

Maqāṣid al-Syarī'ah as an Ethical Framework for Islamic Law in the Big Data Era: An Analysis of Personal Data Protection in the Digital Ecosystem

Muhammadong^{a*}

^a Universitas Negeri Makassar, Indonesia
email: muhammadong@unm.ac.id *

INFO ARTIKEL

Riwayat Artikel:

Received : 12 September 2026

Revised : 4 Oktober 2026

Accepted : 12 Oktober 2026

Keywords:

Maqāṣid al-Sharī'ah; Personal
Data Protection; Islamic Law;
Big Data; Digital Ethics.

DOI: 10.62335

ABSTRACT

The activities of collecting, processing, storing, and exchanging personal data have increased due to the rapid development of the digital ecosystem and the increasing dependence on big data. While there are many benefits to these developments, there are also significant risks, including data misuse, privacy violations, information breaches, and the use of people's personal information without their consent. This study aims to examine personal data protection from the perspective of Maqāṣid al-Sharī'ah and evaluate its applicability as an ethical framework of Islamic law in addressing the issues presented by the big data era. Both conceptual and statutory normative legal research methods are used in this study. Primary and secondary legal documents pertaining to Islamic law, Maqāṣid al-Sharī'ah, and personal data protection are examined using qualitative descriptive analysis. The findings demonstrate that the objectives of Maqāṣid al-Sharī'ah, particularly *ḥifḍ al-naḥs* (protection of life), *ḥifḍ al-'aql* (protection of intellect), *ḥifḍ al-'māl* (protection of property), and *ḥifḍ al-'ird* (protection of dignity), are closely related to the protection of personal data. The need of informed consent, data security, purpose limitation, openness, and preventing harmful data exploitation are all highlighted by these concepts. In order to build personal data governance that promotes public welfare, upholds human dignity, and prevents harm in the digital ecosystem, the study concludes that Maqāṣid al-Sharī'ah provides an additional ethical foundation to positive legislation.

INTRODUCTION

The development of digital technology has changed how people connect with one another in a number of spheres of life, including social communication, public services, education, and the economy. (I.O. Assayouti and S.A. Ogunwolu, 2026). The growing use of internet-based platforms, artificial intelligence, cloud computing, and big data technologies which can process enormous volumes of data quickly and intricately are characteristics of this digital transformation. Personal

data is now considered a strategic asset with substantial economic, political, and social significance rather than just administrative data. Electronic transactions, social media use, online healthcare services, and digital government systems are just a few examples of the many digital activities that constantly produce data footprints that may be examined and used for a variety of objectives. (F. Rafiq, M.J. Awan, A. Yasin, H. Nobanee, A.M. Zain and S.A. Bahaj, 2022).

But the growth of the digital ecosystem has also brought up serious problems with the security of personal information. (A. Majeed, S. Khan and S.O. Hwang, 2022). The hazards of data abuse, data breaches, unauthorised digital monitoring, and the exploitation of personal information without sufficient authorisation have increased due to the growing volume of data gathering and processing. Numerous instances of data leakage in various industries show that individual data protection cannot be ensured by technology security measures alone. The ethical, moral, and legal issues of the proper management and use of human information are all part of the problem of personal data protection, in addition to its technological aspects.

In response to new digital issues, several nations have created personal data protection laws within the scope of contemporary law. One of the most significant legal frameworks is the General Data Protection Regulation (GDPR) of the European Union, which emphasises user permission, transparency, data processing constraints, and individual rights over personal information. (V. Mone and C.L.V. Sivakumar, 2022). An analysis of the GDPR). Law Number 27 of 2022 concerning Personal Data Protection, which governs data subject rights, data controller obligations, and procedures for oversight and dispute resolution, reflects Indonesia's attempts to improve personal data protection. Positive legal alternatives, however, are still unable to adequately handle the moral dilemmas brought on by ever-more complicated technical advancements. (E.A.P. Manurung, 2023).

Prior research has looked at personal data protection from a number of angles, including digital ethics, information technology, and legal frameworks. Compared to earlier regulatory models, research on the GDPR shows that rights-based regulatory methods offer better protection for individual privacy. (M.A. Dar and S.A. Wani, 2023). In order to reduce the dangers of a data breach, several research on digital data security stress the significance of putting technological measures like encryption, access control, and information security governance into place. In the meantime, the relationship between digital privacy concerns and Islamic principles pertaining to the defence of individual rights, public welfare, and human dignity has been the subject of more recent Islamic legal research. (Y. Lestari M.M. Mujib, 2022).

The notion of *maqāṣid al-syarī'ah*, which refers to the core goals of Islamic law in achieving human wellbeing (*maṣlahah*) and preventing harm (*mafsadah*), can be used to analyse personal data protection from an Islamic perspective. The preservation of religion (*ḥifḍ al-dīn*), life (*ḥifḍ al-nafs*), intelligence (*ḥifḍ al-'aql*), lineage (*ḥifḍ al-nasl*), and property (*ḥifḍ al-māl*) are the five fundamental tenets of this philosophy. (M. Mohadi and Y. Tarshany, 2023). *Maqāṣid al-syarī'ah* has been extended in modern Islamic legal philosophy as an analytical framework for dealing with novel topics that were not specifically covered in traditional Islamic law, such as the protection of personal information and digital technologies. Personal information can be viewed as a component of personal security, ownership rights, and individual dignity (*ḥifḍ al-'ird*), (M. Supardi, H. Hanif, M. Rahman, A.F. Arham

and A.M.A. Amiruddin, 2026), all of which need to be protected from exploitation and abuse.

There are still a number of restrictions, despite the fact that earlier research has made significant contributions to the understanding of the connection between digital law, privacy, and Islamic ethical principles. (K.P. Wicaksana, T.P. Alfath H. Kuswanto, 2026). First, legal legislation and technical security measures are the main focus of many research on personal data protection, with little attention paid to the ethical underpinnings of data protection. Second, current research on *maqāṣid al-syarī'ah* and digital technology is mainly conceptual and has not adequately developed an analytical framework that links *maqāṣid* principles with modern Big Data challenges, such as large-scale data collection, predictive algorithms, and data utilisation outside of data owners' direct control. Third, little research has looked at an integrated strategy that combines contemporary data governance with Islamic law ethics as a whole way to deal with issues in the digital ecosystem. (I.M. Fauzi, F. Nurfatwa, D.S.S.R. Sandiana, R.D. Anjani, M.N. Fawwaz, M. Latifa and T. Wijaya, 2026).

In light of these constraints, the purpose of this study is to examine the protection of personal data in the digital environment from the standpoint of *maqāṣid al-syarī'ah*, an ethical framework of Islamic law. (Elmahjub, E. (2023). The goal of this study is to determine how *maqāṣid* principles might offer ethical direction for controlling the gathering, use, and safeguarding of personal data in the Big Data era. Additionally, by investigating the applicability of *maqāṣid al-syarī'ah* in addressing new digital concerns, this work seeks to advance modern Islamic legal discourse. (M. Nidhom and A. Murtadho, 2025). This study uses a normative-conceptual legal research design and a qualitative methodology to investigate the protection of personal data using the framework of *maqāṣid al-syarī'ah*. Both primary and secondary legal materials are used in the study. The primary materials include Indonesian Law Number 27 of 2022 on Personal Data Protection, pertinent verses from the Qur'an, and prophetic traditions pertaining to privacy, dignity, and the defence of individual rights. Peer-reviewed journal papers, scholarly books, and academic publications about digital privacy, Big Data, digital ethics, data governance, and *maqāṣid al-syarī'ah* are examples of secondary resources. (R. Budiman, 2023)

Combinations of the terms "personal data protection, data privacy, Big Data, digital privacy, Islamic law, and *Maqasid al-Shariah* are used in the literature search throughout Scopus, Web of Science, ScienceDirect, and Google Scholar. The selection of sources is based on their scholarly credibility, accessibility, relevance to the research issues, and direct connection to the security of personal data in digital ecosystems. To improve transparency and reduce selection bias, the selection process uses systematic literature review approaches, especially specific inclusion and exclusion criteria (Snyder, 2019).

Thematic analysis is used to examine the gathered resources in accordance with Braun and Clarke (2006). Data collection, processing, storage, utilisation, transfer, and abuse are the six categories into which data protection issues fall. Based on Auda's (2008) systems approach to *maqāṣid al-syarī'ah*, the identified themes are then mapped into the principles of *ḥifḍ al-naḥs*, *ḥifḍ al-'aql*, *ḥifḍ al-māl*, *ḥifḍ al-nasl*, and *ḥifḍ al-'ird*. Lastly, a *maqāṣid*-based ethical framework for personal data governance in the Big Data era is developed by synthesising these findings through interpretive and comparative studies.

RESEARCH METHOD

This study uses a normative-conceptual legal research design and a qualitative methodology to investigate the protection of personal data using the framework of *maqāṣid al-syarī'ah*. Both primary and secondary legal materials are used in the study. The primary materials include Indonesian Law Number 27 of 2022 on Personal Data Protection, pertinent verses from the Qur'an, and prophetic traditions pertaining to privacy, dignity, and the defence of individual rights. Peer-reviewed journal papers, scholarly books, and academic publications about digital privacy, Big Data, digital ethics, data governance, and *maqāṣid al-syarī'ah* are examples of secondary resources.

Combinations of the terms "personal data protection," "data privacy, Big Data, digital privacy, Islamic law, and *Maqasid al-Shariah* are used in the Scopus and Google Scholar literature search. The selection of sources is based on their scholarly credibility, accessibility, relevance to the research issues, and direct connection to the security of personal data in digital ecosystems. To improve transparency and reduce selection bias, the selection process uses systematic literature review approaches, especially specific inclusion and exclusion criteria (Snyder, 2019).

In accordance with Braun and Clarke, the gathered materials are subjected to thematic analysis. Data protection concerns are classified into six categories: data collection, processing, storage, utilisation, transfer, and abuse. (V. Braun and Clarke, 2006). Auda's systems approach to *maqāṣid al-syarī'ah* informs the mapping of the identified themes onto the principles of *ḥifḍ al-naḥs*, *ḥifṣ al-'aql*, *ḥifṣ al-māl*, *ḥifḍ al-nasl*, and *ḥifṣ al-'ird*. Lastly, a *maqāṣid*-based ethical framework for personal data governance in the Big Data era is developed by synthesising these findings through interpretive and comparative studies. (J. Auda, (2008).

RESULT AND DISCUSSION

The results show that one of the main goals of *maqāṣid al-sharī'ah* is the protection of personal data in the digital environment. The protection of human dignity, individual security, property, intellectual autonomy, and the continuation of human interests in digital settings are all intimately linked to personal data, in addition to informational secrecy. In this sense, *ḥifḍ al-'ird* (protection of dignity), *ḥifḍ al-māl* (protection of property), *ḥifḍ al-naḥs* (protection of life), and *ḥifḍ al-'aql* (protection of intellect) were shown to be most closely linked to the protection of personal data. Together, these four factors create a cohesive ethical framework for evaluating the gathering, storing,

According to the first significant finding, the dimension most closely linked to digital privacy is *ḥifḍ al-'ird*, or the protection of dignity. A person's dignity and reputation may be compromised by unauthorised disclosure, publication, or access to personal data since it is an essential component of their identity and private space. This result is in line with Assayouti and Ogunwolu's (2026) assertion that *ḥifḍ al-'ird* is a fundamental criterion for assessing digital surveillance, especially with regard to human dignity, consent, proportionality, and the avoidance of unwarranted intrusion. In a similar vein, Rozani, Ahmad Fuad, and Abd Aziz (2026) highlight the importance of confidentiality, honour, and accountability in information management as fundamental components of Islamic privacy ethics.

The second finding shows that *ḥifḍ al-māl* and personal data protection are closely related. Personal data has economic worth in the big data ecosystem and can be used for consumer analysis, business profiling, and profit-making. As a result, improper control over the use of personal data may lead to economic exploitation in addition to privacy concerns. This result is in line with Wan Zakaria and Zeki's (2026) assertion that one of the main ethical issues with big data techniques is the exploitation of financial and personal data.

The final conclusion emphasises the importance of *ḥifḍ al-nafs* in guaranteeing personal safety. When personal information is used for fraud, tracking, intimidation, identity theft, or other types of harm, data breaches and misuse may pose concerns that go beyond digital environments. This implies that safeguarding people from possible danger is closely related to data security. Within Islamic value-based approaches to digital governance, Mustofa et al. (2026) also link data privacy to *ḥifḍ al-nafs*, *ḥifḍ al-'ird*, and *ḥifḍ al-māl*.

The fourth finding demonstrates how *ḥifḍ al-'aql* has fresh relevance in the age of big data and algorithms. Building behavioural profiles, forecasting preferences, and influencing personal decisions are all possible with data processing. As a result, maintaining intellectual autonomy and decision-making freedom is closely related to protecting personal data. This result is consistent with Wan Zakaria and Zeki's (2026) identification of algorithmic bias, lack of transparency, and unapproved surveillance as significant ethical issues in big data settings. Overall, the results show that *maqāṣid al-sharī'ah* offers a multifaceted framework for protecting personal information. Such protection includes safeguarding human autonomy, economic interests, security, and dignity in addition to information secrecy. The results thus establish *maqāṣid al-sharī'ah* as a pertinent ethical basis for enhancing responsible data governance in the big data era.

The results show that, in the context of *maqāṣid al-sharī'ah*, protecting personal data in the digital environment can be seen as a crucial part of defending basic human rights. This is especially evident in *ḥifḍ al-'ird*, *ḥifḍ al-māl*, *ḥifḍ al-nafs*, and *ḥifḍ al-'aql*. These connections can be explained by the fact that personal data serves not only as identifying information but also has ramifications for economic interests, human dignity, security, and individual decision-making freedom. As a result, the misuse of personal data may have consequences that go beyond the loss of confidentiality, such as harm to one's reputation, financial exploitation, security threats, and behavioural manipulation motivated by algorithms.

These results align with Assayouti and Ogunwolu's (2026) identification of *ḥifḍ al-'ird* as an ethical basis for restricting digital surveillance that could violate privacy and human dignity. The findings are also consistent with the findings of Rozani et al. (2026), who stress the significance of responsibility, *amānah*, secrecy, and respect for privacy in the handling of digital information. According to this convergence, protecting personal data from an Islamic perspective involves more than just following the law; it also has a moral component that calls for responsibility and caution while using personal data.

In contrast to Wan Zakaria and Zeki (2026), who identify algorithmic bias, data exploitation, lack of transparency, and unauthorised monitoring as important ethical challenges in big data, the current

study expands on this view by directly connecting these difficulties to *ḥifḍ al-ʿaql*. This suggests that data-driven manipulation may jeopardise freedom of choice and intellectual autonomy in addition to privacy. The results support Mustofa et al.'s (2026) assertion that data privacy is a component of Islamic value-based digital governance. Overall, the findings show that *maqāṣid al-sharīʿah* offers a multifaceted ethical framework for evaluating personal data protection more thoroughly in the big data era.

The results show that protecting personal data in the digital ecosystem should be viewed as an ethical matter closely linked to the defence of basic human rights rather than just as a technical information security issue. The study's goal, which presents *maqāṣid al-sharīʿah* as an ethical framework of Islamic law for addressing the difficulties of protecting personal data in the big data era, is addressed by this finding. This finding is primarily significant because it broadens the definition of data protection to include the protection of human dignity, security, economic interests, and individual autonomy in addition to the maintenance of confidentiality. As a result, measures that are exclusively focused on regulatory compliance do not have the same moral implications as personal data protection.

The connection between *ḥifḍ al-ʿird* and personal data protection suggests that personal information is a component of a person's domain of honour and dignity. When used without permission or released illegally, information about identification, behaviour, interests, and digital activities may have an impact on a person's reputation and social standing. In this sense, data protection entails more than just stopping information leaks; it also entails making sure that people maintain control over the access and use of their digital identities. Even in situations when interactions are mediated by digital technologies, this interpretation upholds the importance of human dignity as an ethical priority.

Within the big data ecosystem, personal data has gained significant economic worth, as demonstrated by the *ḥifḍ al-māl* discovery. User data can be processed to support business plans, determine preferences, and create consumer profiles. This situation implies that misuse of data could lead to new types of economic exploitation, especially when data subjects don't have enough control, comprehension, or fair reward. As a result, *ḥifḍ al-māl* highlights how crucial it is to use data fairly and to stop actions that turn people into nothing more than digital commodities.

In the meantime, the relationship with *ḥifḍ al-naḥs* shows that data exploitation may have repercussions outside of virtual environments. Leaked or carelessly managed personal data may be exploited for fraud, tracking, intimidation, or other types of harm that compromise people's safety and wellbeing. This result demonstrates that data security has a real protective component and is intimately linked to preventing personal injury. In the era of algorithms, the dimension of *ḥifḍ al-ʿaql* becomes very important. In addition to being gathered to comprehend user behaviour, data can also be utilised to forecast and impact personal choices. At this stage, personal autonomy and freedom of thought are tightly linked to data protection. The problem goes beyond privacy to include the possible deterioration of a person's ability to make independent decisions when digital systems have the ability to influence choices in opaque ways. (M.K.I. Mukmin Hakim and M. Mat Jubri Shamsuddin, 2024).

Overall, the results show that *maqāṣid al-sharī'ah* serves as both an evaluative tool and a normative framework for data governance activities. Data-processing procedures can be assessed in terms of accountability, meaningful consent, harm prevention, justice, and societal benefit using the principles of *amānah*, *tarāḍī*, *dar' al-mafāsīd*, *'adālah*, and *maṣlaḥah*. (Arminsyah, A. (2025). This study thus confirms the importance of *maqāṣid al-sharī'ah* in directing data governance that is not only compatible with the law but also morally sound, human centered, and focused on advancing human welfare.

CONCLUSION

This study shows that the framework of *maqāṣid al-sharī'ah* can provide a thorough understanding of personal data protection in the digital ecosystem. The results verify that data protection extends beyond information confidentiality and includes safeguarding human dignity through *ḥifḍ al-'irḍ*, economic interests through *ḥifḍ al-māl*, individual security through *ḥifḍ al-'nafs*, and intellectual autonomy through *ḥifḍ al-'aql*. According to this approach, commercial exploitation, excessive surveillance, data misuse, and algorithmic manipulation could all be considered types of harm that are at odds with the core goals of Islamic law. This ethical approach is further reinforced by the concepts of *amānah*, *tarāḍī*, *'adālah*, *maṣlaḥah*, and *dar' al-mafāsīd*, which emphasise accountability, meaningful consent, justice, public benefit, and harm prevention.

These results logically point to the necessity of creating Islamic education that is more sensitive to modern digital challenges. In order for students to comprehend digital concerns from both a technological and an ethical and Islamic standpoint, educational approaches should incorporate data literacy, algorithmic ethics, privacy, digital security, and responsible technology use. These results emphasise the significance of expanding *maqāṣid al-sharī'ah* discourse into the domains of technology, artificial intelligence, and data governance for the advancement of Islamic studies. While maintaining their normative commitment to human dignity, justice, and welfare, such an expansion can enhance the contextual and multidisciplinary nature of Islamic studies. In this way, Islamic scholarship can continue to support the safety and welfare of people and society while remaining intellectually relevant in the face of the swift digital transition.

REFERENCES

- Arminsyah, A. (2025). Maqasid al-Shariah in contemporary legal systems: An analysis of digital rights and privacy protection. *Al-Qadha: Jurnal Hukum Islam dan Perundang-Undangan*, 12(2), 289–308. <https://doi.org/10.32505/qadha.v12i2.11178>
- Assayouti, I. O., & Ogunwolu, S. A. (2026). Digital surveillance and human dignity (*ḥifẓ al-'irḍ*): An Islamic ethical appraisal with reflections from Nigeria. *International Journal of Research and Innovation in Social Science*, 10(2), 4652–4665. <https://doi.org/10.47772/IJRISS.2026.10200341>

- Auda, J. (2008). *Maqasid al-Shariah as philosophy of Islamic law: A systems approach*. International Institute of Islamic Thought.
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp063oa>
- Budiman, R. (2023). The development of personal data protection law in Indonesia: Challenges and prospects for the implementation of Law No. 27 of 2022. *Jurnal Smart Hukum*, 2(1), 24–36. <https://doi.org/10.55299/jsh.v2i1.1352>
- Dar, M. A., & Wani, S. A. (2023). COVID-19, personal data protection and privacy in India. *Asian Bioethics Review*, 15(2), 125–140. <https://doi.org/10.1007/s41649-022-00227-0>
- Elmahjub, E. (2023). Artificial intelligence (AI) in Islamic ethics: Towards pluralist ethical benchmarking for AI. *Philosophy & Technology*, 36(4), Article 73. <https://doi.org/10.1007/s13347-023-00668-x>
- Fauzi, I. M., Nurfatwa, F., Sandiana, D. S. S. R., Anjani, R. D., Fawwaz, M. N., Latifa, M., & Wijaya, T. (2026). Tinjauan Maqashid Syariah terhadap perlindungan data pribadi nasabah pada digital payment. *SIL'AH: Jurnal Ekonomi Syariah*, 3(1), 1–16. <https://doi.org/10.64994/silah.v3i1.78>
- Lestari, Y., & Mujib, M. M. (2022). Optimizing personal data protection legal framework in Indonesia: A comparative law study. *Supremasi Hukum: Jurnal Kajian Ilmu Hukum*, 11(2), 203–234. <https://doi.org/10.14421/sh.v11i2.2729>
- Majeed, A., Khan, S., & Hwang, S. O. (2022). Group privacy: An underrated but worth studying research problem in the era of artificial intelligence and big data. *Electronics*, 11(9), 1449. <https://doi.org/10.3390/electronics11091449>
- Manurung, E. A. P. (2023). The right to privacy based on the Law of the Republic of Indonesia Number 27 of 2022. *Journal of Digital Law and Policy*, 2(3), 103–110. <https://doi.org/10.58982/jdip.v2i3.287>
- Mukmin Hakim, M. K. I., & Mat Jubri Shamsuddin, M. (2024). Maqasid Al-Shariah in the age of AI: A critical examination of ChatGPT usage among International Islamic University Malaysia students. *Online Journal of Research in Islamic Studies*, 11(2), 1–18. <https://doi.org/10.22452/ris.vol11no2.1>
- Mohadi, M., & Tarshany, Y. (2023). Maqasid al-Shari'ah and the ethics of artificial intelligence: Contemporary challenges. *Journal of Contemporary Maqasid Studies*, 2(2), 79–102. <https://doi.org/10.52100/jcms.v2i2.107>
- Mone, V., & Sivakumar, C. L. V. (2022). An analysis of the GDPR compliance issues posed by new emerging technologies. *Legal Information Management*, 22(3), 166–174. <https://doi.org/10.1017/S1472669622000317>

- Nidhom, M., & Murtadho, A. (2025). Does Islam protect digital privacy? An Islamic studies approach to personal data protection. *Al-Afham: Journal of Islamic Studies*, 2(2), 107–128. <https://doi.org/10.62509/ajis.v2i2.260>
- Rafiq, F., Awan, M. J., Yasin, A., Nobanee, H., Zain, A. M., & Bahaj, S. A. (2022). Privacy prevention of big data applications: A systematic literature review. *SAGE Open*, 12(2), 1–23. <https://doi.org/10.1177/21582440221096445>
- Rozani, M. A. S., Ahmad Fuad, A. H. F., & Abd Aziz, M. H. (2026). Penyelesaian cabaran privasi dan keselamatan data dalam era digital: Analisis tematik terhadap hadis Sahih Muslim [Solutions to privacy challenges and data security in the digital era: A thematic analysis of hadiths from Sahih Muslim]. *HADIS*, 16(1), 1–15. <https://doi.org/10.53840/hadis.v16i1.344>
- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339. <https://doi.org/10.1016/j.ibusres.2019.07.039>
- Supardi, M., Hanif, H., Rahman, M., Arham, A. F., & Amiruddin, A. M. A. (2026). Artificial intelligence ethics through the lens of Maqāsid al-Sharī'ah: Constructing a normative framework for civilized technology governance. *West Science Islamic Studies*, 4(3), 282–296. <https://doi.org/10.58812/wsiss.v4i03.3023>
- Wan Zakaria, W. M. F. A., & Zeki, A. M. (2026). Big data privacy and ethical concerns: Islamic perspective. *International Journal on Islamic Applications in Computer Science and Technology*, 14(2).
- Wicaksana, K. P., Alfath, T. P., & Kuswanto, H. (2026). Personal data protection in the digital era: A Maqasid al-Shariah perspective on contemporary legal challenges. *MIZAN: Journal of Islamic Law*, 10(1), 114–122. <https://doi.org/10.32832/mizan.v14i1.24363>