DOI: https://doi.org/10.31410/ITEMA.2023.1

Benefits and Risks: Combined Literature Review on the Use of AI Models and Company Data Disclosure

Stojan Ivanišević[1]
Rajko Ivanišević[2]
Aleksandar Ivić[3]

Received: October 9, 2023
Accepted: January 20, 2024
Published: May 28, 2024

Keywords:
AI;
AI models;
Data resource management;
Decision making;
Data security;
Risk assessment;
Data loss;
GDPR;
Data breach

Abstract: *As the use of artificial intelligence (AI) language models in business operations becomes an everyday reality, the management of company data resources, including the prevention of loss, raises critical questions about data privacy, security, and ethical considerations become increasingly important. This study presents a comprehensive examination - literature review, as a foundation for further research on AI model usage and the effective management of company data resources. The literature review surveys current research, revealing key themes and trends related to the topic, and offering insights into the reality of AI model use. This study aims to provide a holistic understanding of the complex interaction between AI, data resource management, and corporate decision-making.*

1. INTRODUCTION

In the era of digital transformation, the interaction of artificial intelligence (AI) models and corporate data has ignited a discussion about the way businesses use their data. AI models, driven by advanced machine learning techniques, have emerged as formidable tools capable of processing vast amounts of data, extracting insights, and augmenting human capabilities. The urge to exploit these models to enhance productivity and use AI models as tools to gain competitive advantage is tempting. The public availability of AI models such as Chat GPT allows any employee to add part of the company data into a prompt and expose the company resource (data) to the AI model. This event could potentially have a double negative effect: not only as company data/know-how/resources loss/disclosure but also as a disclosure of the client's data that the company is obliged to protect.

While the integration of AI models into business processes offers unprecedented opportunities, it also creates challenges, none more pressing than the safeguarding and effective management of company data resources. As organizations now use AI in the everyday work of the average employee to drive growth, optimize operations, and enhance customer experiences, they simultaneously engage with the complexities of data privacy, security, and ethical considerations. The delicate balance between using the benefits of AI-driven insights and guarding against the loss of company data resources is a point that is worthy of scientific discussion.

[1] No Affiliation
[2] University of Novi Sad – Faculty of Economics, Segedinski put 9-11, 24000 Subotica, Serbia
[3] No Affiliation

2. AI MODELS – CONCEPTS

Artificial Intelligence (AI) has emerged as a transformative force in the world of technology and data science. At the heart of AI lies the concept of AI models—sophisticated algorithms and computational structures that enable machines to simulate human intelligence. To understand the broader concept and research background, it is important to show concepts of AI models, shedding light on their underlying principles, applications, and significance in today's data-driven world.

Concepts: At its core, an AI model is a mathematical representation of a real-world process. These models leverage statistical and computational techniques to make predictions, classify data, or perform other tasks without explicit programming. The primary concepts underpinning AI models include:

Machine Learning (ML): Machine learning is a subset of AI that focuses on enabling machines to learn from data. ML models can identify patterns and make predictions by analyzing large datasets. This learning process enables the model to improve its performance over time.

Deep Learning: Deep learning is a specialized branch of ML that uses artificial neural networks to model and solve complex problems. These neural networks consist of interconnected layers of nodes, mimicking the human brain's structure. Deep learning models have achieved remarkable success in image recognition, natural language processing, and other tasks.

Supervised Learning: In supervised learning, an AI model is trained on labeled data, where the input data is paired with corresponding target outcomes. The model learns to make predictions or classifications by identifying patterns in the data and adjusting its parameters to minimize errors.

Unsupervised Learning: Unsupervised learning deals with unlabeled data, where the model seeks to discover hidden patterns or structures within the data. Clustering and dimensionality reduction are common tasks in unsupervised learning.

Reinforcement Learning: Reinforcement learning is a framework where an agent interacts with an environment to achieve specific goals. The agent receives feedback in the form of rewards or penalties, enabling it to learn optimal actions over time. This approach is widely used in robotics and game playing.

3. COMPANY DATA RESOURCES - DEFINITION AND SIGNIFICANCE

Today data is the lifeblood of modern organizations. From multinational corporations to small startups, businesses across the spectrum are accumulating vast volumes of data. This data, often referred to as company data resources, is a wide array of information assets that are pivotal for decision-making, strategy formulation, and operational efficiency. For clarification purposes, the authors attempted a comprehensive exploration of company data resources, defining their scope and significance in contemporary business operations. These resources can range from structured database data to unstructured forms of communication, such as emails and social media interactions. Borges et al. (2021) stated "Huge volume of data in diverse formats being generated faster than ever has demanded the development of new technologies, resulting in

an acceleration of technological progress, which includes increasing the computational processing capacity and the development of new AI techniques. Many organizations are motivated to adopt AI technologies, mainly by their disruptive potential demonstrated by top digital corporations. The text also highlights the potential benefits, challenges, and opportunities of integrating AI into organizational strategy".

At its core, company data resources encompass the collective information assets that an organization collects, manages, and analyzes to facilitate its day-to-day operations, strategic planning, and competitive positioning. These resources span a spectrum of data types, each with its characteristics and relevance to business operations:

1. Structured Database Data: Structured data, stored in relational databases, represents the backbone of many company data resources. It includes organized information such as customer profiles, transaction records, and inventory levels. Structured data is amenable to traditional data analysis techniques and is foundational for business intelligence.
2. Unstructured Data: In contrast to structured data, unstructured data lacks a predefined format. This category includes textual documents, multimedia content, and social media posts. Unstructured data is abundant and valuable for extracting insights through natural language processing (NLP) and image analysis.
3. Semi-Structured Data: Semi-structured data bridges the gap between structured and unstructured data. It includes formats like XML or JSON, often used for data exchange and flexible data representation.
4. Email Communication: Email communication serves as a rich source of data resources within organizations. Email archives contain a historical record of interactions, negotiations, and decisions. These archives are critical for compliance, dispute resolution, and knowledge management.
5. Social Media Interactions: Social media platforms have evolved into potent channels for customer engagement and feedback. Analyzing social media data offers insights into market sentiment, brand perception, and consumer preferences.
6. Sensor and IoT Data: With the proliferation of sensors and the Internet of Things (IoT), organizations gather data from physical devices and sensors. This data informs predictive maintenance, supply chain optimization, and product performance monitoring.
7. Financial Data: Financial data resources encompass financial statements, income reports, and transaction histories. These data types are essential for financial analysis, budgeting, and regulatory compliance.

4. LEVERAGING COMPANY DATA RESOURCES AND AI MODELS FOR ENHANCED PRODUCTIVITY AND DECISION-MAKING

Wamba-Taguimdje et al. (2020) and Fountaine et al. (2019) focus on the business value of AI-based tools and how they can positively impact an organization's performance. However, their work also discusses the importance of culture, structure, and ways of working to support road AI tools adoption, and the need for businesses to align their culture and structure to support AI adoption.

In today's digitally interconnected business landscape, the effective utilization of company data resources, coupled with the integration of sophisticated AI models, has emerged as a mainstream practice for organizational success. Employees across diverse functions and hierarchies use AI language models to foster productivity gains and elevate decision-making to a new level of sophistication.

AI-Powered Efficiency and Innovation: Beyond the realm of traditional data analysis, AI models have revolutionized how employees interact with data. Machine learning algorithms, natural language processing (NLP), and predictive analytics are augmenting human capabilities. AI automates repetitive tasks, extracts meaningful insights from unstructured data like emails and social media interactions, and facilitates predictive analysis that was previously unattainable. Employees now wield AI tools to unlock operational efficiencies, explore innovative possibilities, and enhance their contributions to the organization.

The integration of AI models plays a pivotal role in decision-making processes. It brings about a transformation in decision-making by bolstering accuracy and speed. Employees, equipped with AI-augmented data resources, are not only able to process vast volumes of data swiftly but also with exceptional precision.

In essence, the synergy between company data resources and AI models represents a monumental shift in the way employees operate within organizations. It transcends traditional boundaries, creating a data-driven culture where employees leverage the power of data and AI to enhance productivity, drive innovation, and make decisions that propel their organizations toward success in an increasingly dynamic and competitive business environment.

However, the authors state that the use of AI models is not only limited to the IT department within the company but is available to all employees as an open-source online tool. This by default enables the employees to use them without sufficient understanding and proper training. This creates many challenges which are discussed in the next chapter.

5. CHALLENGES IN THE USE OF COMPANY DATA RESOURCES IN INTERACTION WITH AI MODELS

5.1. Data Exposure and the Risk of Loss to the Company

The integration of language models into company workflows has enabled transformative possibilities for natural language processing and communication. However, this integration also introduces a critical concern - data exposure. When sensitive company data, whether from databases or emails, is shared with a language model, it poses a significant risk that can lead to substantial loss for the organization. Exposing sensitive company data to a language model without proper safeguards can result in data security and confidentiality breaches. Language models are designed to process and generate text, and in doing so, they may inadvertently reveal sensitive information. Unauthorized access, data leaks, or even accidental disclosures through generated text can compromise confidential business data. Such breaches can lead to reputational damage, legal liabilities, and loss of customer trust.

5.2. Compliance Violations:

Many industries are subject to strict regulatory frameworks that mandate the protection of sensitive data. For example, healthcare organizations must comply with the Health Insurance Portability and Accountability Act (HIPAA), which governs the privacy and security of patient health information. Similarly, financial institutions are bound by the Sarbanes-Oxley Act (SOX) and other regulations. Exposing data to a language model without appropriate measures to maintain compliance can result in violations, leading to hefty fines and legal consequences.

5.3. Intellectual Property Risks:

Companies often store proprietary information and intellectual property in their databases and email systems. When such data is exposed to a language model, there is a risk that it may be inadvertently included in generated content. This could lead to the unintentional sharing of intellectual property or trade secrets, potentially benefiting competitors or exposing the company to litigation.

5.4. Data Leakage through Generated Content:

Language models generate text based on patterns learned from the data they have been trained on. In some cases, this means that the model may generate text that unintentionally contains sensitive or confidential information from the data it has been exposed to. This text could be used in various ways, such as in customer communications, reports, or public-facing content, inadvertently exposing sensitive data to external parties.

5.5. Ethical and Privacy Concerns:

Exposing sensitive data to a language model raises ethical and privacy concerns, particularly when it comes to personal data about employees, customers, or partners. Mishandling such data can lead to breaches of trust and damage to the company's reputation.

5.6. Loss of Competitive Advantage:

Companies often rely on their data resources as a competitive advantage. Data exposure, especially if it leads to intellectual property theft or the leaking of sensitive business strategies, can erode this advantage and compromise the company's market position.

6. LITERATURE REVIEW

In this chapter, the authors explore what various scientific studies have to say about how companies use their data with AI models. This article looks at the most widely discussed research papers and what they reveal on this topic. The authors aim to distill the main ideas and challenges presented in scientific literature. By doing this, we aim to provide you with a clear overview of the findings from multiple studies, shedding light on how businesses are leveraging data and AI use benefits. This review should offer valuable insights drawn from existing scientific research, which can inform further inquiry and practical applications in the ever-evolving landscape of modern business and technology.

Methodology: This systematic literature review was put together using Kitchenham's (2004) methodology for doing so. Kitchenham (2004) claims that a systematic literature review may be broken down into three key stages: planning, carrying out, and reporting. A list of research questions, as well as inclusion and exclusion standards, are the main topics of the literature review.

Planning: In the planning stage of the systematic literature review, it is important to acknowledge the need for writing the review itself for a certain topic. The need for a systematic literature review can be established by evaluating already existing scientific literature reviews in the chosen

subject area. To the author's best knowledge, no systematic review of the literature has been found that summarizes the challenges and potential risks of exposing company data to open AI Models. Therefore, this systematic literature review is the first one to be written on the defined topic.

According to the chosen methodology, the following research questions were established:

RQ1: Are there any studies that discuss the use of company data in the interaction with open AI models?

RQ2: What are the main possible risks of data exposure to the AI models according to these studies?

RQ3: Can these risks be avoided or mitigated?

The Scopus database was searched for this literature review. Search terms defined for search in this database are:

- the paper has to be in the area of AI, AI data models, Company Data Use,
- the paper is written in English,
- the paper is written between 2019-2023.,
- the paper is a scientific article,
- the paper must represent a study in which challenges or opportunities of using AI models with company or organization data.

Conducting the review: The researchers carefully examined 64 scientific papers that matched the defined criteria. Out of those 15 papers were selected as insightful and helpful for the study related to the abovementioned research questions.

6.1. Reporting the review

The authors selected relevant papers and created summaries of the parts that are relevant to the research questions.

Lee et al. (2019) discuss the potential benefits of using AI models to analyze company data, such as improving performance and innovation. However, the author also acknowledges that there are challenges associated with data use, such as data quantity and uncertainty, and that companies may lack the internal expertise to effectively implement AI technology. Additionally, the author notes that there may be ethical concerns related to data privacy and security that need to be addressed.

The study by Di Vaio et al. (2020) consider intellectual property, data privacy, liability, and compliance with evolving laws and standards. They state "AI relies heavily on data, and ensuring the quality, integrity, and security of data used in SBMs is crucial. Data governance and data management become critical aspects of AI adoption".

"AI models can be transformative for businesses but also highlight potential risks and challenges associated with data use. These include issues related to data exposure to AI models, data loss, and the need for clear processes towards consent. The author suggests that future research should investigate these factors and their implications for the strategic business value of digital transformation. Additionally, the author emphasizes the importance of full disclosure and

transparency about the intelligent agent or hybrid systems to clarify the roles of humans and machines" according to Akter et al. (2022).

Cheatham et al. (2019) warn that "ingesting, sorting, linking, and properly using data has become increasingly difficult as the amount of unstructured data being ingested from sources such as the web, social media, mobile devices, sensors, and the Internet of Things has increased. As a result, it's easy to fall prey to pitfalls such as inadvertently using or revealing sensitive information hidden among anonymized data." The authors also mention that technology and process issues across the entire operating landscape can negatively impact the performance of AI systems and that security snags are another emerging issue. The author emphasizes that leaders need to be aware of these issues as they work to stay in line with privacy rules and otherwise manage reputation risk".

Reddy et al. (2020) emphasize the importance of protecting patient confidentiality and obtaining informed consent for the usage of personal health data in AI systems. The author also highlights the risks of privacy breaches and data loss associated with sharing patient data with AI developers. The author recommends seeking fully informed consent from patients and anonymizing data to minimize the risks of analysing confidential and sensitive data. The author also suggests using public datasets to develop AI software to minimize privacy breaches. Overall, the author stresses the need for ethical and transparent practices in the use of company data with AI models to prevent potential issues related to data exposure and loss.

Campbell et al. (2020) note that there are concerns about data exposure and loss, particularly considering recent data breaches and harvesting of data without consumer consent. The author suggests that firms need to be aware of the increasingly important challenges of privacy and regulation and that consumers are growing more concerned about what data is being collected from them and how it is being used by marketers.

Loureiro et al. (2021) discuss the potential benefits of using AI to gain insights from vast amounts of data that organizations produce or have access to. Additionally, the author mentions that there is a risk of data loss when using AI models, as the models may not be able to accurately interpret complex data.

Enholm et al. (2022) present a balanced view of the potential benefits and challenges of using AI in company data analysis.

Bharadiya (2023) emphasizes the importance of ethical considerations in AI development and deployment, particularly in terms of protecting user privacy and ensuring compliance with data protection regulations. The use of vast amounts of data, often including sensitive and personal information, requires organizations to implement robust security measures, data anonymization techniques, and secure data handling practices to safeguard user information. Additionally, the author highlights the potential risks associated with biased data and unintended consequences and stresses the need for transparency and accountability frameworks to detect errors, biases, or unethical behaviour and facilitate remedial actions.

Rudin and Radin (2019) discuss the potential issues with using black box models in AI, particularly in terms of data exposure and data loss. They argue that trusting a black box model means trusting not only the model's equations but also the entire database it was built from, which can contain imperfections and errors. The author suggests that using interpretable models can help

mitigate these issues and improve transparency and accountability in industries such as finance and healthcare.

Gregory et al. (2021) emphasize the importance of treating data as a strategic asset and carefully managing it to reap the benefits of data network effects. The author suggests that developing or acquiring a superior platform AI capability is not enough, and that attention must be paid to three key mechanisms of data network effects: (1) data stewardship, (2) user-centric design, and (3) platform legitimation. The author also discusses the need for responsible use of personal data collected from users, implementing principles of privacy-by-design and security-by-design, and ensuring the explainability of predictions generated by AI on the platform. The author does not specifically address issues of data exposure to AI models or data loss.

Overgoor et al. (2019) discuss the use of AI to support marketing decisions and provide a process for managers to use when executing a Marketing AI project. The authors note that while AI has proven to be useful in many applications, many firms lack a process by which to execute a Marketing AI project. The article also discusses issues that might arise, such as data exposure to the AI models and data loss. The authors suggest that companies should be transparent about their use of AI and ensure that their data is secure. The authors mention two issues related to data in the context of using AI for marketing: data exposure to the AI models and data loss. Data exposure refers to the possibility that sensitive or confidential data may be exposed to the AI models, which could lead to privacy violations or other negative consequences. Data loss refers to the possibility that data may be lost or corrupted during the process of using AI for marketing, which could lead to inaccurate or incomplete results. The authors suggest that companies should be aware of these issues and take steps to mitigate them.

Jöhnk et al. (2021) suggest that change management can help employees understand and cope with AI-induced organizational change and that data security and privacy concerns should be addressed to prevent data exposure and loss. Yes, the authors suggest that data security and privacy concerns should be addressed to prevent data exposure and loss. They note that data breaches can lead to significant financial and reputational damage to organizations and that AI-based systems can be vulnerable to cyber-attacks. Therefore, they recommend that organizations implement appropriate security measures, such as encryption, access control, and monitoring, to protect their data from unauthorized access and misuse. Additionally, they suggest that organizations should comply with relevant data protection regulations, such as the General Data Protection Regulation (GDPR), to ensure that personal data is processed lawfully and transparently.

Loureiro et al. (2021) discuss the increasing need for companies to integrate Big Data information to better serve the consumer and improve production efficiency. However, the use of AI models to analyze this data raises concerns about data exposure and loss. The author notes that deep learning models are often black boxes, making it difficult to understand how they arrive at their predictions. To address this issue, the author suggests the use of eXplainable AI (XAI) algorithms, which can provide more transparency and accountability in AI applications. Additionally, the author emphasizes the importance of ethical and legal issues regarding the data protection of citizens and the new role of robots in society.

According to Benbya et al. (2021), "Researchers should explore potential unintended consequences that arise as AI is increasingly integrated into decision-making practices, including data exposure to AI models and data loss".

7. CONCLUSION

The authors think that without any doubt there are substantial benefits from the use of AI models in day-to-day business activities. However, this new opportunity brings new dangers and security pitfalls. Business organizations should make adjustments in their strategy and policies to harness the power of AI Models while minimizing the potential risks. To mitigate the risk of data exposure when using language models, organizations should implement strict data access controls, encryption mechanisms, and data anonymization techniques. Additionally, they should carefully review and redact sensitive information from data before it is exposed to the model. Employee training and awareness programs can also play a vital role in preventing unintentional data exposure.

In conclusion, data exposure from databases or other data sources to language models presents a real risk to companies, encompassing data security breaches, compliance violations, intellectual property risks, and ethical concerns. Recognizing and mitigating this risk is essential for organizations seeking to leverage language models while safeguarding their data assets and reputation. Proper data protection measures and adherence to regulatory requirements are indispensable to achieve benefits and minimize the risk.

References

Akter, S., Michael, K., Uddin, M. R., McCarthy, G., & Rahman, M. (2022). Transforming business using digital innovations: The application of AI, blockchain, cloud and data analytics. *Annals of Operations Research*, 1-33.

Benbya, H., Pachidi, S., & Jarvenpaa, S. (2021). Special issue editorial: Artificial intelligence in organizations: Implications for information systems research. *Journal of the Association for Information Systems, 22*(2), 10.

Bharadiya, J. P. (2023). Machine Learning and AI in Business Intelligence: Trends and Opportunities. *International Journal of Computer (IJC), 48*(1), 123-134.

Borges, A. F., Laurindo, F. J., Spínola, M. M., Gonçalves, R. F., & Mattos, C. A. (2021). The strategic use of artificial intelligence in the digital era: Systematic literature review and future research directions. *International Journal of Information Management, 57*, 102225.

Campbell, C., Sands, S., Ferraro, C., Tsao, H. Y. J., & Mavrommatis, A. (2020). From data to action: How marketers can leverage AI. *Business Horizons, 63*(2), 227-243.

Cheatham, B., Javanmardian, K., & Samandari, H. (2019). Confronting the risks of artificial intelligence. *McKinsey Quarterly, 2*(38), 1-9.

Di Vaio, A., Palladino, R., Hassan, R., & Escobar, O. (2020). Artificial intelligence and business models in the sustainable development goals perspective: A systematic literature review. *Journal of Business Research, 121*, 283-314. https://doi.org/10.1016/j.jbusres.2020.08.019

Enholm, I. M., Papagiannidis, E., Mikalef, P., & Krogstie, J. (2022). Artificial intelligence and business value: A literature review. *Information Systems Frontiers, 24*(5), 1709-1734.

Fountaine, T., McCarthy, B., & Saleh, T. (2019). Building the AI-powered organization. *Harvard Business Review, 97*(4), 62-73.

Gregory, R. W., Henfridsson, O., Kaganer, E., & Kyriakou, H. (2021). The role of artificial intelligence and data network effects for creating user value. *Academy of Management Review, 46*(3), 534-551.

Jöhnk, J., Weißert, M., & Wyrtki, K. (2021). Ready or not, AI comes—an interview study of organizational AI readiness factors. *Business & Information Systems Engineering, 63*, 5-20.

Kitchenham, B. (2004). Procedures for Performing Systematic Reviews (Technical Report). Keele University.

Lee, J., Suh, T., Roy, D., & Baucus, M. (2019). Emerging technology and business model innovation: the case of artificial intelligence. *Journal of Open Innovation: Technology, Market, and Complexity, 5*(3), 44.

Loureiro, S. M. C., Guerreiro, J., & Tussyadiah, I. (2021). Artificial intelligence in business: State of the art and future research agenda. *Journal of Business Research, 129*, 911-926.

Overgoor, G., Chica, M., Rand, W., & Weishampel, A. (2019). Letting the computers take over: Using AI to solve marketing problems. *California Management Review, 61*(4), 156-185.

Reddy, S., Allan, S., Coghlan, S., & Cooper, P. (2020). A governance model for the application of AI in health care. *Journal of the American Medical Informatics Association, 27*(3), 491-497.

Rudin, C., & Radin, J. (2019). Why are we using black box models in AI when we don't need to? A lesson from an explainable AI competition. *Harvard Data Science Review, 1*(2), 1-9.

Wamba-Taguimdje, S. L., Fosso Wamba, S., Kala Kamdjoug, J. R., & Tchatchouang Wanko, C. E. (2020). Influence of artificial intelligence (AI) on firm performance: the business value of AI-based transformation projects. *Business Process Management Journal, 26*(7), 1893-1924.