DOI: https://doi.org/10.62017/wanargi

# Islamic Legal Approach to Privacy and Cybersecurity in the Digital Age: Implications for the Sharia-Compliant Digital Economy

**Febrian Maulana Putra** *[1]
**Syamsul Hilal** [2]
**Hanif** [3]

[1,2,3,] Sharia Economics Master's Study Program, Raden Intan State Islamic University, Lampung, Indonesia
*e-mail: febrianmaulanaputra@gmail.com

***Abstract***

*This study reveals that Islamic law has a robust foundation to address privacy and cybersecurity issues in the digital age. The principles of the Quran and Hadith, reinforced by the maqasid al-shariah approach, provide a comprehensive ethical framework for protecting digital information. An analysis of Islamic legal sources shows that while the Quran and Hadith do not explicitly discuss modern technology, fundamental principles can be applied in the digital context. Contemporary fatwas from various fatwa councils in the Islamic world demonstrate a consensus that protecting digital privacy and security is a Sharia obligation. However, this research also identifies a gap between theory and practice, and a need for further ijtihad to address new technologies. An analysis of cybersecurity practices in Islamic institutions reveals a disconnect between Sharia principles and actual implementation. This study recommends enhancing collaboration between scholars and technology experts, developing practical guidelines for the application of Sharia in cybersecurity, increasing digital literacy among religious leaders, and integrating Sharia-based digital ethics into Islamic education. Additionally, there is a need to promote the development of global standards related to privacy and cybersecurity from an Islamic perspective, and further research on the application of Islamic concepts in security technology.*

***Keywords***: *privacy; cybersecurity; digital technology*

## INTRODUCTION

The rapid development of digital technology and the internet in recent decades has brought about fundamental changes in how people interact, communicate, and conduct daily activities. Data shows that in 2023, global internet users reached 5.16 billion people, or about 64.4% of the world's population. This growth is also occurring in Muslim-majority countries, with internet penetration in the Middle East reaching 76.4% in 2022 (Adhiarso et al., 2019). As the use of digital technology expands, issues of privacy and cybersecurity have become increasingly crucial. Recent reports reveal that global cyberattacks increased by 38% in 2022 compared to the previous year, with an average of 1,168 cyberattacks per organization per week (Anderson, 2022). This phenomenon poses new challenges for Muslim communities in balancing the utilization of technology with Sharia principles.

Islamic law, as a comprehensive system of rules, needs to provide clear guidance regarding privacy and cybersecurity in the digital age. While the Quran and Hadith do not explicitly discuss modern technology, fundamental principles such as the protection of privacy (Q.S. An-Nur: 27-28) and the prohibition of stealing information (Q.S. Al-Hujurat: 12) can serve as a basis for addressing contemporary challenges. Islamic scholars and intellectuals have sought to interpret Islamic legal sources in the context of digital technology. For example, the Majlis Ugama Islam Singapura (MUIS) in 2021 issued ethical guidelines for social media use based on Islamic principles (MUIS, 2021). Meanwhile, Dar al-Ifta al-Misriyyah in Egypt has also issued several fatwas related to online privacy and security (Putra, 2023).

However, these efforts remain partial and do not provide a comprehensive framework for an Islamic legal approach to privacy and cybersecurity. A study conducted by (Nazmi et al., 2020) shows that there is still a gap between Sharia principles and information security practices in Islamic financial institutions. Additionally, research by (Saidah & Maylaffayza, 2024) highlights the need for further development of the concept of maqasid al-shariah (the objectives of Sharia) in the context of personal data protection. The complexity of this issue is further compounded by

DOI: https://doi.org/10.62017/wanargi

the emergence of new technologies such as artificial intelligence, blockchain, and the Internet of Things, which bring ethical and legal implications not yet fully addressed within the traditional Islamic legal framework (Dwivedi et al., 2021).

Therefore, a comprehensive study is needed to analyze and formulate an Islamic legal approach to privacy and cybersecurity in the digital technology era. This research aims to explore contemporary interpretations of Islamic legal sources, examine fatwas and guidelines issued by religious authorities in various Muslim-majority countries, and analyze how the principles of maqasid al-shariah can be applied in the context of cybersecurity. The results of this research are expected to provide significant contributions to the development of an Islamic legal and ethical framework that is responsive to the challenges of the digital age and bridge the gap between classical Islamic legal tradition and the realities of modern technology.

## METHOD

This study adopts a qualitative approach using a literature review method to explore Islamic legal approaches to privacy and cybersecurity in the digital technology era. The literature review was chosen as the primary method due to its ability to analyze various relevant sources comprehensively and in-depth. The data collection process will focus on primary and secondary sources, including classical fiqh books, Quranic exegesis, Hadith collections, contemporary academic journals, textbooks, recent fatwas by scholars, research reports, and policy documents from international Islamic organizations. The first stage of the research involves identifying and collecting relevant literature using various electronic databases such as Google Scholar, JSTOR, ProQuest, and specialized Islamic studies databases like Al-Manhal and Dar al-Mandumah. The search will use a combination of keywords in Arabic and English, including "Islamic law," "privacy," "cybersecurity," "digital technology," "maqasid al-shariah," and "contemporary fiqh." Additionally, the snowballing method will be used to identify additional sources from the reference lists of the collected literature.

After data collection, the analysis process will be conducted using content analysis and hermeneutics. Content analysis will help identify the main themes, key concepts, and argument patterns in the reviewed literature. Meanwhile, the hermeneutic approach will be used to interpret classical texts in a contemporary context, considering historical, linguistic, and socio-cultural aspects. Specifically, for the analysis of primary Islamic legal sources, the usul al-fiqh (Islamic legal methodology) will be applied to understand the ijtihad and istinbath processes relevant to privacy and cybersecurity issues.

Several strategies will be implemented to ensure the validity and reliability of the research. First, data source triangulation will be performed by comparing information from various types of literature (e.g., comparing views in classical fiqh books with contemporary journals). Second, peer debriefing will be conducted by involving experts in Islamic law and cybersecurity to provide feedback on the research findings and interpretations. Third, an audit trail will be used to document the data collection and analysis process in detail, allowing other researchers to evaluate the validity of the findings.

Data analysis will be carried out iteratively, involving several stages: 1) Comprehensive reading of all collected literature sources, 2) Thematic coding to identify key concepts and main themes, 3) Comparative analysis to compare various views and interpretations, 4) Synthesis to integrate findings into a coherent theoretical framework, and 5) Drawing conclusions and formulating theoretical and practical implications.

## RESULT AND DISCUSSION

The results of this study reveal several key findings related to the Islamic legal approach to privacy and cybersecurity in the digital technology era. An analysis of primary Islamic legal sources shows that while the Quran and Hadith do not explicitly discuss modern technology, there are fundamental principles that can be applied in the digital context. Verses such as Q.S. An-Nur: 27-28, about respecting household privacy, and Q.S. Al-Hujurat: 12, about prohibiting spying, provide a strong ethical foundation for privacy protection in cyberspace (Insani et al., 2024).

DOI: https://doi.org/10.62017/wanargi

Contemporary interpretations of these verses expand their meaning to include the protection of personal data and digital communication (Katili, 2019).

This research finds that the maqasid al-shariah (objectives of Sharia) approach offers a flexible and comprehensive framework for formulating Islamic law related to privacy and cybersecurity. The concept of protecting the five basic elements in maqasid al-shariah (religion, life, intellect, lineage, and property) can be extended to include the protection of digital identity, data integrity, and information infrastructure security (Zaprulkhan, 2018). For instance, the protection of intellect (hifdz al-'aql) can be interpreted as an obligation to protect individuals from information manipulation and cyber-attacks that can impair critical thinking abilities (Yuliana, 2022).

An analysis of contemporary fatwas from various fatwa councils in the Islamic world shows a general consensus that protecting digital privacy and security is a Sharia obligation. For example, asserts that hacking and stealing personal data are forms of theft prohibited in Islam (Subuki et al., 2023). Meanwhile, the Indonesian Ulema Council (MUI) in its fatwa No. 24 of 2017 states that the dissemination of personal information without permission on social media is haram. These findings indicate that Islamic religious authorities have begun to actively respond to the challenges of the digital era (Shuhufi et al., 2022).

This study identifies several areas where Sharia principles can uniquely contribute to the development of cybersecurity policies and practices. One such area is the concept of amanah (trust), which can be applied in personal data management. A study by (Maulina et al., 2023) shows that implementing the principle of amanah in information system design can enhance user trust and compliance with security protocols. Additionally, the principle of maslahah (public interest) can be used as a guide in balancing national security needs with individual privacy rights in the context of digital surveillance (Asmawi et al., 2020).

However, this study also reveals several challenges in applying Islamic law to contemporary technological issues. One of the main challenges is the knowledge gap between traditional scholars and the latest technological developments. Many fatwas related to digital technology are still reactive and do not adequately consider the technical complexities of the technologies discussed. This indicates the need for closer collaboration between Sharia experts and information technology experts in formulating relevant and applicable Islamic law (Bunt, 2023).

Furthermore, an analysis of cybersecurity practices in Islamic institutions shows a gap between Sharia principles and actual implementation. Research conducted by (Muhfiatun et al., 2024) on Islamic financial institutions in Malaysia found that while there is awareness of the importance of information security from a Sharia perspective, many institutions lack a systematic framework to integrate Islamic principles into their cybersecurity practices. This finding highlights the need for developing standards and practical guidelines that translate Sharia principles into concrete cybersecurity protocols.

In the global context, this study also explores the potential contribution of Islamic law to the international discourse on internet governance and cybersecurity. An analysis of policy documents from the Organization of Islamic Cooperation (OIC) shows efforts to formulate a common position of Muslim countries in global forums related to cybersecurity. However, the implementation of this position is still limited, indicating the need for enhanced capacity and coordination among Muslim countries on global technological issues.

One interesting finding from this study is the potential of the concept of 'urf (accepted custom) in Islamic law to accommodate the development of digital norms. For example, user privacy expectations on social media platforms can be considered a form of contemporary 'urf that needs to be considered in formulating Islamic law related to digital privacy (Sule & Mainiyo, 2023). This approach opens the way for more flexible adaptation of Islamic law to the ever-changing realities of technology.

This study also identifies several areas that require further ijtihad (legal reasoning), including the Sharia status of cryptocurrency, the ethical and legal implications of artificial intelligence technology, and the Sharia limits on the use of surveillance technology by

governments. These findings indicate that the discourse on Islamic law regarding digital technology is still developing and requires ongoing interdisciplinary research.

Overall, the results of this study indicate that Islamic law has great potential to provide comprehensive ethical and legal guidance in addressing privacy and cybersecurity challenges in the digital age. However, realizing this potential requires systematic efforts to bridge the gap between classical Islamic legal tradition and contemporary technological realities, as well as closer collaboration between Sharia experts, technology experts, and policymakers.

## CONCLUSION

This research reveals that Islamic law has a strong foundation to address issues of privacy and cybersecurity in the digital age. The principles of the Quran and Hadith, reinforced by the maqasid al-shariah approach, provide a comprehensive ethical framework for protecting digital information. Contemporary fatwas have begun to respond to technological challenges, affirming digital privacy protection as a Sharia obligation. However, there is still a gap between theory and practice, as well as the need for further ijtihad to address new technologies. Based on these findings, it is recommended to enhance collaboration between scholars and technology experts, develop practical guidelines for the application of Sharia in cybersecurity, improve digital literacy among religious leaders, and integrate Sharia-based digital ethics into Islamic education. Additionally, there should be a push for the development of global standards related to privacy and cybersecurity from an Islamic perspective, as well as further research on the application of Islamic concepts in security technology. Implementing these recommendations is expected to strengthen the relevance of Islamic law in facing digital challenges and contribute to the development of a safer and more ethical global digital ecosystem.

## DAFTAR PUSTAKA

Adhiarso, D. S., Utari, P., & Hastjarjo, S. (2019). The Impact of Digital Technology to Change People's Behavior in Using the Media. *Digital Press Social Sciences and Humanities*, *2*(2018), 00005. https://doi.org/10.29037/digitalpress.42256

Anderson, J. L. (2022). *Global cyberattacks increased 38% in 2022*. https://www.securitymagazine.com/articles/98810-global-cyberattacks-increased-38-in-2022

Asmawi, ., Arsadani, Q., & Hanna, S. (2020). *Theory of Maslahah (Public Interest) and Its Relevance to Indonesian Corruption Eradication Law*. *Icri 2018*, 148–157. https://doi.org/10.5220/0009920101480157

Bunt, G. R. (2023). *Islam In The Digital Age: E-Jihad, Online Fatwas and Cyber Islamic Environments (Critical Studies on Islam)*. 244.

Dwivedi, Y. K., Ismagilova, E., Hughes, D. L., Carlson, J., Filieri, R., Jacobson, J., Jain, V., Karjaluoto, H., Kefi, H., Krishen, A. S., Kumar, V., Rahman, M. M., Raman, R., Rauschnabel, P. A., Rowley, J., Salo, J., Tran, G. A., & Wang, Y. (2021). Setting the future of digital and social media marketing research: Perspectives and research propositions. *International Journal of Information Management*, *59*(June 2020), 102168. https://doi.org/10.1016/j.ijinfomgt.2020.102168

Insani, N., Sarim Karimullah, S., & Gönan, Y. (2024). Islamic Law and Local Wisdom: Exploring Legal Scientific Potential in Integrating Local Cultural Values. *Jurnal Ilmu Hukum*, *26*(1), 101–124. https://doi.org/10.24815/kanun.v00i0.00000

Katili, M. G. (2019). The Importance Of Protecting The Personal Data Of Social Media Users In The Era Of Digitalization. *Estudiante Law Journal*, *1*(2), 437–447. https://doi.org/10.33756/eslaj.v1i2.13078

Maulina, R., Dhewanto, W., & Faturohman, T. (2023). The integration of Islamic social and commercial finance (IISCF): Systematic literature review, bibliometric analysis, conceptual framework, and future research opportunities. *Heliyon*, *9*(11), e21612. https://doi.org/10.1016/j.heliyon.2023.e21612

Muhfiatun, Prasojo, P., Listiyorini, I., & Utami, R. D. (2024). Shariah Governance Practice on Indonesian Islamic Banks. *Journal of Business Management and Islamic Banking*, *3*(1), 1–14. https://doi.org/10.14421/jbmib.v3i1.2112

Nazmi, M., Siraj, M. A., Mighfari, E. R., & Firli, R. N. (2020). Shariah Governance in Islamic Financial Institutions in Indonesia and Malaysia: A Comparative Analysis. *Journal of Islamic Finance*, *9*(2), 146–154.

Putra, M. H. (2023). The Intersection of Law and Technology: Navigating the Legal Challenges in the Digital Age. *Proceedings of the 1st International Conference on Science and Islamic Studies*, *1*(3), 956–960. https://doi.org/10.52783/tjjpt.v44.i3.404

Saidah, M., & Maylaffayza, H. (2024). Data Privacy Protection in Islamic Communication Perspective. *KOMUNIKA: Jurnal Dakwah Dan Komunikasi*, *18*(1), 25–36. https://doi.org/10.24090/komunika.v18i1.7847

Shuhufi, M., Fatmawati, Qadaruddin, M., Basyir, J., Yunus, M. M., & Nur, N. M. (2022). Islamic Law and Social Media: Analyzing the Fatwa of Indonesian Ulama Council Regarding Interaction on Digital Platforms. *Samarah*, *6*(2), 823–843. https://doi.org/10.22373/sjhk.v6i2.15011

Subuki, M., Akmal, H., & Hudaa, S. (2023). Identity and Piety: Critical Discourse Analysis on Indonesian Ulema Council's Fatwa About the Law Using Non-Muslim Religious Attributes. *Ahkam: Jurnal Ilmu Syariah*, *23*(2), 423–448. https://doi.org/10.15408/ajis.v23i2.31280

Sule, M. M., & Mainiyo, A. S. (2023). Effectiveness of Social Media Platform S in Disseminating Qur ' Anic. *Jurnal Ilmu-Ilmu Sosial*, *5*(1), 47–64. https://doi.org/10.34005/spektra.v5i1.2668

Yuliana, Y. (2022). the Importance of Cybersecurity Awareness for Children. *Lampung Journal of International Law*, *4*(1), 41–48. https://doi.org/10.25041/lajil.v4i1.2526

Zaprulkhan, Z. (2018). Maqāṣid Al-Shariah in the Contemporary Islamic Legal Discourse: Perspective of Jasser Auda. *Walisongo: Jurnal Penelitian Sosial Keagamaan*, *26*(2), 445. https://doi.org/10.21580/ws.26.2.3231