International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 12 | Dec 2023 www.irjet.net p-ISSN: 2395-0072

INTERPLAY OF ARTIFICIAL INTELLIGENCE ON TRADE SECRETS

Durga C, Shanthoshiya TC

BBA.,LLB(HONS) STUDENT, SCHOOL OF LAW, SASTRA UNIVERSITY

Abstract

Artificial intelligence is a potential mechanism in the digital age to leak or expose sensitive Information that has commercial value in a business around the world, and most business Promoters use artificial intelligence to analyze the business plan, strategies, and Implementation. In today's digital age, protecting trade secrets has become a growing Challenge. Trade secrets include a variety of confidential data such as formulas, processes, Customer lists, and proprietary algorithms that give companies a competitive advantage. The advent of artificial intelligence (AI) is significantly changing the landscape of trade secret protection. The business's success depends on these trade secrets. Information confidentiality is crucial to safeguarding the company's competitive edge. Trade secrets are stored in the internal information system or register of the business. It can be kept in a safe place or in an electronic framework those guards against unauthorized data access. Non-disclosure agreements or NDA must be signed by partners in the company as well as workers in order to prevent the sharing of private knowledge. So the AI system will process the data incorrectly, and it also depends on the components of strangers. Many cybercriminals use artificial intelligence to access data and reveal trade secrets. Due to artificial intelligence, corporate privacy is greatly affected. Adequate security or preventive measures should be in place to protect sensitive information. The main purpose of this study was to determine the impact of artificial intelligence intruding on trade secrets and Legal measures to protect the trade secrets of the digital artificial intelligence system

Keywords-*ARTIFICIAL INTELLIGENCE,TRADE SECRETS,DATA PRIVACY, SENSITIVE INFORMATION.*

INTRODUCTION

Trade secrets are closely guarded and shrouded in secrecy, much like the hidden valuables of businesses. These are trade secrets that offer a business a competitive advantage over competitors. Trade secrets, in contrast to patents or copyrights, don't need to be formally registered; rather, their value depends on the organization's capacity to maintain their confidentiality. By granting creators and innovators exclusive rights, intellectual property rights (IPR) are the legal guardianship wings that flutter around the invisible landscape of human ingenuity.

INTERNATIONAL STANDARDS

(Trade-Related Aspects of Intellectual Property Rights): trips are an agreement. It establishes international standards for intellectual property rights protection, including trade secrets. TRIPS require WTO members to provide effective protection against unfair competition and the unauthorized acquisition, disclosure, or use of trade secrets. It establishes a foundation for the protection of trade secrets in the context of international commerce. The Paris conference for the protection of business belongings (Paris convention): This international treaty addresses industrial property protection, which includes patents, trademarks, and trade secrets. It establishes minimum standards for trade secret protection among its member countries. Many signatory countries to the Paris Convention provide trade secret protection.

THREE COMPONENTS OF TRADE SECRETS

Trade secrets are composed of three primary elements:

Information: Formulas, procedures, methods, designs, patterns, techniques, and any other kind of information that gives a company a competitive edge are all considered trade secrets. Many times, people are unaware of this information or find it difficult to obtain.

Secrecy: In order to retain its value, the information needs to be kept private. It is the trade secret owner's responsibility to take appropriate steps to protect the information's confidentiality. This can involve putting security procedures into place, employing non-disclosure agreements, limiting access to important employees, and taking other precautions to avoid unintentional disclosure.

Commercial Value: Since the information is not widely known to the public or is not readily obtainable by others, it must have a financial worth.

COMMAN LAW PRINCIPLE IN INDIA

In India, common law such as those governs trade secret law.

1. The parties were obligated by Section 27 of the Contract Act to refrain from disclosing any information that went against the provisions of their confidentiality agreements.

2. The Criminal Code of 1860, Sections 405–409, deals with cases involving criminal breaches of trust.

SEVERAL LEGISLATIONS GOVERNS THE TRADE SECRETS

1. The America' uniform trade secrets and techniques act (United States): Many US states have ratified the UTSA, which offers a unified legal framework for trade secret protection. It establishes the definition of a trade secret, the standards for misappropriation, and the available legal remedies.

2. The alternate secrets and techniques directive of euro union: Adopted in 2016, the EU Trade Secrets Directive unifies trade secret protection legislation amongst member states of the European Union. It lays out uniform guidelines, norms, and procedures for the defense of trade secrets across the European Union.

3. The settlement on trade-associated components of intellectual belongings rights (trips): World Alternate Corporation An international pact known as TRIPS establishes guidelines for the defense of intellectual property rights, which includes trade secrets. It is mandatory for member nations to furnish legal mechanisms for the efficient safeguards against deceptive business practices and the avoidance of trade secret theft.

4. Law at the national level: Trade secret protection is covered by specialized national laws in many nations. These laws g and delineate the legal redress available in cases of misappropriation. The UK exchange secrets and techniques (enforcement, and so forth.). Regulations and the Defend Trade Secrets A

5. (DTSA) in the United States and the United Kingdom are two examples. Not unusual law defenses: Common law principles serve as the foundation for trade secret protection in various jurisdictions. When making decisions in trade secret cases, courts may draw from prior decisions and accepted legal doctrines.

6. Contractual Conditions: Contractual agreements like confidentiality and non-disclosure agreements (NDAs) are frequently used by businesses to strengthen the security of their trade secrets. These contracts specify the parameters

PARTIES IN RELATION TO TRADE SECRETS

In case of Businesses and Pioneers: By utilizing sophisticated secrecy, access controls, and other security measures, AI can assist businesses in fortifying the defense of their trade secrets. But Businesses that incorporate AI into their goods and services may have to contend with increased competition as well as difficulties safeguarding their exclusive algorithms and procedures against reverse engineering. Contractors and Workers: Through automated monitoring and training, AI tools may improve employees' and contractors' comprehension of and adherence to trade secret protection measures. Trade secrets could be more easily misused or appropriated by staff members who have access to AI-driven technologies.Competitors.AI developments may help rivals, promoting more creativity and possibly bringing levels of competition. But the advanced tools can be used to pass through and steal trade secrets from rival companies; AI can also help with corporate espionage. Consumers; I-driven innovation may result in the creation of fresh goods and services, giving customers more options. If trade

secrets pertaining to AI technologies fall into the wrong hands, it could have an indirect impact on consumers by raising security and privacy issues. Governing Authorities: Regulatory agencies can use AI to monitor and enforce trade secret laws to guarantee compliance. Regulatory obstacles may arise from the need to keep up with the quick developments in AI and its use in situations involving trade secrets. The judicial and criminal systems: It can help with trade secret litigation by doing analysis but huge data sets and finding misuse the patterns.

Liability

Trade secret owner has a legal option, if their information is stolen, including seeking a court order to prevent further disclosure and claiming financial compensation for economic losses. The owner must prove that the trade secret provided a competitive advantage and was acquired unlawfully. However, the protection does not extend to instances where someone independently discovers the secret without illegal means, emphasizing the importance of taking reasonable measures to maintain secrecy.

IN SUFFICIENT SECURITY PROTOCOLS

In the event that entities fail to establish strong security protocols, such as encryption, access controls, and secure data storage, artificial intelligence may unintentionally reveal weaknesses that could be taken advantage of by malevolent entities.

Artificial intelligence (AI) systems themselves may be exploited due to AI system vulnerabilities

Attackers may find ways to manipulate the system and obtain unauthorized access to sensitive data if there are flaws in the AI algorithms or implementation.

In adversarial attacks, input data is manipulated to trick AI models. Attackers may be able to obtain information or compromise the AI system if a trade secret is incorporated into the training set or model.

Data Violations: Large datasets are frequently used by AI for analysis and training. If sensitive trade secrets are present in these datasets confidential information may be revealed in a data breach if these datasets, which include sensitive trade secrets, are not sufficiently protected.

Insider Risks Using AI-Powered Tools: AI tools could be abused by staff members or insiders to obtain or reveal trade secrets. This could entail breaking into secret databases, analyzing data without authorization, or tampering with AI algorithms to expose private data.

Inversion Attacks on Models: Reverse engineering an AI model to expose private information about the training set is known as a "model inversion attack." An attacker may be able to reconstruct proprietary information by using this vulnerability if trade secrets are present in the training data.

Improved Social Engineering with AI: AI has the potential to improve social engineering techniques. AI-generated phishing emails or messages, for instance, could deceive staff members. Insufficient controls on get proper of entry to confidential information may be accessed by unauthorized users if access controls to AI systems are not set correctly. This can involve distributing reports or analyses produced by AI that contain trade secrets improperly.

Unsafe Collaboration Instruments: Sensitive information shared on these platforms runs the risk of being exposed due to the growing use of AI in collaboration tools. Attackers may take advantage of weak authentication procedures or insecure APIs. Unsecure AI Model Transfer If AI models are transferred between devices or entities without adequate security, there is chance that they will be intercepted or tampered with. Trade secrets stored in the AI models may leak as a result of this. If AI models are transferred between devices or entities without adequate security, there is a chance that they will be intercepted or tampered with. Trade secrets stored in the AI models may leak as a result of this. Organizations should prioritize strong cyber security procedures, update and patch AI systems on a regular basis, use secure development practices, carry out in-depth risk assessments, and train staff members on the value of protecting sensitive data in order to reduce these risks. In addition, contractual and legal actions might be required to hold people or organizations responsible for trade secret leaks made possible by AI. In the event that entities fail to establish strong security protocols, such as encryption, access controls,

and secure data storage, artificial intelligence may unintentionally reveal weaknesses that could be taken advantage of by malevolent entities.

CASE LAWS ON PROTECTION AND ENFORCEMENT OF INTELLECTUAL PROPERTY

Bib Apparels Private Ltd v. retina private ltd

Facts: A lawsuit alleging infringement on apparel designs was submitted. Could a trade secret injunction be issued without identifying the trade secrets and proving ownership? The court debated this possibility. Order: The court decided that specific trade secrets had to be identified and ownership had to be established in order for an injunction order pertaining to trade secrets to be granted. It was not acceptable to issue a broad order for unidentified trade secrets. Furthermore, because of the restrictions of the Copyright Act, no relief was given under the Act.

Calendar siv v. Genetics India Private Ltd

Facts: Private information was at issue in this case. The court emphasized how important it is to give the need of submitting pleadings in business secret lawsuits that demonstrate the information's confidentiality was emphasized by the court. It underlined that evidence of reasonable measures to preserve confidentiality must be provided.

Order: The plaintiff must provide pleadings outlining the information's secret character, the court declared. In addition, the plaintiff needs to demonstrate that adequate precautions were taken to protect the privacy of the information. If this isn't done, secrecy status can be lost.

Importance of establishing a robust framework in India for protecting trade secrets

The established framework in India to protect trade secrets, the subject of trade secrets appears to be neglected. Although this type of intellectual property is relatively new in India, it is a crucial area of IP. The safeguarding of trade secrets is a crucial and arduous undertaking for the Indian government, as it serves to augment foreign investment in the country, thereby stimulating the economy. To conduct business with our nation, foreign investors must have the assurance that their trade secrets will be protected. The security of our own industry will be further improved by an appropriate trade secret protection policy. Theft of trade secrets, especially via cyber attacks, is a serious problem. With the growing usage of the internet and advanced hacking methods, safeguarding private data from unwanted access is a difficult undertaking.

AI developers and businesses must make significant investments in strong cyber security measures to meet this challenge. This includes security best practices training for staff members, encryption, access controls, and routine security audits to identify and address possible breaches.

AI-Enhanced Cyber security: To protect priceless trade secrets from theft or espionage, AI is being used to develop cutting-edge cyber security measures that can identify and react to possible threats in real-time.

Automation of IP Management: AI-powered solutions lower the possibility of human error and enhance overall IP protection by automating trade secret identification, tracking, and security procedures.

M&A Due Diligence: AI-powered analytics assist with due diligence in mergers and acquisitions by spotting possible hazards in the IP portfolios of target companies and guaranteeing that acquired assets are safeguarded after acquisition.

MEASEURES TO PROTECT THE TRADE SECRETS

Determine the Information that Qualifies as a Trade Secret: The first step is to precisely determine which information in your company is a trade secret. Technical data, formulas, customer lists, marketing plans, and other proprietary information that gives an advantage over competitors can all fall under this category. Limited Access: Within the company, restrict who has access to trade secrets. Grant access solely to staff members or associates who require the information in order to carry out their duties.

Establish confidentiality agreements: To legally obligate staff members and business associates to maintain the privacy of your trade secrets, have those sign non-disclosure agreements (NDAs) or confidentiality agreements. Documents, prototypes, and other tangible assets that contain trade secrets should be kept physically secure. Use safes, locked cabinets, or locations with limited access.

Digital Security: Use secure access controls, encryption, and strong passwords to safeguard digital trade secrets. Update and patch software frequently to stop illegal access. Employee Education: Educate staff members on the value of upholding confidentiality. Inform them of the moral and legal responsibilities pertaining to trade secrets.

Keeping Records: Keep track of who has access to the trade secrets, when they were created, and any updates or modifications to the data. This record may come in handy if there are any legal disputes. Ensuring secure transmission of sensitive information via encrypted channels is crucial, particularly in electronic communication.

Vendor and partner agreements: To safeguard your trade secrets when disclosing them to others, incorporate confidentiality clauses in agreements with outside suppliers, vendors, and business partners.

Monitoring and auditing: Keep an eye out for any unusual or unauthorized activity by routinely monitoring and auditing access to your trade secrets. Implementable Regulations: Create and implement policies that are unambiguous about the penalties for violating confidentiality. Ensure that staff members are aware of the consequences of failing to protect trade secrets.

Legal Remedies: In the event that your trade secrets are compromised, be ready to defend yourself in court. To learn about your rights and the available legal remedies, speak with an attorney. Labeling and staining: Clearly label and mark papers and other materials as "trade secret" or "confidential" to alert others to their sensitive nature. Periodic Review is to keep up with evolving times and technological advancements, periodically review and update your trade secret protection strategies. Strict get entry to controls in vicinity sturdy get entry to controls in area to restrict get entry to sensitive records. Apply the least privilege principle to make sure AI systems and staff only have access to the information required for their particular roles. Music and audit consumer access: Keep an eye on and audit sensitive data access on a regular basis for both AI and human users. Putting real-time monitoring into practice can assist in identifying anomalous activity that might point to a possible security risk.

Employee Education: Employees should receive thorough instruction on the value of protecting trade secrets. Make them understand the dangers of artificial intelligence as well as their part in preserving the privacy of sensitive data. Practice AI to safety surveillance: Use security monitoring tools powered by AI to identify and address possible threats. Artificial Intelligence has the capability to examine behavioral patterns and detect deviations that might point to a security compromise, instantly alerting security staff. Data Loss Prevention (DLP) Solutions into Practice: Install DLP programs that are able to keep an eye on, identify, and stop illegal data transfers. These remedies can aid in enforcing laws that limit AI System Updates and Patches: Update and patch AI systems frequently to fix any vulnerabilities. Ensuring that the AI tools utilized by the organization are outfitted with the most recent security features and safeguards is imperative. Make sure that policies and procedures are clear: Create and implement explicit policies and processes for managing trade secrets, particularly when artificial intelligence is involved. Make sure AI developers and staff are aware of their responsibilities and the repercussions of handling sensitive data improperly. legal safeguards and agreements: Use contracts, non-disclosure agreements (NDAs), and other legal tools to enforce your rights. In contracts with workers, vendors, and partners, clearly state the conditions of use for AI tools and the safeguarding of trade secrets.

Frequent audits of security: Carry out routine security assessments to find any possible gaps in your systems. Internal and external audits may be used to evaluate the success of security measures and pinpoint areas in need of development.

IMPACT ON SOCIETY

The displacement of Economic Inequality and Employment occur Because of AI's automation capabilities, workers in some industries may lose their jobs to machines, which could have a negative financial impact on them. This may lead to a rise in economic disparity.

Privacy concerns arise from the widespread use of AI to handle large amounts of sensitive and personal data. Trade secrets may be compromised by unauthorized access or security flaws in AI systems, which would reduce a company's ability to compete. The occurrences of Unintended Consequences and Ethical Concerns and the application of AI to trade secrets raise moral questions about consent, data ownership, and responsible AI usage.

Unintentional outcomes, like biases in AI algorithms, can give some people or companies unfair advantages or disadvantages.

There are new cyber security risks associated with the increased reliance on AI. AI systems are susceptible to cyber-attacks that could compromise trade secrets and have negative social and economic effects if they are not sufficiently secured. Regulatory Obstacles held Because AI technology is developing so quickly, it is becoming more difficult for regulators to create and implement laws that effectively safeguard trade secrets. Inadequate regulation could allow AI technologies to be abused for information theft or leakage. Employment Losses and Skill Mismatch of AI-driven automation could lead to the loss of traditional jobs, which would increase unemployment and possibly create a skills gap in the workforce. Social repercussions from this could include rising unemployment and discontent in the community. Trade secrets may be manipulated or misused by malicious actors using AI systems for personal benefit. This could entail employing AI-generated content for dishonest ends or to evaluate and extract sensitive data. Adverse Public Attitude is the severe impact where a poor public image of AI technologies can be exacerbated by instances of trade secret misappropriation, unethical behavior, or breaches related to AI. This mistrust could prevent AI from being widely used and reaping its benefits.

LEGAL IMPACT OF TRADE SECRETS

Identifying Ownership is more difficult when the definition of ownership may become more ambiguous when trade secrets are developed and improved using AI. Determining who is entitled to the resulting trade secrets the AI developer, the company using the AI, or both may present legal challenges.

Uncertainty occurs when it comes to cases of AI-related trade secret misappropriation, legal systems might encounter difficulties. There may be legal ambiguities when attempting to ascertain the purpose and accountability for misappropriation motivated by artificial intelligence.

Unclarity Regarding Data Ownership. The processing of significant data sets is an increasingly prevalent AI application. Legal frameworks may find it difficult to establish precise rules regarding data ownership, particularly in cases where AI algorithms are involved in the creation or alteration of datasets that contain trade secrets.

Insufficient Regulation of AI Technologies: In the event that businesses utilize AI to protect trade secrets, the lack of specific regulations governing this use may result in inadequate protection. The legal framework may also lag behind technological advancements, making businesses susceptible to new threats posed by AI. When AI applications process sensitive or personal data to protect trade secrets, privacy concerns may give rise to legal action, particularly in the event of data breaches that reveal confidential information. Moral Challenges and Legal Gray Subjects like ethical issues surrounding AI technologies may give rise to legal ambiguities. These may include biased methods, unfair competition policies, or unintended consequences.

It can be difficult to determine who is legally liable for decisions or actions taken by AI, especially when it comes to trade secret protection. Insufficient guidelines could lead to legal disputes about culpability for AI-related incidents that jeopardize trade secrets. Difficulties with Global Harmonization when Businesses that operates globally may face difficulties due to regional variations in trade secrets and artificial intelligence legal frameworks and standards. International efforts to safeguard trade secrets may be hampered by inconsistent regulations.

Misuse of artificial intelligence (AI) tools, such as fabricating evidence through analyses or content produced by AI, can have an impact on legal proceedings concerning trade secrets. The integrity and fairness of the legal system may be impacted. Responsibility for developing, implementing, and overseeing AI systems rests with the people or organizations that do so, not with AI per se. Both the companies that own and run the technology and the people who programmed, implemented, and oversaw the AI system are held accountable if it results in the disclosure of trade secrets. **Burlington Home Shopping Pvt. Ltd. v. Rajneesh Cibber'**

The defendant was a former worker for the plaintiff's company, and when he left, he launched a similar business using the plaintiff's contacts database. The Hon'ble High Court of Delhi ruled that the plaintiff had used skill and labor to create the contacts database, protecting it under the laws pertaining to trade secrets and confidential information.

CONCLUSION

Businesses looking to keep a competitive edge in the global market must prioritize protecting their trade secrets. A company's success can be greatly impacted by a variety of valuable information that falls under the category of trade secrets, such as customer lists, formulas, processes, and technological advancements.

Organizations must put strong security measures in place, like non-disclosure agreements, access controls, and employee training programs, to protect trade secrets. Furthermore, legal frameworks that offer a basis for legal recourse in the event of misappropriation include the Uniform Trade Secrets Act in the United States and comparable laws in other jurisdictions.

Reference

1. https://kpmg.com/nl/en/home/insights/2023/06/the-copyright-aspects-of-free-ai-applications/ai-and-the-impact-on-trade-secrets.html
2. https://kpmg.com/nl/en/home/insights/2023/06/the-copyright-aspects-of-free-ai-applications/ai-and-the-impact-on-trade-secrets.html
3. https://arapackelaw.com/trade-secrets/trade-secret-ai-ip/
4. https://www.wipo.int/tradesecrets/en/
5. https://blog.ipleaders.in/protection-of-trade-secrets-and-confidential-information-in-india-and-global-trends/
6. https://www.kashishipr.com/blog/trade-secrets-in-intellectual-property-rights-iprs/
7. https://www.lexology.com/library/detail.aspx?g=4f23531b-10a4-4b69-a9fe-b7d3a10de67d
8. https://legal.thomsonreuters.com/blog/trade-secret-litigation-101/
9. https://www.wipo.int/tradesecrets/en/tradesecrets_faqs.html
10. https://www.lexology.com/library/detail.aspx?g=d867aed5-efd5-404c-8478-eed93f1b321c
11. https://gowlingwlg.com/fr/insights-resources/guides/2022/trade-secrets-guide-uk-2022-trends-developments/
12. https://www.irmi.com/term/insurance-definitions/common-law-defenses
13. https://www.wipo.int/tradesecrets/en/
14. https://www.law.cornell.edu/wex/trade_secret
15. https://www.avocats-mathias.com/contentieux/trade-secrets-directive
16. http://www.securitysa.com/8330r
17. https://en.wikipedia.org/wiki/Judiciary
18. https://www.belfercenter.org/publication/AttackingAI
19. https://zvelo.com/the-role-of-ai-in-social-engineering/

20. https://www.apollo.io/companies/Retina-Software-Pvt--Ltd-/55edebb6f3e5bb77a3004981

21. https://indeemo.com/blog/research-ops-toolki

22. https://ericlambert.net/blog/2015/12/14/key-security-provisions-for-all-vendor-contracts

23. https://www.compliance.com/resources/compliance-officers-responsibility-ongoing-auditing-monitoring-high-risk-areas/

24. https://zipdo.co/statistics/ai-in-cyber-security/

25. https://geekflare.com/best-ipam-software/