provide legal protection when companies are not putting in place serious cybersecurity and data management practices. This safeguarding is not guaranteed especially when there is sensitive information contained in artificial intelligence trainings.

With an increasing number of employees working remotely and using the cloud to collaborate with business partners or clients, proprietary information is often accessed over unsecured networks on personal devices, which has led to a dramatic increase in lawsuits related to downloading, copying, transferring, or otherwise accessing proprietary information. In several recent cases, courts have considered endpoints, monitoring systems, and employee compliance programs to be part of a trade secret owner's "reasonable efforts."[28]

More generally, although judicial precedents are not actively tested in court, it seems more probable that the courts would resolve such cases on a fact-specific and risk-based test depending upon the kind of data involved, how the model was trained, and whether the leakage could reasonably be foreseen[25].

Moreover, a new wave of controversies around employee usage of third-party AI services has begun, including publicly accessible generative AI applications. These systems allow

[25]Sharon K. Sandeen & Elizabeth A. Rowe, Trade Secret Law in a Nutshell (West Academic, 2023).

employees to enter confidential business information so as to improve on productivity, unintentionally exposing trade secrets to other servers or model training. This has led organizations to adopt stringent internal policies governing the use of AI, and courts are already starting to take into consideration whether a failure to control such use amounts to a failure to uphold secrecy[26].

## 11. Critical Analysis: Trade Secrets in the Era of Generative AI

The rise of generative artificial intelligence is a paradox to the traditional mechanisms of creating proprietary value: it both diminishes the traditional mechanisms of producing proprietary value and also destroys the prospect hitherto unknown before the emergence of generative artificial intelligence. This duality is to be criticized using critical imagination of current doctrine of law, its limitations, and multiple avenues of the changes.

Generative AI expands the trade secret risk landscape. The use of proprietary trade secret materials to train large language model (LLMs) and generative image models presents novel trade secret risk that is difficult to track and manage. Additionally, as AI data storage is maintained for much longer as statistics, it can be difficult to ascertain whether any particular trade secret was imbedded, transformed, or recoverable. This brings about a situation where organizations might lose meaningful control over their proprietary information without any clear act being an event of intentional disclosure. The lack of proper disclosure in generated outputs in disaggregative or approximative form also creates problems since sensitive data may re-emerge in outputs generated by the model in fragmented or approximated versions and pose challenging questions on what is disclosure under the trade secret law[27].

Concurrently, AI capable of producing new things is not only a ubiquitous source of woe - it's also a powerful resource to create new secrets that companies would wish to keep under wraps. They assist companies in creating very valuable assets that only are valuable, such as special sets of data that they use to train their systems, the best way to build their models, the specific settings they use, and the specific results they obtain out of their systems. What makes these assets valuable is that they are kept as trade secrets; they are unknown to anyone except those who own them and hence trade secret legislations are enacted to prevent the loss of such assets. This way, we are changing our perception about a trade secret and going beyond things such

[26]Epic Systems Corp. v. Tata Consultancy Services Ltd., 980 F.3d 1117 (7th Cir. 2020).
[27] *E.I. duPont de Nemours & Co. v. Kolon Industries, Inc.*, 637 F.3d 435 (4th Cir. 2011)

as recipes, methods and customer lists, to how algorithms are configured, and what we can learn about data[28].

The growth of artificial intelligence is revealing some major flaws in our current laws. Trade secrets laws, such as the Defend Trade Secrets Act or the TRIPS Agreement, traditionally were based on a few key ideas; namely, that it is simply known to whom trade secrets belong, that it is easy to know whom the owner of trade secrets is, and that people are making decisions about what happened to the information about the owner of trade secrets[29]. However, today with artificial intelligence that has the capacity to create new things, these notions no longer really hold. It is not evident as to who owns anything when lots of people have contributed to making the AI model; and the fact that the AI is only making guesses and producing new things based on what it has learned is problematic.

There is a huge issue as far as we treat misappropriation, that is, when a person takes something that is not his/her. In most instances we have to demonstrate how someone received something in a manner other than was intended or received a confidence which was later broken. However, in the case of artificial intelligence, it becomes tricky. In some cases more importantly misappropriation may occur without anyone noticing, such as when AI is trained on data that has affixing information concealed within it. The laws that we have now are not clear on how to deal with this, and we may need to establish who should be accountable in case this occurs. That is why we are supposed to think more about changing our attitude and focus on whether a person could have predicted and prevented the injuries, but not just to pay attention to what one was going to do. In this manner, we can ensure that everybody is held responsible to the actions that go wrong, even though such individuals did not intend to make any action go wrong. We must consider how to ensure this works, so we can ensure people legally have their rights and that AI is used ethically and in a socially acceptable manner[30].

## 12. Conclusion

Growth of generative artificial intelligence produces an enormous transformation in the manners that individuals produce, process, and disseminate human knowledge. It has been noted that generative artificial intelligence systems do not simply help humans in their decision

[28] Sharon K. Sandeen & Elizabeth A. Rowe, *Trade Secret Law in a Nutshell* (West Academic, 2023).
[29] *HiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180 (9th Cir. 2022)
[30] Epic Systems Corp. v. Tata Consultancy Services Ltd., 980 F.3d 1117 (7th Cir. 2020).

because they do the active work of creating information that will have a market value. The trade secret law faces a challenging test since this law generally assumes that people are powerful, that they are keeping a secret with their knowledge willingly and voluntarily, and that they are setting clear boundaries to their own privately owned facts.

Protection of trade secret depends on three main sections since these sections are the fundamental beliefs of the law of the rule. The opinion held by many is that generative artificial intelligence dissolves these foundations. Control of data is undermined when company facts are fed into machine learning models since these models do not generate things that their owners can see at the same time. Reasonable efforts to conceal confidential information must now involve highly technical safety measures such as designated, secured teaching areas where models can be taught, methods of privacy, and restricting the information available to ensure that trade secret is not compromised. Generative artificial intelligence sometimes reproduces private facts due to the fact that the systems might reproduce the secret words used to train a given system.

It presents a huge issue to the industry because of leakage of facts through what the machine is producing. According to experts, large language models are able to regurgitate little portions of their training data when certain conditions occur. This situation poses legal questions since the law needs to determine whether this can be considered the revealing of a trade secret. It has to be put on the shoulders of the creator, the user or the person who runs the machine because the law requires an object on which to exercise blame? Our traditional doctrines are not well geared to answer these questions as they were not made to deal with systems that are probabilistic and lack intentionality.