



Big Data Privacy and Ethical Concerns: Islamic Perspective

Wan Muhammad Fakhruddin Aiman Bin Wan Zakaria¹ and Akram M Zeki²

Kulliyyah of Information and Communication Technology, International Islamic University
Malaysia

¹fakhruddin.aiman@live.iium.edu.my and ²akramzeki@iium.edu.my

Abstract

Big Data ethical challenges were discovered through the lens of Islamic ethical principles, Maqasid al-Shariah. By highlighting its principles, it provides a comprehensive approach to managing privacy, fairness, and accountability in big data practices. The article addresses critical ethical dilemmas such as algorithmic bias, lack of transparency, unauthorized surveillance, and exploitation of personal and financial data, offering solutions that promote justice, fairness, and human dignity. By comparing Islamic ethical principles with secular frameworks like GDPR, the article demonstrates how Maqasid al-Shariah can fill ethical gaps in privacy protection, offering a more holistic and culturally sensitive model for data governance. While rooted in Islamic teachings, the framework is presented as a globally relevant approach that applies to both Muslim-majority and non-Muslim societies which concludes by calling for interdisciplinary research to integrate Islamic ethics with modern technological frameworks, promoting a more ethical, transparent, and socially responsible global data governance system.

Keywords - *Big Data Ethics, Privacy, Data Protection, Maqasid al-Shariah, Islamic Ethics*

1. INTRODUCTION

1.1. Big Data and its Ethical Implications

Big Data is a term that denotes extraordinarily large and intricate data sets that surpass the processing capabilities of conventional data management tools. This concept incorporates a wide array of data types, including structured, semi-structured, and unstructured data, which are generated from heterogeneous sources such as social media platforms, sensors, and transactional systems. The significance of Big Data is often encapsulated in the framework of the "Three Vs," which are Volume, Velocity, and Variety.

While big data has become a backbone of modern society, providing solid benefits such as improved decision-making, and enhanced operational efficiency, it raises critical ethical concerns around privacy and security. Privacy issues include inadvertent data collection by smart devices, re-identification of anonymized data, and exposure of sensitive behavioural information [1], [2]. On the security front, organizations face persistent threats from hackers, risks of data leakage, and vulnerabilities introduced by emerging technologies like differential privacy and

homomorphic encryption [3]. Addressing these challenges necessitates robust safeguards and innovative approaches to uphold ethical standards in data handling.

1.2. The Need for Islamic and Cultural Perspective on Big Data Privacy

In contemporary discussions about data privacy, secular frameworks like the GDPR emphasize individual autonomy and legal protections but often lack the cultural sensitivity required to address ethical concerns in Muslim societies. These frameworks prioritize personal rights and legal compliance, sometimes neglecting the communal and ethical dimensions that are deeply rooted in Islamic cultural contexts [4]. This gap becomes particularly evident in societies where religious values play a significant role in shaping public life and governance. Without incorporating these values, secular frameworks may struggle to resonate with local populations, potentially resulting in a lack of trust or adherence to privacy regulations. Moreover, the focus on individualism in secular ethics may conflict with the collective responsibilities emphasized in Islamic traditions, highlighting a mismatch between the ethical foundations of these societies and the frameworks designed to govern them.

Islamic ethics, rooted in the Quran and Hadith, provide an alternative perspective that aligns with the cultural and religious values of Muslim societies. By emphasizing the sanctity of privacy as a communal obligation, Islamic principles address both individual and collective responsibilities in safeguarding data [5]. Countries like Indonesia have begun integrating Islamic principles into their data protection laws, showcasing the potential for ethical governance that aligns with cultural values [6]. This approach not only ensures that privacy regulations resonate with local populations but also enhances accountability by embedding ethical considerations into legal frameworks. Therefore, integrating Islamic ethics into data privacy discussions offers a more inclusive and culturally attuned approach, addressing gaps that secular frameworks may leave unfilled.

1.3. Objectives

While several works explored ethical implications of Big Data and proposed general frameworks for responsible data management, the inclusion of Islamic perspectives remains limited and largely unstructured. A few studies, such as those by Alsharidah and [4], address ethical challenges in Islamic banking or digital consumer data security through an Islamic lens, yet they lack comprehensive theoretical frameworks that can systematize these insights. Additionally, existing frameworks, like those by [7], focus on general ethical and privacy concerns without addressing the nuanced requirements of Islamic ethics, which emphasize principles such as privacy, trustworthiness, and community well-being (Maqasid al-Shariah).

Although Islamic virtue-based approaches to artificial intelligence discussed by [8] show promise, they are not specifically adapted for Big Data contexts, leaving a gap in literature regarding how Islamic ethics can inform privacy frameworks within Big Data environments. Consequently, there is a need for a well-defined theoretical framework that applies Islamic ethical principles systematically to Big Data practices, offering actionable insights for ethical governance and data privacy in sectors influenced by Islamic values. So, the main objectives of this article:

- To explain how Islamic principles can be used to guide big data governance.
- To highlight the ethical issues in big data.

2. OVERVIEW OF BIG DATA AND ETHICAL CHALLENGES

2.1. Modern Applications of Big Data

Big data refers to the large volumes of data generated from various sources, characterized by its high velocity, variety, and volume. It has revolutionized sectors like healthcare, finance, and information technology by enabling the analysis of vast datasets to derive valuable insights. Big data applications rely on statistical approaches to ensure privacy and data utility. Techniques such as differential privacy, which adds calibrated noise to datasets, allow organizations to protect individual identities while maintaining the usability of data [9]. Similarly, secure multiparty computation (MPC) facilitates collaborative data analysis without exposing sensitive information, making it particularly beneficial in sectors like healthcare and finance. Anonymization and de-identification further enhance data privacy by masking identifiable information, ensuring compliance with regulations such as the GDPR and HIPAA [9].

In the healthcare sector, big data has significantly improved patient outcomes and disease management through analytics and predictive modeling. However, the utilization of medical big data comes with challenges in safeguarding patient privacy. Strategies such as encryption, anonymization, and secure sharing protocols are employed to protect sensitive patient data [10]. Additionally, ethical, and legal considerations are paramount in balancing the protection of personal information with the advantages of big data utilization. Regulatory frameworks and guidelines, such as those outlined in HIPAA, play a crucial role in maintaining this balance [11]. These measures ensure that healthcare data remains confidential while enabling valuable insights into disease trends and treatment efficacy. The integration of big data with information and communication technology (ICT) applications has introduced new tools for privacy protection. For instance, advanced encryption techniques like Two-Trapdoor Homomorphic Encryption (TTHE) enable secure data processing, enhancing both computational efficiency and data security [12]. Privacy-preserving machine learning models, such as federated learning and differential privacy, allow organizations to harness big data while minimizing the risk of data breaches [13]. Despite these advancements, challenges such as balancing privacy with utility, securing cloud-based data, and addressing evolving privacy attacks require ongoing research and innovation. By integrating robust privacy-preserving technologies with legal and ethical frameworks, big data can continue to drive innovation while protecting sensitive information.

2.2. Common Ethical Issues in Big Data

The vast and complex nature of big data has led to significant ethical concerns, particularly in areas such as privacy, discrimination, and accountability. One of the primary challenges is the lack of privacy and data protection, as big data collection often occurs without explicit consent, exposing individuals to risks of manipulation and loss of autonomy [14]. Technologies that enable extensive surveillance and profiling exacerbate this issue, allowing for automated decision-making that is not always transparent or fair as mentioned in [15]. These practices can undermine trust and lead to societal harm, especially when personal data is used irresponsibly. For instance, without robust protection measures, individuals may face exploitation through targeted manipulation or invasive profiling, posing a serious threat to their autonomy and privacy.

Another critical concern in big data is the potential for discrimination and unfair practices driven by algorithmic bias. Algorithms trained on biased datasets can perpetuate existing inequalities,

leading to discriminatory outcomes in sectors like healthcare and business analytics as in [16]. Additionally, a lack of fairness arises when datasets fail to represent diverse populations or when algorithms are not designed to account for equality [14]. This lack of inclusivity can exacerbate systemic inequities, disproportionately impacting marginalized groups. Coupled with the opacity of algorithms, which makes accountability and transparency challenging, these issues highlight the need for comprehensive ethical guidelines and regulatory frameworks to govern the responsible use of big data [17], [18]. By addressing these ethical challenges, big data can be harnessed to drive innovation while ensuring respect for individual rights and societal values.

In Islam, these ethical concerns are especially significant because privacy and fairness are not just legal or societal values but also deeply rooted in Islamic teachings. The Quran and Hadith emphasize the sanctity of privacy, justice, and accountability, which are integral to preserving individual dignity and communal harmony. Violations of data privacy through unauthorized collection or surveillance conflict with the Islamic principle of respecting others' confidentiality [14]. Additionally, algorithmic biases and discriminatory practices contradict the Islamic values of fairness and equality, which mandate that all individuals, regardless of their background, be treated justly. The lack of transparency in big data algorithms poses a further ethical challenge, as Islam advocates for accountability and openness in all matters, aligning closely with the concept of ethical governance. Addressing these issues in the context of Islamic values requires integrating ethical principles with technological advancements to ensure that big data serves the collective good without compromising religious and cultural integrity.

3. ISLAMIC ETHICAL FRAMEWORKS: MAQASID AL-SHARIAH

3.1. Maqasid Al-Shariah and its Relevance to Big Data

The Maqasid al-Shariah framework, which emphasizes the higher purposes of Islamic law, provides a comprehensive ethical foundation for addressing modern challenges in big data governance. Rooted in five key objectives — protection of faith (deen), life (nafs), intellect (aql), lineage (nasl), and wealth (maal) — Maqasid al-Shariah aims to promote human welfare and societal well-being. This ethical framework is especially relevant in the realm of big data, where issues such as privacy, transparency, and fairness are of paramount importance. By aligning big data governance with these objectives, organizations can ensure that their data practices prioritize ethical considerations, promote human welfare, and protect individual rights [19]. The Maqasid framework provides guidance on balancing the moral responsibilities of data collection, storage, and processing, ensuring that no harm is inflicted on individuals or communities. This approach allows for more responsible data governance, where the pursuit of technological advancement does not come at the expense of human dignity and societal equity [20].

The relevance of Maqasid al-Shariah to big data is further demonstrated in its emphasis on privacy, transparency, and equitable distribution. The framework promotes the protection of individual rights, which directly addresses ethical concerns surrounding privacy violations and data manipulation in big data systems [21]. By upholding these principles, organizations can create data governance policies that respect privacy, prevent exploitation, and ensure accountability in data-driven decision-making. Additionally, the integration of Maqasid principles into digital technologies, as seen in digital economy models like those implemented in pesantren, illustrates how Islamic values can be embedded within modern technological systems [22]. This integration not only promotes sustainable and responsible data management but also ensures that the benefits

of big data are equitably distributed among all stakeholders. Therefore, Maqasid al-Shariah offers a robust framework for navigating the ethical complexities of big data governance in a way that aligns with both Islamic values and global ethical standards.

3.2. Maqasid Al-Shariah Principles in Big Data Context

The Maqasid al-Shariah framework, which focuses on the preservation of religion, life, intellect, lineage, and property, provides a holistic approach to the governance of big data and privacy. By aligning big data governance with these objectives, organizations can ensure ethical, transparent, and socially responsible data practices. Each of these objectives offers specific guidance on how data should be collected, processed, stored, and shared in ways that respect Islamic ethical principles and societal welfare. This study explores how the five primary objectives of Maqasid al-Shariah relate to big data privacy and governance, supported by references from the Quran and Hadith.

The preservation of religion (Hifz al-Deen) emphasizes the protection of moral and ethical conduct in all aspects of life, including big data governance. Data practices should align with Islamic ethical values, ensuring that personal data is not exploited for purposes that violate religious principles. Ethical governance frameworks based on Maqasid al-Shariah prevent the misuse of data and promote justice, transparency, and accountability [19], [23]. Misuse of personal information, manipulation, and unethical surveillance violate the Quranic

principle found in Surah Al-Hujurat (49:12), which states: “And do not spy or backbite each other...”

This verse underscores the prohibition of unauthorized monitoring and privacy invasion. Islamic data governance should ensure that data privacy is respected, and ethical standards are upheld. By promoting justice and integrity, organizations can foster public trust and ensure that technological advancement aligns with Islamic principles.

The preservation of life (Hifz al-Nafs) aims to safeguard human life, health, and security. In the context of big data governance, this objective emphasizes the importance of protecting individuals' privacy and ensuring the security of personal information. Data breaches, unauthorized access, and identity theft pose direct threats to the well-being and security of individuals and communities. To fulfill this objective, big data governance must implement strong security protocols, such as encryption and access controls, to prevent the exploitation of personal data [24]. This aligns with the Islamic principle found in Surah Al-Ma'idah (5:32), which states: “Whoever saves a life, it is as if they have saved all of humanity.”

By protecting individuals from harm that could arise from privacy violations, organizations uphold the preservation of life. Big data practices must prioritize security to prevent breaches and misuse of personal data, ensuring the protection of individuals and their well-being.

The preservation of intellect (Hifz al-Aql) focuses on safeguarding human intellect, promoting knowledge, and preventing deception or misinformation. In the context of big data governance, this objective emphasizes the importance of using data to promote learning, understanding, and informed decision-making. It also calls for transparency and accountability in data analytics to ensure that individuals are not deceived or misled [25]. This principle aligns with the Quranic

command found in Surah Al-Baqarah (2:282), which emphasizes the importance of transparency and accountability in transactions: “And do not conceal testimony, for whoever conceals it – his heart is indeed sinful.”

This principle can be applied to big data governance, where concealing or manipulating data insights contradicts the Islamic value of transparency. Therefore, big data practices should be transparent, fair, and accountable, ensuring that decisions made using data are ethically sound and based on truthful, accurate information.

The preservation of lineage (Hifz al-Nasl) focuses on protecting family, social structure, and community welfare. Big data governance can support this objective by ensuring that data practices respect cultural and social norms while promoting equitable access to information and resources [26]. For instance, ensuring that marginalized communities are not excluded from technological advancements aligns with the Islamic value of social equity. Surah An-Nisa (4:1) emphasizes the importance of social welfare and kinship ties, stating: “Be mindful of your duties towards your kin and fear Allah.”

This principle can be applied to big data by ensuring that social welfare is promoted through equitable access to technological resources. Organizations should use big data to bridge social and economic divides rather than reinforce existing inequalities. Privacy considerations must also respect the social fabric, ensuring that family and community data are not misused in ways that could harm relationships or community well-being.

The preservation of property (Hifz al-Mal) seeks to protect individual and communal wealth and ensure economic justice. In big data governance, this objective requires the responsible and ethical management of data as a valuable digital asset. Organizations must prevent the misuse of personal data for financial exploitation or economic injustice, ensuring fairness in economic transactions and preventing wealth disparities [27]. The Quran emphasizes the importance of protecting wealth in Surah Al-Baqarah (2:188), which states: “Do not consume one another’s wealth unjustly or send it [in bribery] to the rulers in order that [they might aid] you to consume a portion of the wealth of the people in sin, while you know [it is unlawful].”

This principle can be applied to big data governance, where organizations should avoid data-driven practices that exploit or unfairly profit from consumers. Companies must ensure fair distribution of wealth, avoid data monetization practices that harm users, and uphold the principle of fairness and economic justice in data-driven decision-making.

The five key objectives — preservation of religion, life, intellect, lineage, and property — offer essential guidance for managing data ethically and responsibly. Each objective is grounded in the Quran and Hadith, providing specific moral imperatives that can be applied to contemporary data governance. From protecting privacy and ensuring security to promoting transparency and social welfare, the Maqasid framework aligns with Islamic principles of justice and fairness. By integrating these objectives into big data governance, the practices of ethical, inclusive, and sustainable data practices in the organizations can be developed to respect Islamic values and contribute to societal well-being.

4. DISCUSSIONS

4.1. Ethical Dilemmas in Big Data from an Islamic Perspective

Big data technologies have introduced several ethical dilemmas, especially in privacy, accountability, and fairness. From an Islamic perspective, it is a profound moral and spiritual issue rather than just a technical or regulatory obstacle. Maqasid al-Shariah should be used as a framework for governing big data as it aims to preserve fundamental human values. These principles provide guidance for assessing and rectifying ethical dilemmas in big data governance.

One major ethical dilemma in big data is the issue of algorithmic bias, as mentioned in [14] where AI models trained on biased datasets produce unfair or discriminatory outcomes. This is especially problematic in sectors like hiring, finance, and healthcare, where biased algorithms can result in unjust treatment of marginalized groups. From the perspective of Hifz al-Aql (preservation of intellect), fairness and transparency in decision-making are essential to protect human reasoning and knowledge. The Quran emphasizes this value in Surah Al- Baqarah (2:282), which states, "And do not conceal testimony, for whoever conceals it – his heart is indeed sinful." Transparency in AI models aligns with this Quranic directive, as it ensures that the logic and rationale behind decisions are clear and explainable. To address this dilemma, organizations should employ fairness audits, ensure datasets are diverse, and require that AI models are explainable, thereby upholding the principle of Hifz al-Aql.

Another key dilemma is the lack of transparency in AI and data-driven models, often referred to as the "black box problem," where the internal logic of AI models remains opaque and inaccessible. This lack of accountability contradicts Islamic teachings on openness and justice. The principle of Hifz al-Nafs (preservation of life) calls for measures that protect individuals from harm, which extends to preventing harm caused by opaque AI systems. Individuals are at risk of unfair decisions that affect their lives, such as being denied loans, medical care, or job opportunities without transparency. Islamic teachings emphasize fairness and justice, as seen in Surah An-Nisa (4:135), which states, "Be persistently standing firm in justice, witnesses for Allah, even if it be against yourselves or parents and relatives." This verse highlights the importance of justice and fairness, which should be embedded into AI and big data governance by requiring organizations to disclose the logic and criteria used in decision-making processes.

Islamic ethical principles from Maqasid al-Shariah offer a vigorous framework for addressing ethical dilemmas in big data governance. Issues like algorithmic bias, opaque AI models, unauthorized surveillance, and data commodification can be assessed and resolved through the application of these principles. By maintaining the principles of Maqasid al-Shariah, designing, and governing big data can be improved to protect privacy, promote transparency, and ensure justice. Embedding these principles into data governance policies and technological frameworks can create a more ethical, inclusive, and socially responsible approach to big data governance in Muslim-majority countries and beyond.

5. CONCLUSION

The Islamic perspective on big data ethics offers a holistic and universally applicable framework for privacy and governance that extends beyond the scope of secular frameworks like GDPR. Unlike secular approaches that prioritize individual autonomy, the Islamic approach emphasizes collective responsibility, societal welfare, and moral accountability which are principles that are

relevant to all societies, not just Muslim-majority countries. By embedding these universal ethical principles into big data governance frameworks, nations can bridge the gap between ethical obligations and technical standards, promoting a more inclusive, just, and culturally attuned approach. Countries like Indonesia have demonstrated the potential for integrating Maqasid al-Shariah into data protection laws, setting a precedent for other nations seeking to align their regulatory frameworks with comprehensive ethical values. As ethical challenges in big data continue to grow, the Maqasid al-Shariah framework provides a globally relevant model for ensuring justice, equity, and dignity in digital ecosystem.

6. REFERENCES

- [1] X. Chen, 'A preliminary discussion on data privacy and data security issues', *Appl. Comput. Eng.*, 2024, doi: 10.54254/2755-2721/71/20241710.
- [2] A. Shahzad, H. U. R. Kayani, A.A.Malik, M. A. Raza, and A. Saleem, 'Big data security, privacy protection, tools and applications', *Pak. J. Sci.*, 2023, doi: 10.57041/pjs.v75i02.850.
- [3] A. Asasfeh, L. Tarawneh, M. R. Pradhan, and N. A. Al-Dmour, 'Privacy and Security Concerns in Big Data', 2024, pp. 1–5. doi: 10.1109/iccr61006.2024.10532931.
- [4] A. A. Saputra, M. I. Fasa, and D. Ambarwati, 'Islamic-Based Digital Ethics: The Phenomenon of Online Consumer Data Security', *Share J. Ekon. Dan Keuang. Islam*, 2022, doi: 10.22373/share.v11i1.11167.
- [5] W. Nadwi and M. A. M. Uday, 'The Right to Privacy: Foundations and Protections in Islamic Jurisprudence', *Int. J. Relig.*, 2024, doi: 10.61707/864v8350.
- [6] T. I. Putra, A. J. Islam, and A. M. A. Rahman, 'Integrating Islamic Laws into Indonesian Data Protection Laws: An Analysis of Regulatory Landscape and Ethical Considerations', *Contemp. Issues Interfaith Law Soc.*, 2024, doi: 10.15294/ciils.v3i1.78690.
- [7] E. Vayena, U. Gasser, A. Wood, D. O'Brien, and M. Altman, 'Elements of a new ethical framework for big data research', *Wash. Lee Law Rev.*, 2016, doi: 10.5167/UZH-135645.
- [8] A. Raquib, B. Channa, T. Zubair, and others, 'Islamic virtue-based ethics for artificial intelligence', *Discov. Artif. Intell.*, vol.2, no. 1, pp.1–11, 2022, doi: 10.1007/s44163-022-00028-2.
- [9] H. J. Ezeah, 'Big Data and Privacy with a focus on Statistical Approaches to Ensuring Data Confidentiality', *NEWPORT Int. J. Curr. ISSUES ARTS Manag.*, 2024, doi: 10.59298/nijciam/2024/4.3.7274.
- [10] R. M. Devadas, V. Hiremani, N. S. Rani, K. R. Bhavya, and R. Sapna, 'A Comprehensive Study on Patient Privacy and Data Security in Big Data Healthcare Applications', *Adv. Med. Technol. Clin. Pract. Book Ser.*, 2024, doi: 10.4018/979-8-3693-2703-6.ch002.
- [11] T. Hong and X. Chen, 'Applications of Medical Big Data and Personal Information Protection', *의생명과학과 법*, 2024, doi: 10.22397/bml.2024.31.233.
- [12] S. A. Kumar, T. K, and T. T, 'Privacy-preserving techniques in big data and information security', *ICTACT J. Commun. Technol.*, 2024, doi: 10.21917/ijct.2024.0493.
- [13] Q. H. Dongyuan Ge Qianyi Fang, 'Privacy Protection in Information and Communication Technology Applications Based on Big Data', *J. Electron. Inf. Sci.*, 2024, doi: 10.23977/jeis.2024.090209.
- [14] S. Kröger and R. Bellamy, 'Data Ethics', 2024, doi: 10.1093/oxfordhb/9780198877820.013.36.
- [15] M. D. Bormida, 'The Big Data World: Benefits, Threats and Ethical Challenges', 2021. doi: 10.1108/S2398-601820210000008007.

- [16] N. Daga and G. K. Joseph, 'Big Data and Bigger Dilemmas: Ethical Concerns of Data in Healthcare', 2024, doi: 10.1109/mipr62202.2024.00117.
- [17] A. Lala and P. Jain, 'Investigating the ethics of big data and data mining', 2024. doi: 10.58532/nbennurch293.
- [18] A. Golyan, S. S. Panchal, D. Vaghasiya, and H. Parekh, 'Data Ethics and Privacy', in *Advances in systems analysis, software engineering, and high performance computing book series*, 2024. doi: 10.4018/979-8-3693-3609-0.ch011.
- [19] M. D. @ M. Junus, N. K. M. Husin, N. H. Z. Abidin, N. R. Khadzali, and M. Ma'dan, 'Ethical Governance through Maqasid Shariah Perspective: A Conceptual Framework', *Int. J. Acad. Res. Bus. Soc. Sci.*, 2024, doi: 10.6007/ijarbss/v14-i10/23148.
- [20] R. Sheikh, 'Shari'ah Governance and Shari'ah Non-Compliance Risk Management: A Maqāsid Shari'ah Based Appraisal', *J. Islam. Thought Civiliz.*, 2023, doi: 10.32350/jitc.131.19.
- [21] M. Mohadi and Y. Tarshany, 'Maqasid Al-Shari'ah and the Ethics of Artificial Intelligence', *J. Contemp. Maqasid Stud.*, 2023, doi: 10.52100/jcms.v2i2.107.
- [22] Y. A. Bashori, K. Umami, and S. H. Wahid, 'Maqasid shariah-based digital economy model: integration, sustainability and transformation', *Malays. J. Syariah Law*, 2024, doi: 10.33102/mjssl.vol12no2.647.
- [23] S. Sumarta, B. Burhanudin, and T. Budiyanto, 'Maqasid Al-Syariah Mendorong Keadilan Dan Keseimbangan Dalam Hukum Islam', *Khulasah Islam. Stud. J.*, 2024, doi: 10.55656/kisj.v6i1.120.
- [24] M. S. A. E. Farag and T. Rashed, 'The Impact of Maqasid Al Shariah (Objectives of Islamic Shariah) to Obtain Legal Protection of Humans; A Comparative and Analytical Study of the Qatari Laws', *J. Law Sustain. Dev.*, 2023, doi: 10.55908/sdgs.v11i9.983.
- [25] W. Widya and A. Syafi'i, 'Application of Islamic Business Ethics in the Fintech Industry: an Analysis of the Foundation of Sharia Maqashid', 2024, doi: 10.58631/ajemb.v2i12.68.
- [26] A. Munir and K. Kusnadi, 'Maintaining the Social Environment: Urgency and Principles in Maqasid Al-Shariah', *Tribakti Kediri*, 2024, doi: 10.33367/tribakti.v35i2.5417.
- [27] M. Habibullah, A. A. Faruque, M. O. Faruque, and M. Atiullah, 'Islamic Economic Framework for the Exercise of Islamic Financial Activities: its Conformity with Maqasid Shari'ah', *AL-BURHAN*, 2023, doi: 10.31436/alburhn.v7i1.300.