2025 First International Conference on Advances in Computer Science, Electrical, Electronics, and Communication Technologies (CE2CT)

AI and Data Privacy in Business

1st Aaryan Gupta
Dept of Artificial Intelligence and Machine Learning
Manipal University Jaipur
Jaipur, India
aaryangupta1200@gmail.com

2nd Mansi Amarnani
Dept of Artificial Intelligence and Machine Learning
Manipal University Jaipur
Jaipur, India
amarnanimansi04@gmail.com

3rd Surendra Soanki
Dept of Artificial Intelligence and Machine Learning
Manipal University Jaipur
Jaipur, India
surendra.solanki@jaipur.manipal.edu

4th Jaydeep Kishore
Dept of Artificial Intelligence and Machine Learning
Manipal University Jaipur
Jaipur, India
jaydeep.kishore@jaipur.manipal.edu

***Abstract*—This review paper discusses AI innovation and data privacy imperatives in modern business applications converging. Now, with AI taking over the role of process optimization and even customer personalization, organizations that rely on this data will be more sensitive to issues related to privacy starting from data security down through potential biases introduced in models which makes it crucial for them remaining compliant. Here we review privacy-focused principles such as the pillars of Privacy-by- Design, Data Governance and Transparency that are necessary to mitigate the risks posed by AI with respect to individual or societal information. Second, it analyzes the global regulatory environments driving AI implementation and underscores that data integrity in combination with accountability are ethical imperatives when deploying AI. Fulfilling these privacy challenges can also foster trust with consumers and lead to more responsible AI usage in the longer term. This paper presents a comprehensive examination of what it will take to build an accountable AI culture, to align the next wave of technical progress with privacy ethics and responsible innovation, and for organizations so that they understand how both can be compatible truthfully.**

Keywords*—*Artificial Intelligence Ethics, Data Privacy in AI, Privacy-by-Design, AI Governance, Regulatory Compliance in AI

I. Introduction

It is without a doubt, the rapid evolution of artificial intelligence has revolutionised business and opened doors to additional pathways for greater efficiency, innovation and overall competitive advantage. In other words, disparate enterprises are investing in AI technologies — machine learning algorithms and solutions like natural language processing systems to streamline operations across verticals by analysing massive data stores automatically while automating decisions for better customer experiences. But this advancement in technology comes with its fair share of hurdles, mainly around the issue of data privacy and ethics. With businesses capturing and using extensive datasets for developing their AI models, the data privacy gets imminent. In an age of information leaks and misuse, it's more important than ever to protect your customers' privacy. These statistically generated errors extend to the increasingly powerful regulatory frameworks–think GDPR in Europe and CCPA in California – that are popping up all over the world aimed at limiting data handling practices and protecting rights of individuals. However, the changes brought forth by AI are moving at a rapid pace and current rules can not keep up with these new challenges.

Through elucidation of the ethical concerns involved with AI/ML models, followed by exploration on regulation land scape and practical strategies for protecting data privacy; we attempt to navigate complexity that is associated between facets of business operations in respect to Artificial intelligence, Machine Learning models, and Data Privacy aspects. We thus seek here to distil the insights from existing literature and case studies, both successes and failures, regarding how best to balance AI's potential for innovation with our current data privacy mandate. This research is intended to add back further weight in this ongoing debate around AI suitability and maintaining consumer trust as the world digitalises more pervasively.

II. Understanding AI and Data Privacy

A. Defining Artificial Intelligence

Machine learning: Machine Learning refers to the use of Artificial Neural Networks or other statistical tools for finding patterns in large data sets. These processes include various functions like learning, reasoning and self-correction. From advancements in AI technologies to natural language processing, computer vision and predictive analytics that are revolutionizing sectors like finance, healthcare, retail etc have arrived [1].

B. Data Privacy

Information privacy or data privacy is the aspect of information technology that deals with the ability an organization or individual has to determine what data in a computer system can be shared with third parties. The business focus of data privacy is the manner in which organizations handle consumer information, and conform to both applicable law that governs this handling, and basic human rights. Data Principle: Transparency, Consent, Minimisation of Data and Accountability [2]. The way in which AI is incorporates and data privacy fits in to this framework raises important considerations for how organizations deploy AI whilst also protecting personal information of consumers. To make it work, AI have to access huge amount of sensitive data during collection and processing for which all must address the privacy issues throughout entire lifecycle of data [3]. Figure 1 highlights the Distribution of Data Privacy Regulations around the world.

C. The Regulatory Landscape

Data Privacy is in indeed a very dynamic field and the more important point to realize here is that because of ever-growing concerns around data misuse, breaches all has significant impact at high level be it fin tech companies, other related firms but also

2025 First International Conference on Advances in Computer Science, Electrical, Electronics, and Communication Technologies (CE2CT) | 979-8-3315-1857-8/25/$31.00 ©2025 IEEE | DOI: 10.1109/CE2CT64011.2025.10939576

because how regulations are shaping on regular basis due changing environment. Strict laws like the GDPR in Europe and the CCPA in California create requirements around how companies can collect, store, use personal data. It is essential for companies to comply with these laws, as they detail the security measures businesses need to take and require that individuals be aware of how data about them will be used so that you can control it [4]. Failing to follow these regulations can result in stiff penalties and the erosion of goodwill for firms. In addition, abiding by data privacy regulations nurtures trust with consumers which is a critical component of any successful digital age business operations.

D. Challenges at the Intersection of AI and Data Privacy

AI has many benefits when it comes to analysing data and making decisions, but also raises certain concerns about privacy. But the large datasets that AI models are trained on can result in unintended exposure of information, sparking ethical concerns. In addition, opacity and the complexity of some AI algorithms obstruct accountability and transparency in data management efforts [5]. Table 1 shows comparison of AI Techniques and Their Data Privacy Implications. Businesses must wade through complexity to deploy ethical AI responsible for data confidentiality. This involves creating privacy-aware AI systems, anonymizing data where possible and setting up explicit procedures for how the data is accessed and used [6].

TABLE I. COMPARISON OF AI TECHNIQUES AND THEIR DATA PRIVACY IMPLICATIONS

AI Technique	Description	Data Privacy Implications	Example Applications
Machine Learning	Algorithms that learn from data to make predictions	Potential for data leakage and bias	Fraud detection, customer segmentation
Natural Language Processing&	AI that understands and processes human language	Risks related to personal data usage	Chatbots, sentiment analysis
Computer Vision	AI that interprets and processes visual information	Concerns over surveillance and consent	Facial recognition, autonomous vehicles
Federated Learning	Decentralized learning that keeps data on local devices	Enhances privacy by minimizing data sharing	Mobile keyboard prediction
Differential Privacy	Techniques that provide insights while protecting privacy	Complex implementation; risk of data utility loss	Data analytics in healthcare

III. THE ROLE OF AI IN DATA PROCESSING AND MANAGEMENT

A. AI Technologies in Data Management

Artificial Intelligence plays a transformative role in data processing and management by automating and optimizing various tasks associated with data handling. Key AI technologies contributing to this evolution include:

- **Machine Learning:** ML algorithms look at historical data to find patterns that can be used for predictive analytics and in making strategic decisions. This enables improved resource allocation and operational efficiencies across business functions [7].
- **The natural language processing:** Typical organization where businesses can extract valuable insights from unpunctuated data, social media open fields, and email surveys. It helps in customer engagement and customized their services according to sentiment trends [8].
- **Robotic Process Automation:** RPA automates common data entry and processing tasks, eliminating manual errors to drive efficiency. Automating repetitive tasks through RPA wastes less time and resources for organizations, leaving topline personnel free to concentrate on their strategic capabilities with everything aligned neatly data-wise [9].
- **Data Mining:** It is an AI-powered data mining. AI employs some complex algorithms to reveal hidden patterns and correlations in large datasets which enables organizations to colour a picture of actionable insight that they can put into place. Which enable better decisions and strategic planning [10].

B. Enhancing Data Quality and Accuracy

The major impact of AI technologies on data quality and accuracy. AI can help identify inconsistencies, errors, and anomalies in datasets by automating data validation processes, making an organization work on reliable information. Better data quality means better decisions and helps us meet the standards that good data privacy regulations require. Table 2 compares the different regulatory frameworks addressing data privacy in AI [11]. In addition, removing duplicates and data anomalies will be done efficiently by using AI in data cleaning. It also helps organizations simplify data management and access high-quality data for use in applications like customer analytics, market research, or operational optimization.

C. AI-Driven Personalization and Its Implications for Privacy

Personalization is one of the key benefits of AI in data management and processing because of its ability to permit personalization. AI dives deep into customer data and offers customized experiences like targeted marketing campaigns and personalized product recommendations. As great as this level of individualization is for customer satisfaction and engagement, privacy implications are real. Since AI-driven personalization involves the organization and systematic storage of reams of personally identifiable data, companies must ensure adequate privacy protection [12]. Organizations need clear consent for users, transparent information on how data will be treated, and mechanisms to allow the user to control his/her choices of what happens with their own data. Balancing the right level of personalization with privacy is key to retaining consumer trust and compliance with regulation [13].

IV. DATA PRIVACY CONCERNS IN THE AGE OF AI

A. Overview of Data Privacy Regulations

Use of AI in business has increased the demand for data privacy regulations sharply. Rules like the General Data

Protection Regulation in Europe and the California Consumer Privacy Act in the US set up this model of privacy protection for our personal information. These laws require organizations to be clear about what data they are collecting and how, must seek permission from users before hand, and establish protection measures in order not for the databases to get breached [14]. Figure 2 shows the trends in adoption of data privacy over the years.

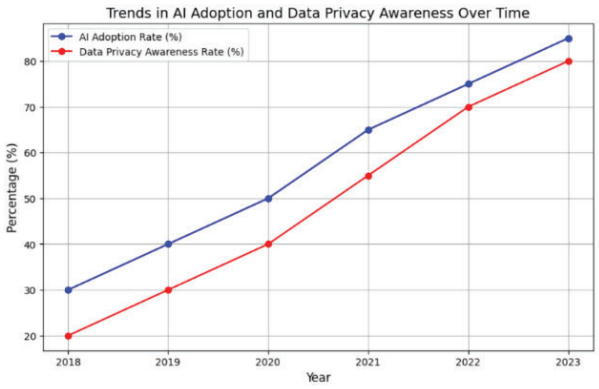

Fig. 1. Trends in AI Adoption and Data Privacy Awareness Over Time

Under these regulations, businesses are required to:

- **Inform Users:** Institutions need to notify users what types of data will be collected from them, why they are collecting the information, and how it is able to use their data and share in different ways [15].
- **Obtain Consent:** Prior consent is always needed for gathering and processing personal data, particularly when it comes to using information in automated decision-making.
- **Provide Access and Control:** As an individual, you have the right to access your data, make corrections on personal information, or ask for them to be forgotten from a company's records.
- **Implement Data Protection Measures:** An organization has an obligation to have appropriate technical and organizational measures that would guarantee the security of personal data processing and limit the occurrence of breaches [16].

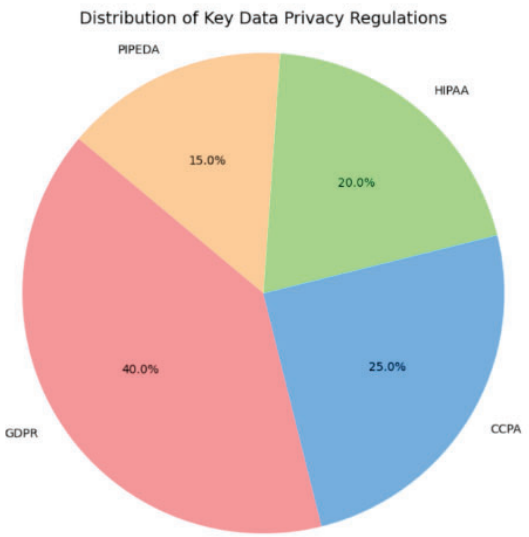

Fig. 1. Distribution of Data Privacy Regulations

B. *Challenges of AI and Data Privacy*

Despite the regulatory landscape, several challenges persist in the realm of data privacy as AI technologies continue to evolve:

- **Data Minimization vs. Data Utility:** Legislation emphasizes data minimization—via requirements to collect only what is necessary for some specific purpose—while AI usually requires big datasets in order to produce successful training and analysis. This creates a challenge for would-be compliers, who are trying to live up to both data minimization and completeness standards [17].
- **Informed Consent:** The issue of properly obtaining informed consent from users can be especially difficult when the AI uses sophisticated algorithmic processes that few consumers will understand. In order to make an informed decision about your data, we need clear and comprehensible information from organizations showing how they are managing people's data.
- **International Use of AI:** Because many applications are not bound by national borders, there is a need to move around personal data globally. This raises concerns about multi-jurisdiction data protection compliance and also the limited nature of certain legal protections [18].
- **Emerging Technologies and Privacy Risks:** Facial recognition and behavioural analytics are prime examples of new AI technologies that carry unique privacy risks due to their rapid development. Such technologies could end up as invasive data collection devices, and the deployment of them bring into focus ethical concerns about surveillance versus individual rights [19].

C. Ethical Considerations in AI Deployment

The ethical implications of AI-driven data practices are becoming increasingly important. Organizations must consider the following:

- **User Sovereignty:** One of the primary ways that we serve as data stewards is to help people make informed decisions about their own data. This is going to mean adding options for people when they attempt to opt-out of their data being collected as well making the process easier in general wherever changes can be made [20].
- **Accountability:** Enterprises will implement mechanisms to ensure the ethical design and use of AI. Regular audits on AI algorithms to ensure solutions remain compliant with data privacy laws and ethical principles [21].
- **Explanation of AI Decision-Making:** Another theme that we see in promoting trust with respect to any AI system is transparency. Of course, the ultimate aim for organizations is to produce a process of decision-making in AI that is transparent and comprehensible by the user—making it clear what their data evokes [22].
- **Fairness:** We need to prevent AI systems from enacting or reinforcing social biases in our society. From bias detection to mitigation, various practices are incorporated at every phase of the AI development process. decision-making.

D. The Importance of Privacy-By-Design

To reduce privacy risks linked to AI, one must take a privacy-by-design approach. The principle argues that privacy should be incorporated at the early stages of AI system development and deployment [23]. This approach is guided by five critical principles of privacy by design, including:

- **Data Protection Impact Assessments:** conducted by organizations can identify and mitigate privacy risks related to their AI projects when required under data protection regulations.
- **User Centric Design:** Create artificial intelligence systems that focus on user experience and gain trust in the process. Duties include ensuring that users can readily access clear privacy notices and control their data preferences [23].
- **Stakeholder Participation:** Involving stakeholders in the development of AI can be beneficial for creating more meaningful solutions to help ensure greater and lasting respect towards user rights.

TABLE II. REGULATORY FRAMEWORKS ADDRESSING DATA PRIVACY IN AI

Regulation	Region	Key Provisions	Relevance to AI
General Data Protection Regulation (GDPR	European Union	Consent, data portability, right to be forgotten	Applies strict rules on data processing and usage by AI systems
California Consumer Privacy Act (CCPA	United States (California)	Consumer rights regarding personal data collection	Mandates transparency in data practices, affecting AI algorithms using personal data
Health Insurance Portability and Accountability Act (HIPAA)	United States	Protects sensitive patient health information	Requires data protection measures in AI applications in healthcare
Personal Information Protection and Electronic Documents Act (PIPEDA)	Canada	Requires consent for data collection and use	Impacts AI systems that utilize consumer data in Canada

V. BEST PRACTICES FOR ENSURING DATA PRIVACY IN AI-DRIVEN BUSINESS MODELS

- **Privacy-by-Design and Data Minimization:** Integrate data protection measures from the design phase of any system undergoing AI. Utilize privacy-by-design When used identify and mitigate risks at the beginning of development, integrated throughout AI design. Please apply the principle of data minimization (never collect more than you absolutely need) and use appropriate anonymization techniques to reduce both your exposure-risk posture as well as some level of regulatory compliance overhead [25].
- **Clear Policies and Governance:** Focus on creating transparent data policies that clearly articulate collection, usage, and how the information is shared with third parties. Create clear governance guidelines, roles, and control mechanisms to secure PII in accordance with data privacy legislation.
- **Employee Training and AI-Driven Security:** Regularly provide privacy training to your employees so they will respect data. Using AI algorithms to better protect data by detecting and responding quickly to security threats, we are now able to more effectively secure personal information [29].

TABLE III. AI STRATEGIES FOR ENHANCING DATA PRIVACY

Strategy	Description	Benefits	Challenges
Privacy-by-Design	Integrating data privacy into the design of AI systems	Reduces risks and enhances compliance	Requires upfront investment and planning
Data Minimization	Collecting only necessary data for AI models	Limits exposure of personal information	May reduce the effectiveness of AI models
Explainable AI	Ensuring AI decisions are understandable to users	Builds trust and accountability	Complexity in implementation
Regular Audits and Assessments	Continuous monitoring of AI systems for privacy issues	Identifies and mitigates risks proactively	Resource-intensive and may require specialized skills

User-Centric Privacy Controls	Providing users control over their data	Empowers users and enhances trust	Requires user education and engagement

VI. Challenges and Considerations in Balancing AI Innovation and Data Privacy

- **Regulatory Compliance and User Consent:** Keeping up with rapidly changing data regulations like GDPR and CCPA, and the need to remain compliant means adapting on a regular basis. Consent mechanisms must be transparent, meaning that users should understand how AI operates over their data in order to trust it and keep control of what they are sharing [26].
- **Data Quality, Privacy, and Bias Prevention:** AIt also usually conflicts with data minimization principles, as the more diverse and of higher quality the dataset is going to perform better. Achieving that balance means collecting less data and addressing the bias of datasets or algorithms.
- **Data Security and Cross-Departmental Collaboration:** AI makes the technology security concerns more critical with even better encryption, intrusion detection, and user training. Reaching privacy-compliant AI further requires a combination of IT and legal or compliance resources working together toward common interests in the development of responsible practices [28].

Table 4 discusses the Key Challenges in Balancing AI and Data Privacy, highlights the impact of these challenges on businesses, and suggests possible solutions.

TABLE IV. Key Challenges in Balancing AI and Data Privacy

Challenge	Description	Impact on Business	Potential Solutions
Data Breaches	Unauthorized access to sensitive data	Legal repercussions and loss of customer trust	Implementing robust cybersecurity measures
Regulatory Compliance	Navigating complex and evolving data privacy regulations	Increased operational costs	Establishing dedicated compliance teams
Consumer Trust	Gaining and maintaining customer confidence in data handling	Affects brand reputation and loyalty	Transparency in data practices and policies
Ethical AI Development	Ensuring AI systems are developed and used ethically	Risk of backlash from stakeholders	Adopting ethical frameworks and guidelines

VII. Future Directions for AI and Data Privacy in Business

Privacy-by-design frameworks and more decentralized/secure machine learning techniques like federated learning will dominate the future of AI for business. This privacy-first methodology includes making the necessary protections, like data minimization and anonymization, an inherent part of AI systems from the start, thereby enabling companies to achieve compliance as they go along while also fostering trust. Federated learning is gaining ground because it allows for some amount of processing to be done locally on the users' device, which minimizes data transfers and associated privacy risks. Also on the enforcement front, our industry will see tightening regulations that require transparency of decisions made by algorithms and therefore accountability, so a literally explainable AI (XAI) becomes ever more important too.

Meanwhile, AI-powered privacy solutions would simplify compliance by doing critical work, like data classification and consent policy enforcement, automatically, while collaborative data ecosystems could allow safe sharing of the datasets in a de-personalized manner for training AI without transgressing on personal rights. Additionally, organizations will highlight consumer awareness as a means of driving transparency and work with regulators beforehand in defining the new data privacy framework. With organizations looking to develop governed, trusted AI ecosystems in line with growing societal expectations and regulatory requirements, ethical practices will be controlled by fairness, accountability, or human rights.

VIII. Conclusion

The real-world business environment of AI is discussed in this review and underlines the role that data privacy plays within it, demonstrating how pure-data class methods impact deployment contexts by underscoring a need for holistic approaches to private AI. AI technology development must be supported by proactive privacy strategies—like the adoption of a technical concept known as “privacy-by-design” and ensuring ethical data management, security compliance, and transparency to protect against bias. The imperatives of regulatory frameworks worldwide are emboldening the deployment of ethical AI and pushing tech innovators to ensure adherence with tight privacy compliance regulations. An accountable culture, backed by good governance and adherence to ethical principles, not only deals with privacy but also engenders consumer trust, which contributes directly in robust AI development. Those that do can take advantage of AI with the confidence it will go hand-in-hand with suitable data privacy controls and ethical standards.

References

[1] Martin, K. D., & Zimmermann, J. (2024). Artificial Intelligence and its Implications for Data Privacy. Current Opinion in Psychology, 101829.

[2] Attard-Frost, B., De los Ríos, A., & Walters, D. R. (2023). The ethics of AI business practices: a review of 47 AI ethics guidelines. AI and Ethics, 3(2), 389-406.

[3] Horzyk, A. (2023, November). Data Protection and Privacy: Risks and Solutions in the Contentious Era of AI-Driven Ad Tech. In International Conference on Neural Information Processing (pp. 352-363). Singapore: Springer Nature Singapore.

[4] Rana, N. P., Chatterjee, S., Dwivedi, Y. K., & Akter, S. (2022). Understanding dark side of artificial intelligence (AI) integrated business analytics: assessing firm’s operational inefficiency and competitiveness. European Journal of Information Systems, 31(3), 364-387.

[5] Saura, J. R., Ribeiro-Soriano, D., & Palacios-Marqués, D. (2022). Assessing behavioral data science privacy issues in government artificial intelligence deployment. Government Information Quarterly, 39(4), 101679.

[6] Aldboush, H. H., & Ferdous, M. (2023). Building trust in fintech: an analysis of ethical and privacy considerations in the intersection of big

data, AI, and customer trust. International Journal of Financial Studies, 11(3), 90.

[7] Azam, N., Michala, L., Ansari, S., & Truong, N. B. (2022). Data privacy threat modelling for autonomous systems: A survey from the gdpr's perspective. IEEE Transactions on Big Data, 9(2), 388-414.

[8] Eboigbe, E. O., Farayola, O. A., Olatoye, F. O., Nnabugwu, O. C., & Daraojimba, C. (2023). Business intelligence transformation through AI and data analytics. Engineering Science \& Technology Journal, 4(5), 285-307.

[9] Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., ... & Platts, J. (2022). Cybersecurity, data privacy and blockchain: A review. SN computer science, 3(2), 127. Bell, A., Nov, O., & Stoyanovich, J. (2023). Think about the stakeholders first! Toward an algorithmic transparency playbook for regulatory compliance. Data & Policy, 5, e12.

[10] Lucaj, L., Van Der Smagt, P., & Benbouzid, D. (2023, June). Ai regulation is (not) all you need. In Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency (pp. 1267-1279).

[11] Viljanen, M., & Parviainen, H. (2022). AI applications and regulation: Mapping the regulatory strata. Frontiers in Computer Science, 3, 779957.

[12] Guha, N., Lawrence, C., Gailmard, L. A., Rodolfa, K., Surani, F., Bommasani, R., ... & Ho, D. E. (2023). Ai regulation has its own alignment problem: The technical and institutional feasibility of disclosure, registration, licensing, and auditing. George Washington Law Review, Forthcoming.

[13] Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., de Prado, M. L., Herrera-Viedma, E., & Herrera, F. (2023). Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. Information Fusion, 99, 101896.

[14] Schuett, J., Anderljung, M., Carlier, A., Koessler, L., & Garfinkel, B. (2024). From principles to rules: A regulatory approach for frontier AI. arXiv preprint arXiv:2407.07300.

[15] Mökander, J., Axente, M., Casolari, F., & Floridi, L. (2022). Conformity assessments and post-market monitoring: a guide to the role of auditing in the proposed European AI regulation. Minds and Machines, 32(2), 241-268.

[16] Papagiannidis, E., Enholm, I. M., Dremel, C., Mikalef, P., & Krogstie, J. (2023). Toward AI governance: Identifying best practices and potential barriers and outcomes. Information Systems Frontiers, 25(1), 123-141.

[17] Mäntymäki, M., Minkkinen, M., Birkstedt, T., & Viljanen, M. (2022). Defining organizational AI governance. AI and Ethics, 2(4), 603-609.

[18] Wirtz, B. W., Weyerer, J. C., & Kehl, I. (2022). Governance of artificial intelligence: A risk and guideline-based integrative framework. Government Information Quarterly, 39(4), 101685.

[19] Prifti, K., Morley, J., Novelli, C., & Floridi, L. (2024). Regulation by design: features, practices, limitations, and governance implications. Minds and Machines, 34(2), 1-23.

[20] Zhang, P., & Kamel Boulos, M. N. (2022). Privacy-by-design environments for large-scale health research and federated learning from data. International Journal of Environmental Research and Public Health, 19(19), 11876.

[21] Qasaimeh, G. M., & Jaradeh, H. E. (2022). The impact of artificial intelligence on the effective applying of cyber governance in jordanian commercial banks. International Journal of Technology, Innovation and Management (IJTIM), 2(1).

[22] Van Noordt, C., & Misuraca, G. (2022). Artificial intelligence for the public sector: results of landscaping the use of AI in government across the European Union. Government information quarterly, 39(3), 101714.

[23] Attard-Frost, B., De los Ríos, A., & Walters, D. R. (2023). The ethics of AI business practices: a review of 47 AI ethics guidelines. AI and Ethics, 3(2), 389-406.

[24] Hunkenschroer, A. L., & Luetge, C. (2022). Ethics of AI-enabled recruiting and selection: A review and research agenda. Journal of Business Ethics, 178(4), 977-1007.

[25] Haenlein, M., Huang, M. H.,& Kaplan, A. (2022). Guest editorial: Business ethics in the era of artificial intelligence. Journal of Business Ethics, 178(4), 867-869.

[26] D'Cruz, P., Du, S., Noronha, E., Parboteeah, K. P., Trittin-Ulbrich, H., & Whelan, G. (2022). Technology, megatrends and work: Thoughts on the future of business ethics. Journal of business ethics, 180(3), 879-902.

[27] Munn, L. (2023). The uselessness of AI ethics. AI and Ethics, 3(3), 869-877.

[28] Nitzberg, M., & Zysman, J. (2022). Algorithms, data, and platforms: the diverse challenges of governing AI. Journal of European Public Policy, 29(11), 1753-1778.

[29] Margetts, H. (2022). Rethinking AI for good governance. Daedalus, 151(2), 360-371.