INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

PROMPT LEAKAGE AND CORPORATE ESPIONAGE: TRADE SECRETS IN THE GENERATIVE AI ECONOMY

AUTHORED BY - JESTY K AJAY

ABSTRACT

The rapid integration of Generative Artificial Intelligence into corporate operations has created unprecedented opportunities for innovation, efficiency, and strategic growth. At the same time, it has introduced new legal and security vulnerabilities, among which prompt leakage has emerged as a significant concern. Prompt leakage refers to the unintended disclosure of sensitive instructions, proprietary data, confidential business strategies, or trade secrets through interactions with AI systems. In the contemporary digital economy, prompts are no longer merely commands given to AI models; they increasingly embody valuable corporate intelligence, reflecting internal workflows, market strategies, research data, and proprietary methodologies. Their exposure may enable competitors, malicious insiders, or external actors to gain unauthorized access to commercially valuable information, thereby facilitating corporate espionage. This paper examines prompt leakage as an emerging threat to trade secret protection within the Generative AI economy. It analyzes how traditional legal doctrines relating to confidentiality, trade secrets, and corporate governance struggle to address AI-enabled information leakage. The study further explores the evolving relationship between corporate law, cybersecurity, and intellectual property protection in mitigating these risks. By evaluating existing regulatory frameworks and identifying legal gaps, the paper argues for AI-specific governance mechanisms to strengthen corporate resilience against espionage in increasingly automated business environments.

INTRODUCTION

The emergence of Generative Artificial Intelligence has transformed the operational landscape of modern corporations. Businesses increasingly rely on AI-powered systems for decision-making, customer engagement, data analysis, product development, and strategic planning. While these technologies offer significant economic advantages, they simultaneously create complex legal and governance challenges. One such challenge is prompt leakage, an emerging phenomenon that poses serious risks to corporate confidentiality and trade secret protection. In the context of Generative AI, prompts function as structured instructions that guide AI models

ISSN: 2582-6433

to produce desired outputs. Within corporate settings, these prompts often contain highly sensitive information, including proprietary algorithms, internal policies, business strategies, research data, customer insights, and confidential operational procedures. As organizations integrate AI tools into daily workflows, prompts themselves have evolved into strategic corporate assets. Their value lies not only in the information they contain but also in the competitive advantage they generate. Prompt leakage occurs when such confidential prompts are exposed, intentionally or unintentionally, to unauthorized parties.[1] Leakage may arise through employee negligence, malicious insider activity, weak cybersecurity safeguards, third-party AI service providers, or vulnerabilities within AI systems. Unlike conventional data breaches, prompt leakage presents a unique challenge because sensitive information may be embedded within seemingly ordinary human-AI interactions, making detection and prevention considerably more difficult. This study seeks to examine prompt leakage as a modern instrument of corporate espionage and analyze its implications for trade secret protection in the Generative AI economy. It further explores whether existing legal mechanisms are sufficient to address these emerging threats and considers the need for specialized regulatory and corporate governance responses suited to AI-driven commercial environments.

MEANING AND IMPORTANCE OF TRADE SECRETS

Trade secrets constitute one of the most significant forms of intellectual capital in the contemporary corporate environment. In contrast to traditional forms of intellectual property such as patents, copyrights, and trademarks, trade secrets derive their legal and economic value primarily from secrecy. A trade secret generally refers to confidential business information that is not publicly known, provides commercial or economic value to its owner, and is subject to reasonable measures undertaken to preserve its confidentiality. Such information may include formulas, manufacturing processes, technical know-how, software source codes, research data, business strategies, pricing structures, marketing techniques, customer lists, supplier networks, and proprietary algorithms. The concept of trade secrecy has existed for centuries, particularly in industries where innovation and competitive advantage depended upon preserving exclusive knowledge. Historically, businesses relied on secrecy to protect formulas, recipes, and manufacturing techniques from competitors. In the modern digital economy, however, the scope of trade secrets has expanded considerably. Information has become one of the most valuable corporate assets, and organizations increasingly derive market power not merely from

[1] OWASP Found., OWASP Top 10 for Large Language Model Applications 2025, https://owasp.org/www-project-top-10-for-large-language-model-applications/ (last visited June 29, 2026).

ISSN: 2582-6433

physical resources but from proprietary knowledge, data-driven insights, and strategic intelligence. This transformation has elevated trade secret protection to a central concern in corporate governance and risk management. The importance of trade secrets lies in their ability to create and sustain competitive advantage. Corporations invest substantial financial, human, and technological resources in developing confidential information that differentiates them from competitors. Proprietary algorithms may enable superior market predictions, confidential pricing strategies may improve profit margins, and unique business models may provide strategic dominance within a sector. The economic value of such information often exceeds that of tangible corporate assets. Consequently, the unauthorized disclosure or misappropriation of trade secrets may result in severe financial losses, erosion of market position, reputational harm, and long-term strategic disadvantages.

Unlike patents, trade secrets offer protection without requiring public disclosure or formal registration. This characteristic makes them particularly attractive for corporations seeking indefinite protection over commercially valuable information. While patent protection provides exclusive legal rights for a limited period in exchange for public disclosure, trade secret protection continues as long as secrecy is maintained. This creates a strategic preference for secrecy in industries where disclosure may benefit competitors or where innovation evolves rapidly. Corporations therefore often choose trade secret protection when maintaining confidentiality offers greater long-term benefits than formal intellectual property registration.[2] The legal recognition of trade secrets depends upon certain essential characteristics. First, the information must possess commercial value because of its secrecy. If information becomes publicly available or easily accessible, it generally loses trade secret status. Second, the information must not be generally known within the relevant industry or among the public. Third, the owner must demonstrate reasonable efforts to preserve confidentiality through internal policies, technological safeguards, restricted access, confidentiality agreements, or other protective measures. These criteria collectively distinguish trade secrets from ordinary business information. Therefore, trade secrets must be understood not merely as confidential information but as strategic corporate assets central to organizational survival and competitiveness. Their protection has become indispensable in sustaining innovation, preserving economic value, and maintaining market leadership. As corporations continue integrating advanced technologies such as Generative Artificial Intelligence into their

[2] Roger M. Milgrim, Milgrim on Trade Secrets § 1.01 (2025).

ISSN: 2582-6433

operations, safeguarding trade secrets becomes increasingly complex, thereby demanding stronger legal, technological, and governance frameworks.

LEGAL PROTECTION OF TRADE SECRETS

The legal protection of trade secrets occupies a unique position within the broader framework of intellectual property law. Unlike patents, trademarks, or copyrights, trade secrets generally do not require formal registration with a governmental authority for legal recognition. Their protection arises primarily from the confidential nature of the information and the legal obligations imposed upon individuals or entities that gain access to such information. This distinctive nature makes trade secret law both flexible and complex, as its effectiveness depends largely on the ability of corporations to maintain secrecy and demonstrate reasonable efforts toward protection. Trade secret protection is rooted in the principle that commercially valuable confidential information deserves legal recognition when unauthorized disclosure or misuse causes competitive harm. Courts and legal systems commonly evaluate three core requirements to determine whether information qualifies for trade secret protection. First, the information must be secret, meaning it should not be generally known or readily accessible to the public or competitors. Second, the information must possess economic or commercial value because of its secrecy. Third, the owner of the information must have taken reasonable steps to maintain confidentiality. These elements collectively form the legal foundation for trade secret protection across many jurisdictions. The absence of a uniform global legal regime has resulted in jurisdictional differences in the treatment of trade secrets. In some countries, trade secret protection is governed by dedicated statutes, while in others it is protected through contractual obligations, equitable principles, and judicial precedents. For example, in India, there is no standalone legislation exclusively governing trade secrets. Instead, protection is derived from contractual law, common law principles, and equitable remedies under breach of confidence. Confidentiality clauses, non-disclosure agreements, employment contracts, and fiduciary obligations therefore play a critical role in protecting proprietary corporate information. Indian courts have repeatedly recognized the importance of protecting confidential business information, particularly where misuse leads to unfair competitive advantage. In contrast, jurisdictions such as the United States provide more structured statutory protection. Trade secrets are protected under both state and federal frameworks, including legislation specifically addressing misappropriation of confidential business information. Similarly, the European Union has adopted harmonized legal standards to strengthen protection against unlawful acquisition, use, and disclosure of trade secrets. These developments reflect growing

ISSN: 2582-6433

international recognition of trade secrets as critical economic assets in innovation-driven industries. Corporations rely heavily on contractual mechanisms to protect trade secrets in day-to-day operations. Non-disclosure agreements remain among the most common tools used to restrict unauthorized sharing of sensitive information. Such agreements are frequently executed between employers and employees, corporations and consultants, or business partners engaged in strategic collaborations. Employment contracts often include confidentiality clauses prohibiting employees from disclosing proprietary information during and after their employment. In addition, corporations implement access control policies, digital security protocols, encryption systems, and internal compliance mechanisms to demonstrate active efforts toward secrecy.[3] Legal remedies for trade secret misappropriation typically include injunctions, compensatory damages, account of profits, and, in certain jurisdictions, criminal sanctions. Injunctions prevent further disclosure or use of confidential information, while damages compensate the injured corporation for financial losses caused by misappropriation. However, despite these remedies, enforcement remains challenging, particularly in technologically advanced environments where information can be copied, transmitted, or leaked instantly across jurisdictions. The rise of digital technology has further complicated trade secret protection. Cloud computing, remote working systems, AI integration, and cross-border digital communications have significantly increased exposure to unauthorized access and information leakage. Traditional legal frameworks were largely designed to address physical or human-mediated breaches of confidentiality. They often struggle to adequately address emerging risks involving automated systems, algorithmic processing, and AI-generated outputs. This creates regulatory gaps in determining liability and enforcing protection when confidential information is compromised through technological channels.

CORPORATE CONFIDENTIALITY IN THE AI ECONOMY

The rapid emergence of Artificial Intelligence, particularly Generative AI, has fundamentally transformed the manner in which corporations create, process, store, and utilize information. In the contemporary digital economy, information has become one of the most valuable corporate resources, and the protection of confidential data has consequently become a central concern for businesses across industries. Corporate confidentiality, which traditionally focused on safeguarding internal documents, trade secrets, proprietary research, and strategic business

[3] National Institute of Standards and Technology (NIST) , Security and Privacy Controls for Information Systems and Organizations (Special Publication 800-53 Rev. 5), https://csrc.nist.gov/pubs/sp/800/53/r5/final (Sept. 2020).

ISSN: 2582-6433

information, now faces unprecedented challenges due to the integration of AI-powered technologies into corporate operations. Corporate confidentiality refers to the obligation of an organization to preserve the secrecy of sensitive business information and prevent unauthorized access, disclosure, or misuse. Confidential information may include financial records, internal communications, customer databases, product development plans, pricing strategies, supply chain data, proprietary algorithms, and strategic decision-making processes. The confidentiality of such information is essential not only for maintaining competitive advantage but also for preserving corporate reputation, investor confidence, and market stability. In modern business environments, the loss of confidentiality can have consequences far beyond immediate financial harm, affecting long-term growth, strategic positioning, and stakeholder trust. The adoption of AI technologies has significantly altered the corporate confidentiality landscape. Corporations increasingly deploy AI systems for automated decision-making, predictive analytics, customer service, market forecasting, legal compliance, and operational optimization. These technologies enable organizations to process enormous volumes of data with remarkable speed and efficiency. However, this increased reliance on AI also introduces new pathways through which confidential information may be exposed, intentionally or unintentionally. Unlike conventional digital systems, Generative AI operates through continuous interaction with human inputs, often in the form of prompts, instructions, datasets, and contextual queries. Employees using AI tools may unknowingly input sensitive corporate information into external AI platforms for analysis, summarization, drafting, or strategic assistance. Such interactions may involve proprietary business plans, confidential legal advice, financial projections, research findings, or internal governance discussions. Once sensitive information enters an AI ecosystem, controlling its storage, processing, and exposure becomes significantly more difficult, especially when third-party AI providers are involved.

The AI economy also blurs traditional boundaries between internal and external information environments. Historically, corporations maintained confidentiality through controlled physical access, secure internal servers, restricted documentation, and hierarchical authorization systems.[4] AI integration disrupts these traditional boundaries by enabling information to flow across cloud infrastructure, application programming interfaces, third-party software systems, and automated analytical tools. This interconnected ecosystem increases vulnerability to data breaches, unauthorized surveillance, cyberattacks, insider

[4] Information Security Management Principles Andy Taylor, David Alexander & Amanda Finch, Information Security Management Principles 45–48 (2d ed. 2013).

ISSN: 2582-6433

threats, and accidental disclosure. One of the most significant confidentiality concerns in the AI economy is the emergence of prompt-based data exposure. Prompts submitted to AI systems may contain highly sensitive business intelligence without users fully appreciating the risks involved. Unlike traditional data-sharing mechanisms, prompt interactions often appear informal and routine, reducing employee caution. This creates a dangerous environment where confidential information may be leaked through ordinary workplace AI usage. In such scenarios, corporate confidentiality is threatened not only by malicious actors but also by negligence, lack of awareness, and inadequate governance frameworks. Furthermore, the global nature of AI services introduces complex jurisdictional and regulatory concerns. Corporate data processed by AI systems may cross national boundaries and become subject to multiple legal frameworks concerning privacy, cybersecurity, and data governance. This complicates compliance obligations and raises difficult questions regarding accountability, ownership, and legal responsibility when confidential information is compromised. Existing legal mechanisms often struggle to address these transnational challenges effectively. In the AI economy, preserving corporate confidentiality therefore requires more than traditional secrecy measures. Corporations must adopt comprehensive governance strategies that integrate legal safeguards, technological security, employee awareness, and AI-specific risk management protocols. This includes establishing internal AI usage policies, restricting sensitive prompt inputs, implementing encryption and monitoring systems, conducting regular compliance audits, and strengthening contractual protections with AI service providers. Corporate confidentiality in the AI era must ultimately be understood as a dynamic governance challenge rather than a static legal obligation. As AI systems continue to evolve and become deeply embedded within corporate structures, the protection of confidential information will depend on an organization's ability to adapt to emerging technological risks. Effective confidentiality management in the Generative AI economy will therefore remain essential for protecting trade secrets, sustaining innovation, and preserving long-term corporate competitiveness.

PROMPT LEAKAGE AND CORPORATE ESPIONAGE

Prompt leakage has emerged as a significant concern in the era of Generative Artificial Intelligence, particularly within corporate environments where AI tools are increasingly integrated into daily operations. A prompt refers to the instruction, command, or query provided by a user to an AI system in order to generate a specific response or output. While prompts may appear simple, in professional settings they often contain highly sensitive information such as proprietary business strategies, internal workflows, legal documents,

ISSN: 2582-6433

financial projections, or confidential research data. Prompt leakage occurs when such confidential prompts are exposed, disclosed, or accessed by unauthorized individuals or entities. This exposure may occur intentionally through malicious activities or unintentionally through employee negligence, weak security systems, or improper AI usage practices. Unlike traditional data leaks, prompt leakage is particularly difficult to detect because sensitive information is often embedded within ordinary human-AI interactions that may not initially appear risky. The growing dependence on third-party AI platforms has further increased the risk of prompt leakage. Employees often use AI tools for drafting documents, summarizing reports, conducting research, and improving productivity. During these interactions, confidential corporate information may be entered into AI systems without sufficient awareness of data retention, processing, or storage practices. If adequate safeguards are absent, such inputs may become vulnerable to unauthorized access, cyberattacks, or misuse. Prompt leakage presents unique legal and corporate challenges because prompts increasingly function as repositories of valuable organizational knowledge. In the Generative AI economy, prompts are no longer mere instructions but strategic assets capable of revealing trade secrets and internal decision-making processes. Consequently, understanding prompt leakage is essential for corporations seeking to protect confidential information and maintain competitive advantage in AI-driven markets. Corporate espionage refers to the unauthorized acquisition of confidential business information for competitive, financial, or strategic advantage. Traditionally, corporate espionage involved activities such as industrial spying, theft of confidential documents, insider misconduct, cyber intrusion, or surveillance of competitors. However, with the rise of Generative Artificial Intelligence, the methods and channels of espionage have evolved significantly. Prompt leakage has emerged as a modern and sophisticated instrument through which sensitive corporate information may be exposed. In the AI-driven corporate environment, prompts often contain commercially valuable information including business strategies, research findings, product development plans, pricing models, and confidential communications.[5] When such prompts are leaked, competitors or malicious actors may gain access to strategic insights that would otherwise remain protected as trade secrets. This creates opportunities for unauthorized replication of business models, reverse engineering of proprietary systems, and unfair competitive advantage. Prompt leakage becomes a form of corporate espionage when leaked information is intentionally exploited for economic gain or strategic manipulation. Unlike traditional espionage, which often required

[5] OWASP Foundation, OWASP Top 10 for Large Language Model Applications 2025, https://owasp.org/www-project-top-10-for-large-language-model-applications/ (last visited June 29, 2026).

ISSN: 2582-6433

direct theft or physical access to confidential records, AI-mediated leakage can occur silently through routine digital interactions. This makes prompt leakage particularly dangerous, as sensitive information may be extracted without obvious signs of intrusion. The increasing reliance on external AI platforms further intensifies this threat. Where corporations fail to implement proper governance and confidentiality safeguards, prompt leakage can become a major pathway for digital corporate espionage. Therefore, in the Generative AI economy, prompt leakage must be recognized not merely as a technical issue but as an emerging corporate security and legal challenge.

METHODS AND RISKS OF INFORMATION LEAKAGE

Information leakage through AI systems can occur through multiple pathways, each presenting distinct risks to corporate confidentiality. One of the most common causes is employee negligence. Employees may unintentionally share confidential data with AI systems while seeking assistance with drafting, analysis, or problem-solving, without fully understanding the associated security risks. Lack of awareness and insufficient training often contribute to such accidental disclosures. Insider threats also represent a serious concern. Employees, contractors, or consultants with authorized access to sensitive corporate data may deliberately misuse AI systems to leak proprietary information for personal benefit or external collaboration. In such cases, prompt leakage becomes a deliberate mechanism of information theft. Cybersecurity vulnerabilities constitute another major source of leakage. Weak security protocols, poor access controls, unsecured cloud storage, and third-party integration risks may expose sensitive prompt data to hackers or malicious actors. Since AI tools frequently operate through interconnected digital infrastructures, a single security weakness may compromise large volumes of confidential information. The risks associated with information leakage are substantial. Corporations may suffer financial losses, reputational damage, regulatory penalties, and loss of competitive advantage. Trade secrets, once disclosed, may permanently lose their legal protection and economic value. In severe cases, leaked information may alter market dynamics by enabling competitors to exploit confidential strategic insights. Consequently, effective management of information leakage has become essential for corporate survival in the AI-driven economy.

REGULATORY CHALLENGES AND CORPORATE LIABILITY

The rapid adoption of Generative Artificial Intelligence has created regulatory challenges that existing legal frameworks struggle to address. Traditional laws governing trade secrets,

ISSN: 2582-6433

confidentiality, cybersecurity, and corporate governance were developed before AI became deeply integrated into business operations. As a result, these legal mechanisms often fail to adequately regulate emerging risks such as prompt leakage and AI-enabled corporate espionage. One major challenge lies in the absence of AI-specific legislation addressing ownership, control, and protection of prompts containing sensitive corporate information. Current laws may protect confidential information in general, but they rarely account for the unique nature of AI interactions, where sensitive data can be embedded in routine prompts and processed across multiple digital systems. Cross-border data processing further complicates regulation, as corporate information shared with AI platforms may be stored or accessed across different jurisdictions with varying legal standards. Additionally, regulatory uncertainty creates difficulties in determining accountability when prompt leakage occurs. Questions often arise regarding whether liability should rest with employees, corporations, AI developers, or third-party service providers. These uncertainties demonstrate the need for more comprehensive legal frameworks capable of addressing AI-related confidentiality risks.

Corporate liability becomes a central issue when prompt leakage leads to unauthorized disclosure of confidential information or trade secrets. In corporate law, organizations have a duty to implement reasonable measures to protect sensitive business assets. Failure to establish adequate safeguards may expose corporations to legal liability, financial losses, and reputational damage. Boards of directors and senior management play a crucial role in corporate governance related to AI usage. Their responsibilities increasingly extend beyond traditional oversight to include AI risk assessment, cybersecurity planning, and confidentiality management. If corporations neglect to monitor AI-related risks or fail to implement appropriate internal controls, questions may arise regarding breach of fiduciary duties and governance failures. Corporate liability may also arise through employee actions. Where employees misuse AI tools or negligently disclose confidential information, organizations may face indirect liability depending on the nature of supervision, internal policies, and compliance mechanisms. Therefore, effective governance requires corporations to treat AI risk management as an essential component of modern corporate responsibility.

RISK MANAGEMENT MECHANISMS

Managing prompt leakage risks requires a combination of legal, technical, and organizational safeguards. Corporations must adopt proactive mechanisms to minimize exposure of sensitive information within AI-driven environments. Risk management begins with clear internal AI

ISSN: 2582-6433

usage policies that define what information may or may not be entered into AI systems. Employee awareness and training are equally important. Since human error remains a major source of information leakage, regular training programs can improve understanding of confidentiality risks associated with AI tools. Access controls, encryption, monitoring systems, and cybersecurity audits further strengthen corporate defenses against unauthorized disclosure. Contractual safeguards also play a critical role in risk management. Corporations should establish strong confidentiality clauses, non-disclosure agreements, and clear contractual obligations with AI service providers regarding data handling and storage.[6] Regular compliance assessments can help identify vulnerabilities before they result in significant harm. Effective risk management therefore requires corporations to integrate legal compliance, governance strategies, and technological safeguards. In the AI economy, preventing prompt leakage is not solely a technical issue but a continuous corporate responsibility essential for protecting trade secrets and maintaining market competitiveness.

CONCLUSION

To address the risks associated with prompt leakage, corporations must adopt stronger AI governance frameworks and confidentiality safeguards. Organizations should develop clear internal policies regulating AI usage and restrict the sharing of sensitive information through external AI platforms. Regular employee training programs should be introduced to improve awareness regarding AI-related confidentiality risks. From a legal perspective, there is a growing need for AI-specific regulatory measures that clarify accountability and liability in cases of prompt leakage. Stronger contractual protections, including enhanced confidentiality clauses and data protection obligations with AI service providers, should also be implemented. In addition, corporations must invest in cybersecurity infrastructure, monitoring systems, and compliance mechanisms to detect and prevent unauthorized information exposure. The rapid growth of Generative Artificial Intelligence has transformed corporate operations while simultaneously introducing new legal and security challenges. Among these challenges, prompt leakage has emerged as a significant threat to trade secret protection and corporate confidentiality. As sensitive business intelligence increasingly flows through AI systems, the risk of unauthorized disclosure and corporate espionage continues to rise. This study concludes that traditional legal and governance frameworks alone are insufficient to address the complexities of AI-driven information leakage. Protecting trade secrets in the Generative AI

[6] E. Allan Farnsworth, Farnsworth on Contracts § 7.17 (4th ed. 2019).

ISSN: 2582-6433

economy requires a comprehensive approach that combines legal reform, corporate governance, technological safeguards, and organizational awareness. As AI adoption continues to expand, effective management of prompt leakage will become essential for ensuring corporate security, maintaining competitive advantage, and preserving long-term business resilience.