International Corporate Governance in the Digital Age: Legal Challenges of Privacy Protection and Data Governance

Bingbing Bi

University of Leeds, Leeds, LS2 9JT, United Kingdom

20224890103@stu.usc.edu.cn

Abstract. In the current age characterised by digital transformation, global organisations encounter unparalleled difficulties in effectively managing and regulating their large quantities of data. This essay examines the theoretical underpinnings of data governance and how it relates to corporate governance, safeguarding privacy in the digital era, the connection between data governance and corporate strategy, the difficulties encountered by multinational corporations in data governance, and suggestions for enhancing data governance practices. This essay seeks to offer a comprehensive framework for multinational organisations to efficiently manage the difficulties of data governance in today's global context. It does so by analysing concepts, principles, and practical solutions. Through explores the fundamental principles of data governance, emphasising its significance within corporate governance frameworks. This text examines the definitions and scopes of data governance, with a particular focus on its strategic significance in efficiently managing corporate data assets, emphasising data as a valuable advantage in the global market and emphasising the connections between data governance and business strategy. Multinational organisations have a range of obstacles when it comes to developing efficient data governance policies. This part provides a thorough overview of the issues encountered by international firms, including negotiating intricate regulatory regimes, addressing technology and operational obstacles, and considering ethical and societal factors.

Keywords: Data Governance, Corporate Governance, Multinational Obstacles.

1 INTRODUCTION

Data has become a crucial asset for multinational organizations in the fast-changing digital environment, playing a key role in promoting innovation, competitiveness, and strategic decision-making. With the growing dependence of companies on data for their operations and expansion, the importance of implementing efficient data governance processes has become crucial. Data governance is a vital component in managing data assets. It involves the implementation of policies, processes, and controls to ensure data

A. Bhunia et al. (eds.), *Proceedings of the 2024 2nd International Conference on Finance, Trade and Business Management (FTBM 2024)*, Advances in Economics, Business and Management Research 304,
https://doi.org/10.2991/978-94-6463-546-1_6

corporate governance has emerged as a central concern for organisations seeking to negotiate the intricacies of the digital era while maintaining ethical norms and regulatory obligations.

In recent years, the Opinions of the State Council on Further Optimising the Foreign Investment Environment and Increasing Efforts to Attract Foreign Investment, issued by the State Council, proposes the exploration of a streamlined security management mechanism for the cross-border flow of data. The system fulfils the mandates of the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law, establishing swift procedures for foreign-invested enterprises that comply with specified criteria. These initiatives aim to facilitate efficient assessments of data and personal information destined for transfer abroad while promoting the secure, orderly, and free exchange of data. Consequently, this research endeavors to delve into the interplay between data governance and corporate strategy, highlighting the importance of data governance and its role in securing a competitive edge in the international marketplace.

This research seeks to elucidate strategies for multinational corporations to navigate the complexities of implementing effective data governance practices amidst challenging regulatory, technological, and ethical landscapes. By examining the core principles of data and corporate governance, the research emphasizes the critical role of data governance in shaping business strategy and achieving a competitive advantage. It aims to dissect and address the multifaceted challenges of regulatory compliance, technological obstacles, and ethical dilemmas, proposing actionable recommendations to enhance data governance frameworks globally. This investigation underscores the importance of robust data governance in maintaining corporate integrity and fostering sustainable growth in the international market.

This research is structured to offer a comprehensive exploration of data governance within the realm of multinational corporations, starting with an analysis of the theoretical underpinnings of data and corporate governance. It then examines the multifarious challenges these corporations encounter, including navigating complex regulatory landscapes, technological and operational impediments, and ethical and societal concerns. It utilises a qualitative methodology, incorporating an extensive analysis of current literature, theoretical frameworks, and case studies to examine the complex connection between data, corporate governance, and strategic decision-making. Through a comparative analysis of privacy laws across jurisdictions, an investigation of technological and operational hurdles, and a contemplation of ethical and societal ramifications, this study aims to forge recommendations for enhancing data governance practices. These recommendations aspire to guide multinational corporations towards achieving global compliance, ethical data management, and the utilization of technology for effective data governance, ultimately fostering sustainable corporate growth and success.

2 Theoretical Foundations of Data Governance and Corporate Governance

2.1 Concepts and Principles of Data Governance

Data plays a crucial role as a factor of production in the digital economy age. The diversity of production subjects, the complexity of the subjects asserting rights, and the ability to replicate and rapidly iterate data elements all differ from traditional factors of production [1]. As a result, these factors are exposed to numerous new risks during their use. The traditional framework for governing factors of production is no longer sufficient to address the emerging challenges in development. Therefore, an urgent need exists for a new system of data governance.

Data governance is essential for managing data assets in a way that is suitable and necessary [2]. This is particularly important in a climate where information is not only a valuable business resource but also poses substantial risks. Data governance involves a broad spectrum of tasks, such as creating data regulations, setting data standards, and implementing steps to guarantee data's availability, usability, integrity and security.

Central to the legal concept of data governance is the principle of accountability, which obligates organizations to not only comply with relevant laws but also demonstrate their compliance through documentation, data impact assessments, and other verifiable means. Moreover, legal data governance encompasses data minimization and purpose limitation principles, advocating for the collection of only necessary data and its use exclusively for stated, lawful purposes. Effective legal data governance also involves establishing clear roles and responsibilities within the organization for data management, including the appointment of data protection officers (DPOs) where required.

A comprehensive framework for data protection necessitates a collaborative approach that includes IT, legal, compliance, business operations, and executive leadership players. Furthermore, the primary objective of data management is to guarantee that data aligns with the strategic objectives of the organization.

Effective alignment necessitates transparent communication between data experts and corporate executives in order to comprehend and endorse the organization's objectives, strategies, and operational requirements. Regarding risk management, data management includes the tasks of recognizing and reducing risks related to data privacy, security, and compliance. This includes the creation of tactics to tackle any data breaches, guaranteeing adherence to regulatory mandates, and overseeing the risks to reputation linked to data management methods.

2.2 Privacy Protection in the Digital Age

The complexity of privacy protection has escalated as a result of the widespread use of digital technologies that gather and analyze substantial quantities of personal data. The legal framework has developed in response to this, with the General Data Protection Regulation (GDPR) and other privacy rules like the California Consumer Privacy Act (CCPA) embodying a worldwide trend towards enhanced safeguarding of personal data

[3]. Similarly, China has introduced data governance principles emphasizing data security, user rights protection, and the maximization of data value, moving towards a "data-enabled" governance model focused on a digital ecosystem.

The importance of promoting the proper allocation and circulation of data property rights is clearly emphasized. The right to possess data resources is defined, while the concept of ownership is weakened. Instead, the focus is on maximizing the rights to use and profit from the data [4]. This approach aims to encourage data holders to actively engage in data collection, processing, and circulation. It also addresses the issues of unclear ownership definition and the absence of rules for data transactions and circulation in data governance.

These laws offer principles to address challenges in data governance, including ambiguous ownership definitions, absence of regulations for data transactions and circulation, and the intricate and varied nature of data types. These rules provide fresh benchmarks for privacy and data security, mandating corporations to have thorough privacy management protocols. Simultaneously, there will be the obstacle of digital consent, and a crucial aspect of digital privacy is acquiring substantial consent from individuals.

However, the complex and obscure nature of data processing activities might pose a challenge for individuals to comprehend the consequences of their consent, potentially undermining the principle of informed consent. Furthermore, theoretical frameworks about privacy highlight the importance of striking a balance between an individual's entitlement to privacy and the broader concerns of public interest, such as national security and public health. Privacy protection is a constantly evolving field that requires ongoing negotiation in response to developing technologies and social change.

2.3 The Nexus between Data Governance and Corporate Strategy

Data governance serves as the fundamental basis for a corporation to construct its strategy for managing information. It includes the policies, standards, and procedures that guarantee the accuracy, accessibility, and security of data. Organisations require robust data governance due to various crucial factors, and numerous industries are bound by strict data protection and privacy rules such as Europe's General Data Protection Regulation (GDPR) and California's California Consumer Privacy Act (CCPA)to fulfil compliance and regulatory obligations.

Data governance is a practice that ensures companies adhere to these requirements in order to prevent significant financial penalties and harm to their brand. Data governance is an essential element of an organization's strategy for managing information. Data governance guarantees that organisations adhere to these requirements, thereby preventing substantial penalties and safeguarding their reputation.

Furthermore, the presence of high-caliber and dependable data is essential for precise examinations and documentation [5]. A data governance system ensures the consistency and correctness of data from its creation to its disposal, guaranteeing that choices are made using dependable information. Effective data governance provides a competitive advantage by reducing the risks of data breaches, data loss, and data mistakes. Organisations may establish trust with their customers by showcasing a strong dedication to safeguarding data privacy and security. This confidence leads to client

loyalty and has the potential to attract additional customers that prioritise data privacy. Enhancements can be made to data analytics, and a meticulously controlled data environment guarantees the uniformity, dependability, and ease of access to data. This facilitates enhanced data analytics and corporate intelligence, offering valuable insights that may be utilised to recognise market trends, customer preferences, and operational efficiencies. Furthermore, governance enhances operational savings by streamlining data management operations and minimising redundancies and errors. Enhancing efficiency leads to cost reduction, enhances service delivery, and establishes the company's competitive advantage.

Data governance plays a crucial role in enabling effective decision making by implementing policies that guarantee authorised people may access data and that different data sources can be merged. This complete perspective facilitates extensive analysis and well-informed decision-making. By implementing data governance practices that consistently monitor and enhance data quality, companies may make informed decisions using precise and current information, thus minimising the potential for expensive mistakes. Effective predictive analytics and AI projects require high-quality and well-managed data. These technologies have the potential to greatly enhance decision-making abilities, ranging from forecasting market fluctuations to automating routine judgements. Driving sustainable business growth by implementing effective data governance. Data governance is essential for ensuring sustainable corporate growth. A suitable data governance framework is created to fit the expansion of a business and allow businesses to expand their data infrastructure as the business grows. Data governance facilitates innovation by guaranteeing the accessibility of data that is of exceptional quality. Organisations have the ability to utilise their data assets in order to create novel goods, services, or business models. Data governance is the practice of managing data assets in a manner that is consistent with long-term strategic objectives.

This alignment ensures that companies maintain their focus on sustainable growth by utilising data to adjust to evolving market conditions and capitalise on opportunities [6]. Data governance encompasses more than a mere collection of guidelines aimed at ensuring compliance and data quality. It is a strategic resource that can facilitate sustainable growth, provide a competitive edge, and enhance decision-making processes. As organisations grapple with the intricacies of the digital era, incorporating data governance into their business plan is not just advantageous, but essential for achieving success.

3 CHALLENGES IN DATA GOVERNANCE FOR MULTINATIONAL CORPORATIONS

3.1 Navigating Complex Regulatory Environments

The regulation of global operations is characterised by a wide range of rules and regulations, with multinational corporations conducting business in several jurisdictions, each with its distinct set of data protection laws and regulations. In 2020, the European

Data Strategy was introduced with the aim of enhancing the EU data sharing mechanism and creating a global single data market. In 2022, the Data Governance Act was passed, which reiterated the importance of establishing a single data market and a mechanism for reusing public sector data, while also strengthening the promotion of data altruistic behaviour. Furthering these endeavors, the proposed Data Law by the EU seeks to deepen the governance infrastructure, focusing on fostering data sharing and maximizing value creation at the enterprise level.

The EU's proposed Data Law expands upon the existing governance system by placing a greater emphasis on data exchange and unlocking its potential within enterprises. The year 2022 The European Union's Data Protection Board has granted approval to Europrivacy, the first certification framework for General Data Protection Regulation (GDPR) compliance. Europrivacy is designated as the official European Data Protection Chapter responsible for evaluating and officially certifying adherence to data compliance standards. The framework was initially introduced in the EU and is now being extended to the worldwide market. It is regularly updated to adapt to legislative modifications. This innovative breakthrough has made a good contribution to the integration of data management and the development of a market for data elements. Furthermore, alongside Europe's trailblazing exploration, the consensus to enhance data empowerment has emerged in other countries.

Some countries are adapting their data governance methods based on their particular national circumstances, while also taking inspiration from the European experience. For instance, India's Personal Data Protection Bill of 2018, inspired by the GDPR, has undergone extensive revisions. The 2022 amended version primarily addresses the development demands of the local data market. It eases the restrictions on cross-border data transfers and includes a list of exemptions to alleviate the burdensome compliance obligations encountered by firms in the data industry. In parallel with Europe, the United States has been at the forefront of implementing data governance initiatives, emphasizing the strategic importance of data as a pivotal governance objective. With a longstanding commitment to data security, highlighted by the enactment of the Computer Fraud and Abuse Act (CFAA) in 1986 and its subsequent amendments, the U.S. has increasingly focused on enhancing the value of public data. Initiatives such as Big Data Research and Development Initiative (BDRDI) launched in 2012 [7], and the Federal Government Big Data Initiative (FGDI) in 2016, underscore the efforts to augment the federal government's capabilities in data collection and analysis. The publication of the "Federal Government Big Data Research and Development Strategic Plan" in 2016, followed by the "Federal Data Strategy" along with the "2020 Action Guide" in 2019, further signifies the emphasis on recognizing data as a strategic asset. These documents emphasise the importance of data as a strategic asset and highlight the need for coordinated management of key data by the federal government. The Federal Data Strategy also emphasises the significance of "ethical governance" as a crucial element of the government's strategy. The federal government plans to release a preliminary Data Ethics Framework in 2020. This framework will provide guidance to government personnel on how to adhere to ethical standards when collecting and using data.

3.2 Technical and Operational Challenges

Multinational organisations encounter two-fold obstacles in upholding data security and attaining efficient data management [8]. These challenges stem from the need to safeguard data against the backdrop of ever-evolving cyber threats and to ensure the seamless management and integration of data across global operations.

In an age where cyber threats are becoming more sophisticated, global corporations must implement innovative defence methods that beyond conventional security procedures. This involves utilising machine learning and artificial intelligence technologies to forecast and detect possible security risks, while also deploying comprehensive encryption and zero-trust architectures to enhance data security [9]. In addition, providing employees with education on identifying phishing emails and social engineering assaults is crucial in order to prevent data breaches. A significant number of global corporations continue to rely on outdated legacy systems that exhibit poor compatibility with contemporary technology and present challenges when it comes to updating.

This results in the creation of data silos, which hinders the efficient integration of data. Without a cohesive perspective on data, the accuracy of reporting and analysis is compromised, hence impacting the efficacy of decision-making. To solve this challenge, it is necessary to establish a uniform data management platform and standards throughout the company. This will enable efficient integration and analysis of data using data lake and data warehouse technologies.

3.3 Ethical and Social Challenges

MNCs face a unique set of ethical and social challenges as they manage and utilize vast quantities of personal data across the globe [10]. Beyond navigating complex regulatory landscapes, these entities must grapple with the ethical implications of using data mining, analytics, and AI technologies. The ethical concerns are not trivial; they revolve around safeguarding human privacy, ensuring autonomy, and preventing the misuse of personal data that could lead to discrimination or injustice. It is imperative to contemplate the ethical ramifications of employing data mining, analytics, and artificial intelligence and machine learning technologies for the purpose of processing personal data [11]. It is imperative for multinational corporations to guarantee that the implementation of these technologies does not violate individual privacy, result in injustice or discrimination, and handle personal data in a clear and open manner.

Furthermore, it is imperative for corporations to implement ethical evaluation systems in order to scrutinise the ethical ramifications of emerging technologies and data utilisation methods, thereby guaranteeing compliance with ethical norms and societal anticipations. In the era of social media, improper management of data can quickly cause public alarm and unfavourable public perception, leading to harm to a brand's reputation. Hence, it is crucial to retain a reputation for conscientious and open data administration in order to cultivate client confidence and foster brand allegiance [12]. It is important for multinational corporations (MNCs) to be transparent regarding their data management policies and procedures. They should take the initiative to clearly communicate the goal and methods of their data usage, as well as the protective

measures they have implemented. This will help establish a responsible reputation among the general public.

In order to overcome the difficulties posed by technology and operations, multinational companies must not only develop new technological solutions and enhance their ability to protect data from cyber threats, but also assume a leading position in promoting ethical behaviour and social responsibility. This is crucial to establish trust and gain the respect of consumers worldwide.

4 RECOMMENDATIONS FOR OPTIMIZING DATA GOVERNANCE IN MULTINATIONAL CORPORATIONS

4.1 Developing Robust Data Governance Frameworks

Data governance is essential for the success of MNCs that operate in a business environment substantially dependent on data. MNCs must include privacy by design principles into every area of product development, business processes, and technology system design. By implementing this proactive approach, the company ensures that data protection measures are ingrained in its culture and operations right from the start. This not only ensures compliance with international data protection laws, but also enhances customer trust and satisfaction. By adhering to the Least Data Principle, businesses can reduce the risk of data breaches and improve the efficiency of data processing. This principle entails collecting only the necessary data to achieve business objectives.

It is essential to have a data governance policy that is cohesive and can comply with the strictest global compliance standards, while still being flexible enough to meet local regulations. This strategy should include data collecting, storage, processing, and disposal processes that adhere to many international data protection legislations such as GDPR, CCPA, and others. Adopting a unified strategy guarantees uniformity in the way data is managed, leading to streamlined operations and improved efficiency.

Integrating privacy by design into the development of products and business processes guarantees that data protection is an essential element [13]. By embracing the Least Data Principle, MNCs can guarantee that only critical data is gathered, hence reducing the likelihood of data breaches and simplifying data management procedures [14]. This method not only improves data security but also fosters customer trust by showcasing a dedication to privacy.

In order to efficiently handle the intricacies of diverse foreign data protection regulations, MNCs need customize their data governance rules to align with the particular requirements of each geographical area in which they conduct business [15]. This involves comprehending cultural subtleties and legal obligations, guaranteeing that data management regulations are uniformly applicable worldwide and specifically tailored to local contexts. Subsequently, these regulations are tailored to conform to the legal and cultural prerequisites of the particular area. This approach not only streamlines the process of ensuring compliance, but also ensures consistency and high quality across all global business units [16].

4.2 Enhancing Compliance and Ethical Practices

Companies should provide ongoing education and foster awareness. Consistent training on data privacy, security, and ethical considerations is essential for equipping personnel with the requisite knowledge and expertise. These teaching workshops can cultivate a thorough organizational culture of data security and ensure that every employee understands their responsibilities and obligations in preserving data and maintaining customer privacy. Employee engagement and knowledge can be improved through various tactics such as simulated attacks, workshops, and online courses.

An internal department dedicated to ethics and compliance can have a crucial impact on upholding stringent ethical standards and ensuring regulatory compliance. This function should possess the power and means to exert influence over corporate decisions, guaranteeing that operations not only conform to legal obligations but also uphold the utmost ethical principles [17].

Enhancing confidence among stakeholders can be achieved by implementing transparency in data processing processes and establishing clear accountability systems. MNCs ought to publicly reveal their data governance protocols and establish mechanisms for stakeholders to express concerns or report instances of unethical conduct. This transparency promotes a culture of confidence and responsibility, which is crucial for maintaining sustainable corporate operations.

Furthermore, creating a specialized role or department within the organization that specifically concentrates on ethics and compliance serves to improve the ethical standards and ensure compliance with rules within the corporation. These experts should possess the combined responsibility of supervising the company's adherence to regulations and actively engaging in the process of making decisions. Their duty is to guarantee that the company's business actions conform not only to legal mandates, but also to ethical standards and public expectations.

4.3 Leveraging Technology for Effective Data Governance

The utilization of cutting-edge technology like as artificial intelligence, blockchain, and cloud computing can significantly improve the efficiency and effectiveness of data governance [18]. Blockchain technology provides an immutable method for storing data, enhancing both the transparency and security of the data. Artificial intelligence and machine learning algorithms can independently detect and alert about any data security breaches or non-compliance, leading to a substantial improvement in the effectiveness and timeliness of data monitoring.

By employing advanced data analytics tools, multinational organizations may extract valuable insights from large volumes of data to guide strategic decision-making [18]. These technologies enable firms to promptly identify market trends, changes in client demand, and potential risks in real-time. Additionally, they provide as a basis for formulating company strategies.

Strong data security measures are essential for effective data governance. This encompasses encryption, access limits, and periodic security assessments. By utilizing

cutting-edge security technologies and implementing best practices, MNCs may preserve sensitive data from cyber threats and unauthorized access [18]. This ensures compliance with regulations and protects their reputation.

Optimizing data governance in international organizations requires a holistic approach that combines strategic planning, ethical considerations, and technology innovation. To effectively traverse the challenges of the global business environment, MNCs can achieve data integrity, compliance, and competitive advantage by implementing strong data governance frameworks, improving compliance and ethical procedures, and utilizing technology. This comprehensive strategy not only fulfills regulatory obligations but also establishes multinational corporations as frontrunners in managing and protecting data, thereby cultivating trust and loyalty among consumers and stakeholders globally.

5 CONCLUSION

In reflecting upon the comprehensive examination of data governance within MNCs, this discourse has navigated through the multifarious challenges and proffered strategic recommendations essential for optimising data governance frameworks. In a context where data breaches can result in irreparable damage to a brand's reputation and where the effective usage of data can offer unmatched competitive benefits, the significance of strong data governance cannot be emphasized enough. MNCs encounter the formidable challenge of complying with numerous regulatory frameworks in various jurisdictions, each with its distinct regulations concerning data protection, privacy, and usage. Through the implementation of comprehensive data governance policies, these organizations can guarantee adherence to legal requirements, as well as secure the security and ethical utilization of data. This, in turn, cultivates consumer trust and improves company reputation. By incorporating cutting-edge technologies like artificial intelligence and machine learning into their data governance plans, MNCs can enhance their ability to comprehend and exploit their data assets. Nevertheless, this also necessitates the implementation of stringent ethical guidelines to regulate the utilization of these technologies, guaranteeing the responsible and unbiased use of data. Furthermore, it is imperative to regularly upgrade cybersecurity safeguards in order to safeguard against ever-changing threats, necessitating a consistent investment in both technological advancements and human knowledge. Flexibility and agility are crucial for multinational corporations when it comes to their data governance frameworks in order to effectively traverse the fast pace of digital transformation. Periodic evaluations and revisions of these frameworks are essential to tackle emerging difficulties and capitalize on technological improvements. In addition, actively including stakeholders, such as consumers, employees, and regulators, is crucial for developing a data governance policy that is both compliant and in line with societal values and expectations. This comprehensive strategy not only aligns with regulatory demands but also positions MNCs at the forefront of ethical and responsible data management.

REFERENCES

1. Alessia Lo Turco, Daniela Maggioni: The knowledge and skill content of production complexity. Research Policy 51(8), 104059(2022).
2. Martin Fadler, Christine Legner: Data ownership revisited: clarifying data accountabilities in times of big data and analytics. Journal of Business Analytics 5(1), 123-139(2020).
3. Rajeev Kumar: Ensuring data integrity of healthcare information in the era of digital health. Healthc Technol Lett 8(3), 66–77 (2021).
4. Simone Cenci, Matteo Burato, Marek Rei & Maurizio Zollo: The alignment of companies' sustainability behavior and emissions with global climate targets. Nature Communications 14 (7831) (2023).
5. Zhao, F., Iacono, S.: Big Data Research and Development Initiative (Federal, U.S.): In: Schintler, L.A., McNeely, C.L. (eds) Encyclopedia of Big Data, pp89-97 Springer, Cham (2022).
6. Liyuan Sun, Hongyun Zhang, Chao Fang. Data security governance in the era of big data: status, challenges, and prospects. Data Science and Management. 2, 41-44(2021).
7. Almahmoud, Z., Yoo, P.D., Alhussein, O. et al: A holistic and proactive approach to forecasting cyber threats. Sci Rep 13, 8049(2023).
8. Ballor GA, Yildirim AB: Multinational Corporations and the Politics of International Trade in Multidisciplinary Perspective. *Business and Politics*. 22(4), 573-586(2020).
9. Jobin, A., Ienca, M. & Vayena, E: The global landscape of AI ethics guidelines. Nat Mach Intell 1, 389–399(2019).
10. Roberto Chierici, Barbara Del Bosco, Alice Mazzucchelli1 & Claudio Chiacchierini: Enhancing Brand Awareness, Reputation and Loyalty: The Role of Social Media. International Journal of Business and Management 14(1),1833-3850(2019).
11. Diamantopoulou, V., Karyda, M: Integrating Privacy-By-Design with Business Process Redesign. In: Katsikas, S., *et al.* Computer Security. ESORICS 2021 International Workshops. ESORICS 2021. Lecture Notes in Computer Science, Vol. 13106, PP127-137 Springer, Cham.
12. Christine Holmström Lind, Olivia Kang, Anna Ljung, Paul Rosenbaum: Involvement of multinational corporations in social innovation: Exploring an emerging phenomenon, Journal of Business Research 151, 207-221(2022).
13. Cervi, G.V: Why and How Does the EU Rule Global Digital Policy: an Empirical Analysis of EU Regulatory Influence in Data Protection Laws**1**(18), (2022).
14. Tobias Seyffarth & Stephan Kuehnel: Maintaining business process compliance despite changes: a decision support approach based on process adaptations, Journal of Decision Systems 31(3), 305-335(2022).
15. Kroll, C. M., & Edinger-Schons, L. M: Corporate power and democracy: A business ethical reflection and research agenda. *Business Ethics, the Environment & Responsibility* 0(0), 1–14(2023).
16. Subhan Ullah, Kweku Adams, Dawda Adams, Rexford Attah-Boakye: Multinational corporations and human rights violations in emerging economies: Does commitment to social and environmental responsibility matter? Journal of Environmental Management, Volume 280,pp.111-689(2021).
17. Sukhpal Singh Gill, Shreshth Tuli, Minxian Xu, Inderpreet Singh, Karan Vijay Singh, Dominic Lindsay, Shikhar Tuli, Daria Smirnova, Manmeet Singh, Udit Jain, Haris Pervaiz, Bhanu Sehgal, Sukhwinder Singh Kaila, Sanjay Misra, Mohammad Sadegh Aslanpour,

Harshit Mehta, Vlado Stankovski, Peter Garraghan: Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges, Internet of Things, Volume 8, pp.100-118(2019).

18. Wasyihun Sema Admass, Yirga Yayeh Munaye, Abebe Abeshu Diro: Cyber security: State of the art, challenges and future directions, Cyber Security and Applications, Volume 2, pp.1-31(2024).