AUDİT 2025, 1 (47), səh. 112-121.
AUDIT 2025, 1 (47), pp. 112-121.
АУДИТ 2025, 1 (47), стр. 112-121.

DOI: 10.59610/bbu1.2025.1.10

Sadiq Sarvan Isayev,
Ph.D. Student,
Baku Business University,
E-mail: sadigisayev13@gmail.com

UDC: 004.8, 004.056.55, 17:004, 316.774, 351.746
JEL: D63, K24, O33, D83, L86

BALANCING INNOVATION AND PRIVACY: ETHICAL CONSIDERATIONS IN AI-DRIVEN DATA USAGE

A B S T R A C T

The purpose of the research is to critically examine the ethical considerations arising from the intersection of AI technologies and personal data usage. Specifically, the study seeks to explore the balance between personalization and privacy, evaluate the effectiveness of privacy-preserving technologies, and analyze the responsibilities of businesses and governments in safeguarding data.

The methodology of the research - this research employs a mixed-methods approach, combining qualitative and quantitative analyses to explore the ethical, technical, and regulatory dimensions of AI and data privacy. The study draws on a comprehensive review of recent academic literature, industry reports, and case studies to identify key trends, challenges, and solutions.

The practical importance of the research - the findings of this research have significant practical implications for businesses, policymakers, and society. For businesses, the study highlights the importance of adopting ethical data practices and privacy-preserving technologies to build trust with customers and gain a competitive advantage.

The originality and scientific novelty of the research - this research contributes to the issues of AI ethics and data privacy by offering a comprehensive analysis of the challenges and opportunities at the intersection of these fields. While previous studies have explored the ethical implications of AI or the technical aspects of privacy-preserving technologies in isolation, this paper integrates these perspectives to provide a holistic understanding of the issues.

Keywords: artificial intelligence, innovation, data privacy, ethical concerns, personalization.

INTRODUCTION

The rapid adoption of artificial intelligence (AI) has brought a new era of digital transformation, reshaping industries through unprecedented innovation. AI-driven technologies, from personalized recommendation systems to automated decision-making tools, have enabled businesses and governments to optimize efficiency, enhance user experiences, and create data-driven strategies. However, this progress has also sparked a critical ethical debate—how can innovation be balanced with the fundamental right to privacy? The increasing reliance on AI

AUDİT 2025, 1 (47), səh. 112-121.
AUDIT 2025, 1 (47), pp. 112-121.
АУДИТ 2025, 1 (47), стр. 112-121.

for data collection and analysis has raised concerns regarding transparency, user autonomy, and potential misuse of personal information.

The ethical considerations surrounding AI-driven data usage extend beyond corporate responsibility to encompass broader societal and regulatory implications. High-profile incidents, such as the Cambridge Analytica scandal, have demonstrated the risks associated with unchecked data collection, underscoring the urgent need for robust privacy-preserving mechanisms. While legislative frameworks like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) aim to enforce responsible data practices, the rapid evolution of AI often outpaces regulatory developments, creating loopholes that can be exploited.

This paper critically examines the ethical dilemmas at the intersection of AI and data privacy, analyzing the responsibilities of businesses, governments, and technology developers in ensuring ethical data stewardship. Through a comprehensive review of existing privacy-preserving technologies, corporate best practices, and evolving regulatory frameworks, the study seeks to illuminate the challenges and opportunities in fostering a sustainable AI-driven ecosystem. Striking the right balance between innovation and privacy is not merely a technical challenge but a societal imperative - one that requires collaborative efforts across industries and policymakers to protect individual rights while enabling AI's transformative potential.

Ethical Considerations in Data Collection and Usage

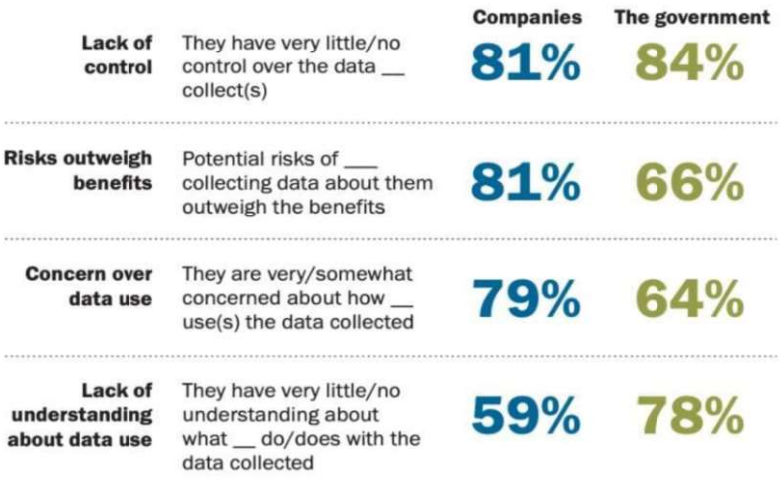
Artificial intelligence (AI) has become a transformative force in the global economy, driving innovation and efficiency across industries. According to Bughin, AI has the potential to contribute up to $13 trillion to the global economy by 2030, with significant impacts on productivity and business models [4, 5]. This projection overlooks a crucial factor: the diminishing role of the human element in economic processes. The economy is fundamentally driven by human creativity, decision-making, and adaptability—qualities that AI, despite its advancements, cannot fully replicate. As AI takes over tasks traditionally performed by humans, the displacement of labor may lead to economic imbalances, rising unemployment, and reduced consumer purchasing power. Without human-driven innovation, AI's productivity gains may not translate into sustainable economic growth. Moreover, AI-driven business models often centralize wealth among a few technology firms rather than fostering widespread economic benefits.

For instance, AI-powered automation has streamlined supply chain operations, while predictive analytics has enhanced decision-making in sectors like finance and healthcare. AI-driven personalization has emerged as a key driver of business success, enabling companies to deliver tailored experiences that enhance customer satisfaction and loyalty. According to a study by McKinsey & Company, personalized recommendations can increase revenue by up to 15% in retail and e-commerce sectors [10, 12]. For example, Amazon's recommendation engine, which analyzes user behavior to suggest products, has been instrumental in driving sales and customer retention [12, 45]. Similarly, streaming platforms like Spotify use AI to curate personalized playlists, improving user engagement and retention. However, the integration of AI into business processes is not without challenges. As noted by Brynjolfsson and McAfee, the reliance of AI on personal data raises ethical and practical concerns, particularly regarding privacy and security [5, 32]. This tension between economic benefits and ethical considerations sets the stage for a deeper exploration of AI's role in the economy. This raises ethical questions

AUDİT 2025, 1 (47), səh. 112-121.
AUDIT 2025, 1 (47), pp. 112-121.
АУДИТ 2025, 1 (47), стр. 112-121.

about the balance between personalization and privacy, a theme that will be explored further in the following sections.

The reliance of AI on personal data has sparked significant privacy concerns, particularly regarding intrusive data collection practices and the potential for misuse. A report by the Pew Research Center found that 81% of Americans feel they have little or no control over the data collected about them by companies:



Source: www.pewresearch.org

Figure 1. The percentages of Americans who feel they have little or no control over the data collected about them by companies.

High-profile incidents, such as the Cambridge Analytica scandal, have drawn significant attention to the dangers and ethical concerns surrounding the misuse of personal data. In this case, sensitive user information was systematically harvested and exploited for political manipulation without the explicit consent or awareness of the individuals involved [6, 3]. Such events have exposed the critical vulnerabilities inherent in centralized data systems, where massive corporations and organizations amass vast quantities of personal data with relatively little accountability or transparency. The lack of robust oversight in these systems creates an environment where data can be easily misused, leading to significant consequences for both individuals and society at large.

Moreover, the aggregation of personal data on such a large scale significantly increases the risk of data breaches, identity theft, and unauthorized surveillance. When centralized entities store immense amounts of sensitive information, they become prime targets for cyberattacks, putting millions of users at risk. Beyond the immediate threats of hacking and theft, the misuse of data can also enable invasive surveillance practices, eroding privacy and civil liberties. These concerns are not merely speculative or theoretical; they have been demonstrated repeatedly in real-world scenarios, with far-reaching implications for individuals, communities, and democratic institutions.

To comprehensively address these privacy concerns, researchers and technologists have developed a range of privacy-preserving technologies that aim to balance the need for data-driven insights with the protection of individual privacy. These advancements are particularly

AUDİT 2025, 1 (47), səh. 112-121.
AUDIT 2025, 1 (47), pp. 112-121.
АУДИТ 2025, 1 (47), стр. 112-121.

crucial in an era where vast amounts of personal and sensitive data are being processed by AI-driven systems across various sectors, including healthcare, finance, and human resource management.

One notable approach is federated learning, which enables AI models to be trained across multiple decentralized devices or servers without requiring the transfer of raw data to a central repository. This decentralized approach minimizes the risk of data breaches and unauthorized access, as sensitive information remains on the local device while only model updates are shared. Federated learning has been successfully applied in industries such as healthcare, where patient data privacy is a top priority, and in mobile applications, where user data is continuously processed for personalized services [9, 3]. However, while federated learning offers significant privacy advantages, its implementation is accompanied by notable challenges. It demands considerable computational power and network bandwidth, which may not be feasible for all organizations, particularly smaller enterprises with limited technological infrastructure. Additionally, ensuring consistent model performance across heterogeneous data sources remains a key research challenge. Another critical privacy-preserving technique is differential privacy, which enhances data security by introducing mathematically calibrated noise to datasets before they are analyzed. This ensures that individual data points cannot be uniquely identified, thereby preventing re-identification attacks. Differential privacy has been widely adopted by major technology firms and governmental organizations to facilitate the secure sharing of statistical data while preserving the anonymity of individuals. Despite its advantages, the use of differential privacy can introduce trade-offs, particularly in terms of data utility. The addition of noise can sometimes degrade the accuracy of AI models, making it necessary to strike a balance between privacy protection and model effectiveness.

Beyond merely implementing technical safeguards, companies hold both a moral and legal duty to ensure the protection of user data. In today's digital landscape, ethical data practices go beyond regulatory compliance; they form an essential pillar of corporate social responsibility. Organizations that actively prioritize transparency and data security not only fulfill their legal obligations but also cultivate trust and long-term loyalty among their customers. As highlighted by the World Economic Forum (2020), businesses that demonstrate a commitment to responsible data management can significantly enhance their reputational standing and strengthen consumer confidence [15].

A compelling example of ethical data stewardship can be seen in Apple's approach to user privacy. The company's introduction of the App Tracking Transparency (ATT) feature allows users to control which apps can track their activity, empowering individuals to make informed decisions about their personal information. This initiative has been widely praised as a benchmark for consumer-first data policies [2, 7]. By prioritizing user rights over unchecked data collection, Apple has positioned itself as a leader in ethical digital practices, setting an industry precedent that others are being urged to follow.

However, not all companies share this commitment to data ethics. Many businesses continue to place profit at the forefront, leveraging user data as a commercial asset without implementing sufficient privacy safeguards. In some cases, personal information is collected, analyzed, and monetized without explicit user consent, raising serious ethical concerns. This ongoing tension between corporate interests and consumer privacy underscores the pressing need for a broader cultural shift within the business world. Ethical considerations should no

AUDİT 2025, 1 (47), səh. 112-121.
AUDIT 2025, 1 (47), pp. 112-121.
АУДИТ 2025, 1 (47), стр. 112-121.

longer be viewed as an afterthought but rather as a fundamental component of business strategy and decision-making. To drive this transformation, organizations must integrate ethical data governance into their operational frameworks, ensuring that privacy protection is embedded in their products and services from the outset. This requires not only compliance with existing regulations but also a proactive approach to establishing industry best practices. By adopting a user-centric mindset and prioritizing responsible data handling, businesses can build stronger, more sustainable relationships with their customers while fostering a digital ecosystem that values privacy and security.

In addition to moral and legal responsibilities, regulatory frameworks play an essential role in shaping ethical data practices and ensuring that organizations adhere to established privacy standards. Governments and policymakers worldwide have recognized the need for clear guidelines to protect user data, leading to the development of comprehensive legislation aimed at safeguarding individual privacy rights. Among the most influential data protection laws are the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States. These regulations have redefined corporate obligations concerning data transparency, user consent, and accountability. GDPR, for example, grants individuals the right to access, correct, and delete their personal data, placing stringent requirements on businesses regarding data processing and storage. Non-compliance can result in severe financial penalties, pushing organizations to adopt more responsible data management practices [14, 45]. Similarly, CCPA empowers consumers by giving them greater control over how their personal information is collected and shared, reinforcing the importance of transparency in digital transactions.

The introduction of these legal frameworks has set a global precedent, encouraging companies beyond the EU and the U.S. to align with higher data protection standards. Many businesses, particularly those operating internationally, have voluntarily implemented GDPR-like policies to maintain customer trust and ensure compliance across different markets. However, despite these advancements, regulatory enforcement remains a significant challenge. Differences in jurisdiction, inconsistent implementation, and resource limitations often hinder the effectiveness of these laws. Some companies exploit these gaps by engaging in data practices that, while technically legal in certain regions, may still be ethically questionable.

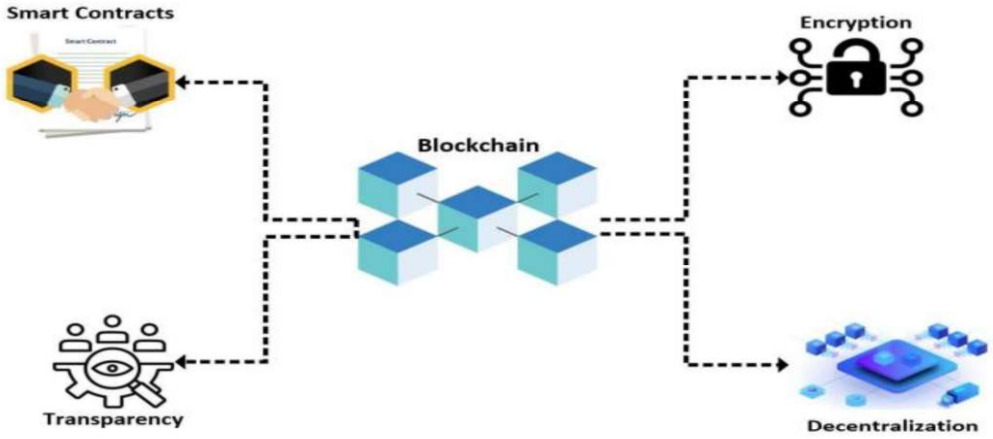
Another key issue is that legislation often struggles to keep pace with technological advancements. The rapid evolution of artificial intelligence, big data analytics, and machine learning continuously reshapes the digital landscape, sometimes outstripping the ability of policymakers to develop timely and effective regulations. This lag creates legal loopholes that can be manipulated, allowing companies to engage in aggressive data collection practices before regulations catch up. In order to address these challenges, regulatory bodies must adopt a more adaptive and forward-thinking approach to data governance. This includes regularly updating policies, collaborating with industry experts, and leveraging AI-driven compliance tools to detect and prevent data misuse in real time. By implementing more dynamic regulatory frameworks, governments can ensure that privacy protections remain robust and relevant in an era of constant technological change. Only through such proactive measures can businesses, consumers, and policymakers collectively create a sustainable and ethical data ecosystem that balances innovation with individual rights.

Governments play a dual role in the AI ecosystem: protecting user privacy and fostering innovation. On one hand, they are responsible for enacting and enforcing policies that safeguard individual rights. On the other hand, they must create an environment conducive to technolo-

AUDİT 2025, 1 (47), səh. 112-121.
AUDIT 2025, 1 (47), pp. 112-121.
АУДИТ 2025, 1 (47), стр. 112-121.

gical advancement and economic growth. Striking this balance is no easy task. Overly restrictive regulations can stifle innovation, while lax policies can lead to privacy violations and public distrust. For example, the European Union's approach to AI regulation, which emphasizes stringent data protection, has been criticized for potentially hindering the competitiveness of European businesses [13, 10]. Conversely, the United States' more laissez-faire approach has been accused of prioritizing corporate interests over individual rights. These contrasting approaches underscore the complexity of government's role in shaping the future of AI and data privacy.

Furthermore, decentralized data systems offer a promising alternative to mitigate the risks associated with centralized data repositories. These systems, particularly those powered by blockchain technology, provide a fundamentally different approach to data management by distributing information across a network of nodes rather than storing it in a single, centralized database. This decentralized structure significantly reduces vulnerabilities, minimizing the risk of single points of failure, large-scale data breaches, and unauthorized access. One of the most compelling advantages of blockchain-based data management is its transparency and immutability. Each data transaction recorded on a blockchain is cryptographically secured, time-stamped, and nearly impossible to alter, ensuring that records remain tamper-proof and verifiable.



Source: www.researchgate.net

Figure 2. The four main features of blockchain technology.

The given figure illustrates how blockchain technology ensures decentralized data control by integrating smart contracts, encryption, transparency, and decentralization. Blockchain, at the center of the image, represents a distributed ledger that operates without a central authority. Smart contracts automate transactions and agreements, reducing the need for intermediaries and ensuring trust through self-executing code. Encryption secures data by making it accessible only to authorized parties, safeguarding privacy and integrity. Transparency ensures that all transactions are recorded and verifiable, preventing fraud and increasing accountability. Finally, decentralization distributes data across multiple nodes, eliminating single points of failure and enhancing system resilience. Together, these elements contribute to a system where data is controlled in a decentralized manner, ensuring security, trust, and autonomy without reliance on centralized entities.

AUDİT 2025, 1 (47), səh. 112-121.
AUDIT 2025, 1 (47), pp. 112-121.
АУДИТ 2025, 1 (47), стр. 112-121.

This built-in accountability mechanism can enhance trust in digital ecosystems, as stakeholders can audit and verify data transactions in real time. Such attributes make blockchain particularly valuable in industries that require high levels of security and data integrity, including finance, healthcare, and supply chain management. A notable initiative that aligns with the principles of decentralized data control is Solid, a project developed by Tim Berners-Lee, the creator of the World Wide Web. Solid introduces a model where individuals can store their personal data in Personal Online Data Pods (PODs), giving them direct control over who can access their information. This approach challenges the current paradigm of centralized data ownership, where tech giants collect and monetize user data with minimal transparency [3, 6]. By shifting power back to users, decentralized systems like Solid could redefine how personal data is managed and shared.

Ultimately, the success of AI technologies depends on the trust of users. Businesses that prioritize ethical data practices can differentiate themselves in a competitive market, building long-term relationships with customers based on transparency and accountability. For instance, companies that adopt privacy-by-design principles, embedding data protection into the development process from the outset, are more likely to earn the trust of their users [7, 3]. Additionally, clear communication about data practices, such as providing easily accessible privacy policies and obtaining explicit consent, can further enhance trust. In an era where data breaches and privacy scandals are increasingly common, businesses that demonstrate a commitment to ethical data practices can gain a significant competitive advantage.

CONCLUSIONS

The rapid adoption of artificial intelligence (AI) has revolutionized the global economy, driving innovation and personalization across industries. However, this progress is accompanied by significant ethical challenges, particularly regarding the collection and use of personal data. This paper has explored the tension between AI's reliance on data and the imperative to protect privacy, highlighting the need for a balanced approach that safeguards individual rights while fostering innovation.

AI-driven personalization offers immense value, enhancing user experiences and driving business outcomes. Yet, the extensive data collection required raises critical privacy concerns, as evidenced by high-profile cases of data misuse. Privacy-preserving technologies, such as federated learning and differential privacy, provide promising solutions, but their implementation requires addressing technical and practical challenges.

Corporate responsibility is central to addressing these ethical dilemmas. Businesses must prioritize transparency, accountability, and privacy-by-design principles to build trust with users. Regulatory frameworks like GDPR and CCPA play a crucial role in shaping ethical data practices, but their effectiveness depends on consistent enforcement and adaptation to technological advancements. Governments must balance privacy protection with innovation, creating policies that support both individual rights and economic growth.

Decentralized data systems, such as blockchain, offer innovative ways to empower users and reduce reliance on centralized data repositories. However, challenges related to scalability

AUDİT 2025, 1 (47), səh. 112-121.
AUDIT 2025, 1 (47), pp. 112-121.
АУДИТ 2025, 1 (47), стр. 112-121.

and adoption must be addressed to realize their full potential. Ultimately, the success of AI depends on user trust, which can be fostered through ethical data practices and a commitment to transparency.

In conclusion, the ethical challenges posed by AI and data privacy are complex but not insurmountable. By integrating technological innovation, corporate responsibility, regulatory oversight, and user empowerment, society can harness the benefits of AI while upholding privacy and ethical principles. This paper has sought to contribute to this dialogue, emphasizing the need for a collaborative and forward-looking approach to ensure that AI serves the greater good.

REFERENCES:

1. Acar, A., Aksu, H.,Uluagac, A. S., & Conti, M. (2018). A Survey on Homomorphic Encryption Schemes: Theory and Implementation. ACM Computing Surveys, p. 1–35.
2. Apple. (2021). App Tracking Transparency: Empowering Users to Control Their Data. Apple Privacy Report, p. 7.
3. Berners-Lee, T. (2018). Solid:A Decentralized Web Project. MIT Technology Review, p 6.
4. Bughin, J., Hazan, E., Ramaswamy, S., Chui, M., Allas, T., Dahlström, P., Henke, N., & Trench, M. (2018). Artificial Intelligence: The Next Digital Frontier? McKinsey Global Institute, p. 5.
5. Brynjolfsson, E., & McAfee, A. (2017). The Business of Artificial Intelligence. Harvard Business Review, p. 32.
6. Cadwalladr, C. (2018). The Cambridge Analytica Scandal. The Guardian, p. 3.
7. Cavoukian, A. (2012). Privacy by Design: The 7 Foundational Principles. Information and Privacy Commissioner of Ontario, p. 3.
8. Dwork, C., McSherry, F., Nissim, K., & Smith, A. (2006). Calibrating Noise to Sensitivity in Private Data Analysis. Journal of Privacy and Confidentiality, p. 1–18.
9. Konečný, J., McMahan, H. B., Yu, F. X., Richtárik, P., Suresh, A. T., & Bacon, D. (2016). Federated Learning: Strategies for Improving Communication Efficiency, p. 3.
10. McKinsey & Company. (2021). The Value of Personalization in Retail and E-commerce. McKinsey Report, p. 12.
11. Pew Research Center. (2019). Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Data. Pew Research Report, p. 8.
12. Smith, J. (2020). AI-Driven Personalization in E-commerce: A Case Study of Amazon. Journal of Digital Marketing, p. 45–50.
13. Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act. Computer Law & Security Review, 1–10.
14. Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer, p. 45.
15. World Economic Forum. (2020). Data Privacy in the Age of AI: A Corporate Responsibility. WEF Report, p. 22.

AUDİT 2025, 1 (47), səh. 112-121.
AUDIT 2025, 1 (47), pp. 112-121.
АУДИТ 2025, 1 (47), стр. 112-121.

İsayev Sadiq Sarvan oğlu,
doktorant,
Bakı Biznes Universiteti,
E-mail: sadiqisayev13@gmail.com

İNNOVASİYA VƏ MƏXFİLİK ARASINDA TARAZLIQ: SÜNİ İNTELLEKT ƏSASLI MƏLUMATDAN İSTİFADƏDƏ ETİK ASPEKTLƏR

X Ü L A S Ə

Tədqiqatın məqsədi - süni intellekt texnologiyaları ilə şəxsi məlumatlardan istifadənin kəsişməsində yaranan etik məsələlərin hərtərəfli şəkildə təhlil edilməsidir. Tədqiqatda əsas diqqət fərdiləşdirmə və məxfilik arasındakı balansın araşdırılmasına, məxfiliyin qorunması texnologiyalarının effektivliyinin qiymətləndirilməsinə və məlumatların qorunmasında biznes və dövlətlərin məsuliyyətinin təhlilinə yönəlmişdir.

Tədqiqatın metodologiyası - bu tədqiqat etik, texniki və normativ aspektləri araşdırmaq üçün keyfiyyət və kəmiyyət metodlarının birləşdiyi qarışıq metodologiyadan istifadə edir. Tədqiqat çərçivəsində son dövrlərə aid akademik ədəbiyyat, sənaye hesabatları və praktiki nümunələr təhlil olunaraq əsas tendensiyalar, çətinliklər və həll yolları müəyyən edilmişdir.

Tədqiqatın tətbiqi əhəmiyyəti - tədqiqatın nəticələri bizneslər, siyasətçilər və cəmiyyət üçün mühüm praktik əhəmiyyət kəsb edir. Bizneslər üçün bu tədqiqat, müştəri etimadını qazanmaq və rəqabət üstünlüyü əldə etmək üçün etik məlumat idarəetməsi və məxfiliyin qorunmasına yönəlmiş texnologiyaların tətbiqinin vacibliyini vurğulayır.

Tədqiqatın orijinallığı və elmi yeniliyi - bu tədqiqat Sİ etikası və məlumatların məxfiliyi mövzularına töhfə verir, bu sahələrin kəsişməsindəki problemləri və imkanları hərtərəfli təhlil edir. Əvvəlki tədqiqatlar ya Sİ-nin etik təsirlərini, ya da məxfilik texnologiyalarının texniki aspektlərini ayrı-ayrılıqda araşdırmışdırsa, bu məqalə bu iki perspektivi birləşdirərək mövzuya kompleks yanaşma təqdim edir.

Açar sözlər: süni intellekt, innovasiya, məlumatların məxfiliyi, etik məsələlər, fərdiləşdirmə.

AUDİT 2025, 1 (47), səh. 112-121.
AUDIT 2025, 1 (47), pp. 112-121.
АУДИТ 2025, 1 (47), стр. 112-121.

Исаев Садиг Сарван оглы,
докторант,
Бакинский Университет Бизнеса,
E-mail: sadigisayev13@gmail.com

БАЛАНС МЕЖДУ ИННОВАЦИЯМИ И КОНФИДЕНЦИАЛЬНОСТЬЮ: ЭТИЧЕСКИЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ДАННЫХ С ПРИМЕНЕНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Р Е З Ю М Е

Цель исследования - критически проанализировать этические вопросы, возникающие на пересечении технологий искусственного интеллекта (ИИ) и использования персональных данных. В частности, исследование направлено на изучение баланса между персонализацией и конфиденциальностью, оценку эффективности технологий сохранения конфиденциальности, а также анализ обязанностей бизнеса и государственных структур по обеспечению безопасности данных.

Методология исследования - в работе используется смешанный методологический подход, сочетающий качественный и количественный анализ этических, технических и правовых аспектов ИИ и конфиденциальности данных. Исследование основано на всестороннем обзоре современной академической литературы, отраслевых отчетов и тематических кейсов для выявления ключевых тенденций, проблем и решений.

Практическая значимость исследования - результаты имеют высокую практическую значимость для бизнеса, политиков и общества. Для компаний исследование подчеркивает важность внедрения этичных практик обработки данных и технологий обеспечения конфиденциальности с целью укрепления доверия клиентов и достижения конкурентных преимуществ.

Оригинальность и научная новизна исследования - настоящее исследование вносит вклад в изучение этики ИИ и конфиденциальности данных, предлагая комплексный анализ возникающих на их стыке проблем и возможностей. В отличие от предыдущих работ, рассматривающих этические аспекты ИИ или технические вопросы обеспечения конфиденциальности изолированно, данное исследование объединяет эти подходы для формирования целостного представления о предмете.

Ключевые слова: искусственный интеллект, инновации, конфиденциальность данных, этические вопросы, персонализация.

Məqalə redaksiyaya daxil olmuşdur: 19.12.2024
Təkrar işlənməyə göndərilmişdir: 29.01.2025
Çapa qəbul olunmuşdur: 17.02.2025

Дата поступления статьи в редакцию: 19.12.2024
Отправлено на повторную обработку: 29.01.2025
Принято к печати: 17.02.2025

The date of the admission of the article to the editorial office: 19.12.2024
Send for reprocessing: 29.01.2025
Accepted for publication: 17.02.2025