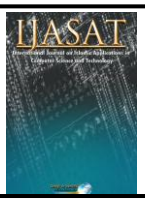

Cyber Laws and Islamic Perspectives on Digital Ethics

Jamilu Isah, Husam Qaser, Akram M Zeki
Kulliyyah of ICT, International Islamic University Malaysia,
akramzeki@iium.edu.my, i.jamilu@student.iium.edu.my, husamqaser11@gmail.com

Abstract
This paper examines the intersection between cyber laws and Islamic perspectives on digital ethics. It analyzes how global and regional legal frameworks address digital threats while incorporating Shariah-based principles such as privacy, harm prevention, and public interest. By reviewing cyber regulations in countries such as Malaysia and Indonesia, alongside Islamic jurisprudential responses to issues like cyber-sectarian conflict and online exploitation of women, the study identifies key areas of convergence and gaps. Core Islamic concepts—including maqasid al-shari'ah, ijtihad, and amanah—are applied to emerging technologies such as artificial intelligence and social media platforms. Case studies from Muslim-majority contexts illustrate practical implementations, while challenges such as enforcement limitations and cultural differences are also discussed. The findings support a balanced approach to digital governance that integrates Islamic ethical accountability with effective legal mechanisms to promote trust and justice in cyberspace.

Keywords: Cyber laws, Islamic digital ethics, Sharia compliance, data privacy, maslahah, cybercrime, ijtihad, digital trust.

1. Introduction

The rapid expansion of digital technologies has significantly transformed modern social, economic, and political systems, created new opportunities while also introducing complex ethical and legal challenges. Cybercrimes—including hacking, identity theft, misinformation, online extremism, and cyberbullying—pose serious threats to individual rights, national security, and social cohesion. Although governments have introduced cybercrime laws and data protection frameworks, these measures often struggle to keep pace with rapidly evolving digital risks, leading to persistent governance gaps. In Muslim-majority contexts, cyber regulations must align with Islamic ethical principles [1].

The Qur'an and Sunnah offer a comprehensive moral framework that addresses issues such as privacy, harm prevention, accountability, and justice. For example, the verse "Do not spy on one another" (Qur'an 49:12) highlights the sanctity of privacy, while the instruction to verify information before sharing it (Qur'an 49:6) directly relates to concerns about misinformation. Additionally, the Prophetic principle "There should be neither harming nor reciprocating harm" (*la darar wa la dirar*) reinforces the ethical responsibility that should guide digital behavior. Despite this rich ethical foundation, there remains limited scholarly work that systematically integrates Shariah principles with contemporary cyber law, particularly in relation to emerging technologies such as artificial intelligence, blockchain, and biometric surveillance.

Moreover, empirical research on digital ethics awareness among Muslim users remains limited, leaving policymakers without sufficient insights to design culturally grounded and ethically

aligned digital governance frameworks. Addressing these gaps is essential to ensure that legal systems not only regulate digital harms but also reflect the moral values of Muslim societies. Accordingly, this study examines global and regional cyber law frameworks and evaluates their compatibility with Shariah-based ethical concepts such as *aurah* (privacy), *maslahah* (public interest), and *'adl* (justice). It also considers public awareness and attitudes toward digital ethics within Muslim communities and proposes a hybrid governance model that integrates modern cyber regulations with Islamic jurisprudential reasoning (*ijtihad*). In doing so, the study contributes to the development of a more ethically grounded and legally coherent framework for digital governance in Muslim-majority contexts.

2. Related work

2.1 Cybercrime and Legal Implementation

The rapid expansion of cybercrime has prompted both national legal systems and Islamic scholars to reconsider the normative frameworks governing digital conduct. Existing studies examine how modern cyber offences resemble traditional crimes and how current legal regulations attempt to address these evolving challenges.

Another study examines the implementation of Indonesia's Electronic Information and Transaction Law (ITE Law) as it applies to cyberbullying [2]. Their analysis not only clarifies key legal provisions—such as Article 27(3) on defamation and harassment—but also highlights the limitations of the law in addressing issues such as anonymity and cross-border digital platforms.

Importantly, they evaluate these offences against Islamic principles of justice (*'adl*) and human dignity (*karāmah al- insān*), arguing that acts such as flaming, denigration, and outing violate Qur'anic prohibitions against harming others and infringing upon personal privacy (*aurah*). This demonstrates early attempts to align statutory measures with Sharia-based ethical norms, though the authors note gaps where jurisprudential guidance has not yet kept pace with digital harms.

Study [3] broadens this perspective by situating cybercrime within global regulatory challenges, tracing its evolution from the 1988 Morris Worm to the rise of ransomware networks. While their analysis is largely secular, their emphasis on user responsibility, ethical decision-making, and proactive security closely reflects Islamic ethical principles such as *amanah* (trustworthiness) in handling information. Their projected global economic impact of $10.5 trillion by 2025 also underscores the need for robust cross-border cooperation, a point relevant to Muslim- majority jurisdictions facing transnational threats.

A related study [4] pushes the discussion further by interrogating how Shariah responds to cyber-sectarian conflicts and hacktivism. He critiques the reluctance of some Muslim scholars to condemn offensive hacking supposedly conducted "in defense of Islam." By drawing parallels between cyberattacks and classical offences such as *hirabah* (banditry) and *ifsad* (sabotage), Maghaireh argues that punishments associated with property crimes could, in theory, be extended to digital contexts through *ijtihad*. His work highlights the flexibility of Islamic jurisprudence but also signals the need for greater scholarly engagement with cyber harms framed as moral, not merely technical, violations.

Collectively, these studies reveal that while national cyber laws provide structural enforcement mechanisms, Islamic ethics imbue the digital sphere with moral obligations grounded in *la*

darar wa la dirar (no harm, no reciprocal harm) and *maslahah* (public welfare). The enduring challenge is integrating these ethical principles within enforceable legal mechanisms that operate across borders.

2.2 Digital Ethics and Moral Responsibility

Digital ethics emerges as a central theme in the literature, with scholars emphasizing the importance of moral conduct online and the application of Islamic values to digital citizenship.

Another research [5] define digital ethics as a set of principles regulating online behavior—spanning information accuracy, privacy protection, ethical communication, and intellectual property rights. Their work frames ethical lapses such as hoaxes, hate speech, and cyberbullying as threats to social harmony. This aligns deeply with Islamic injunctions to verify information (Qur'an Surah Al-Hujurat 49:6), avoid unfounded accusations, and safeguard the dignity of individuals. By calling for digital civic education, the authors indirectly support the integration of Sharia-based ethics in school curricula, linking moral awareness with responsible digital citizenship.

Another study [6] adopts a more philosophical approach, advocating for the development of new interpretive frameworks that integrate Islamic metaphysics with contemporary theories of information and cognition..

Another study further develops this framework through a decolonial lens [4]. They critique Western-centric cybersecurity norms and instead argue for values such as *amanah*, *'adl*, and *niyyah* to shape digital trust and moral responsibility. Their argument that technology is never value- neutral strongly aligns with the Islamic worldview, which considers ethical agency inseparable from spiritual consciousness. This opens a pathway for a hybrid ethical model that complements legal compliance with moral accountability rooted in Shariah.

Taken together, these studies stress that ethical digital conduct cannot rely solely on legal restrictions. Rather, Islamic concepts like *amanah*, *tawhid*, *niyyah*, and *aurah* provide a rich moral foundation for addressing issues such as misinformation, privacy violations, and online extremism. This is directly aligned with the goal of your paper to articulate a Sharia-based ethical framework for contemporary digital challenges.

2.3 Balancing Privacy and Cybersecurity

A recurring theme in the literature is the tension between cybersecurity enforcement and the protection of individual privacy. This debate is especially pertinent to Islamic ethics, which elevate the sanctity of privacy (*hurmat al-aurah*) as a core moral and spiritual value.

Another research [7] examine data privacy regulations, cybersecurity governance, and AI ethics within global digital ecosystems. Their findings show that GDPR-like frameworks enhance transparency and public trust but remain difficult to implement in cross-jurisdictional digital markets. While their analysis is secular, their emphasis on human dignity and justice corresponds with the Islamic requirement that surveillance and data collection must align with principles of *maslahah* and avoid unjust harm (*darar*). This establishes a bridge between international human rights frameworks and Islamic normative requirements.

Another study foregrounds the inherent tensions between privacy protections and the necessity of cybersecurity surveillance [8]. He argues that technological systems often privilege efficiency over ethics, a critique that resonates with Islamic objections to value-neutral approaches to

technology. His advocacy for decolonial ethical frameworks suggests the need for culturally embedded interpretations of privacy—precisely where Islamic jurisprudence offers robust principles governing *aurah*, the limits of surveillance, and the ethical handling of personal data.

Together, these studies illustrate that protecting privacy in digital governance requires more than technical safeguards: it necessitates ethical principles that prevent harm, ensure fairness, and uphold the dignity of individuals. Islamic ethics can contribute substantively to such a balance through doctrines like *la darar*, the preservation of honor (*ird*), and the prioritization of *maslahah ammah* (public interest).

2.4 Islamic Responses to Cyber Challenges

Several authors explicitly address how Shariah-based frameworks can evolve to meet contemporary cyber challenges. In [4] argue for the extension of classical jurisprudence into the digital domain, including conceptual analogies between hacking and traditional crimes like theft and sabotage. Their arguments demonstrate that Islamic law contains adaptable principles, but requires structured *ijtihad* to determine appropriate legal- maqasid (objectives).

Another presentation [6] a more philosophical approach, calling for new interpretive models that integrate Islamic metaphysics with contemporary information theory. Meanwhile, [5] emphasize moral-legal synergy and digital citizenship education rooted in Islamic values. Together, these works illustrate that Shariah has both conceptual flexibility and normative depth to respond to modern cyber threats. However, they also reveal gaps— including scholars' reluctance to address cyber-hacktivism, limited discussion on AI and blockchain ethics, and insufficient legal operationalization of Islamic principles.

Research Gaps. Despite the growing body of literature, several important gaps remain. First, there is a clear misalignment between existing cyber laws and Shariah-based ethics, as many legal studies focus primarily on national regulations without adequately evaluating their compatibility with Islamic principles such as *aurah*, *maslahah*, and *la darar wa la dirar*. Second, Islamic digital ethics in relation to emerging technologies remains underdeveloped; issues such as artificial intelligence, blockchain, biometric surveillance, and data brokerage receive limited attention in contemporary Islamic discourse. Third, empirical research on Muslim digital behavior is scarce, with few studies examining public awareness, attitudes, and ethical decision-making among Muslim users—an area directly addressed in this study. Finally, although scholars advocate for Islamic responses to cyber challenges, practical *ijtihad*-based policy development remains limited, with few concrete frameworks integrating Shariah principles into modern cyber laws. Addressing these gaps enables this study to propose a much-needed hybrid model for cyber governance that harmonizes global legal standards with Islamic ethical principles.

3. RESEARCH METHODOLOGY

3.1 Research Design

This study adopts qualitative, doctrinal, and conceptual research methodology. The study is normative in nature and does not involve empirical data collection, such as surveys or interviews. Instead, it relies on structured legal analysis and Islamic ethical reasoning to examine how cyber laws intersect with Shariah-based digital ethics.

Doctrinal research is appropriate for this study because its primary objective is to analyze legal norms, ethical principles, and jurisprudential frameworks, rather than to measure behavioral

outcomes or perceptions. This approach is commonly employed in legal, ethical, and Islamic studies research where normative evaluation and theoretical synthesis are required.

3.2 Data Sources

The study relies exclusively on secondary and authoritative sources, including the following:

1. **Cyber Law and Digital Governance Instruments**
   - National cybercrime legislation in Muslim-majority jurisdictions (e.g., Indonesia's ITE Law)
   - International cyber law and data protection frameworks (e.g., GDPR, Budapest Convention principles)
   - Peer-reviewed legal and cybersecurity literature

2. **Islamic Primary Sources**
   - The Qur'an
   - Authentic Hadith collections (e.g., Sahih Muslim, Sunan Ibn Majah)

3. **Islamic Jurisprudential Frameworks**
   - Maqasid al-shari'ah (objectives of Islamic law)
   - Classical fiqh maxims (qawāʿid fiqhiyyah), such as la darar wa la dirar
   - Contemporary Islamic ethical scholarship on technology and digital life

4. **Academic Literature**
   - Peer-reviewed journal articles on cyber law, digital ethics, Islamic ethics, and technology governance

3.3 Analytical Framework

The analysis is conducted using three complementary approaches:

1. **Doctrinal Legal Analysis**
   Cyber laws and regulatory instruments are examined to identify how digital harms such as cybercrime, privacy violations, misinformation, and surveillance are legally addressed.

2. **Maqasid-Based Ethical Mapping**
   Identified cyber issues are mapped against the objectives of Shariah—particularly the protection of:
   - religion (dīn),
   - life (nafs),
   - intellect ('aql),
   - lineage ('ird / nasl),
   - property (māl).

3. **Normative Ethical Synthesis (Ijtihad-Oriented Reasoning)**
   Islamic ethical principles such as *amanah* (trust), *'adl* (justice), *maslahah* (public interest), *aurah* (privacy), and *la darar wa la dirar* (no harm) are applied to modern digital contexts to identify governance gaps and ethical contributions beyond legal compliance.

Table 1: Cyber Threats and Maqasid al-Shari'ah Alignment

Cyber Issue	Legal Concern	Relevant Maqasid	Islamic Ethical Basis
Cyberbullying	Harassment & defamation	Protection of honor ('ird)	Prohibition of harm and backbiting
Data breaches	Privacy & data protection	Protection of property (māl) & dignity	Amanah (trust)
Misinformation	Public harm & instability	Protection of intellect ('aql)	Tabayyun (verification)
Surveillance abuse	Rights infringement	Protection of privacy (aurah)	La darar wa la dirar

3.4 Scope and Limitations

This study does not claim empirical generalizability and does not assess user behavior or public attitudes. Its findings are normative and conceptual, intended to inform policymakers, scholars, and researchers. While the focus is on Muslim-majority contexts, the ethical principles discussed have broader relevance to global digital ethics debates.

4. Discussion

The findings of this study indicate that, although contemporary cyber laws are increasingly comprehensive, they remain insufficient in addressing the ethical, moral, and spiritual dimensions of digital life. Modern cyber regulations primarily focus on procedural enforcement—criminalizing hacking, cyberbullying, fraud, data breaches, and misinformation, yet they often lack an underlying moral foundation. In contrast, Islamic ethics, grounded in the Qur'an, Sunnah, and the principles of Maqasid Al-shari'ah, provide deeper guidance that integrates legal compliance with moral responsibility. This study's analysis shows that combining these two frameworks—modern cyber governance and Shariah-based ethics—creates a more holistic approach to addressing digital challenges.

One of the central observations is the tension between cybersecurity enforcement and the sanctity of privacy. Many national laws legitimize forms of surveillance necessary for crime prevention, yet Islamic teachings place great emphasis on respecting privacy (aurah) and prohibiting unwarranted intrusion. The Qur'an explicitly states: "O you who have believed, avoid much [negative] assumption. Indeed, some assumptions are sin. And do not spy or backbite each other. Would one of you like to eat the flesh of his brother when dead? You would detest it. And fear Allāh; indeed, Allāh is Accepting of Repentance and Merciful." (Qur'an 49:12). This verse establishes privacy as both a moral and legal boundary. Similarly, the Prophet Muhammad (ﷺ) said: "A Muslim's blood, property, and honor are sacred." (Sahih Muslim). These teachings position privacy violations— whether through hacking, unauthorized data harvesting, or state surveillance—as ethical crimes beyond mere legal infractions. Therefore, cyber laws must balance the necessity of monitoring with the Islamic requirement to avoid unjust harm (*la darar wa la dirar*). The present study finds that existing legislation often fails to consider such moral limits, suggesting the need for a more Quranic-guided approach to privacy protection.

Digital harms such as cyberbullying, hate speech, misinformation, and digital harassment further illustrate gaps in the legal system that can be bridged through Islamic ethics. While the ITE Law provides criminal sanctions, Islamic teachings provide motivational deterrence rooted in accountability to God and the community. The Qur'an warns: "Believers, when an ungodly person brings to you a piece of news, carefully ascertain its truth, lest you should hurt a people

unwittingly and thereafter repent at what you did." (Qur'an 49:6), establishing the obligation to verify information before sharing it, an ethical requirement directly addressing the spread of "fake news," online slander, and hoaxes. Furthermore, the Prophet (PBUH) commanded: "There should be neither harming nor reciprocating harm." (Sunan Ibn Majah), a maxim that applies to all forms of cyber violence, including phishing, ransomware, and digital stalking. These ethical principles complement existing legal frameworks by fostering a culture of moral self-restraint, which legal enforcement alone cannot achieve.

A major discussion point emerging from the results is that Islamic digital ethics remain underdeveloped in areas such as AI governance, blockchain, algorithmic bias, predictive policing, biometric datasets, and data brokerage. Modern technologies increasingly automate decisions affecting livelihoods and rights, yet their implications remain underexplored in Islamic jurisprudence. The Qur'an emphasizes justice as a universal command: "Indeed Allah commands justice, excellence, and giving to relatives." (Qur'an Surah An-Nahl 16:90). This has direct relevance to algorithmic fairness, AI transparency, and data discrimination, suggesting that any digital system that unfairly harms individuals violates Islamic ethical norms. Moreover, emerging technologies challenge classical fiqh assumptions about agency, responsibility, and intention (niyyah), making ijtihad methodical reasoning essential for updating Islamic law. The present study finds that scholars acknowledge these gaps but rarely propose concrete policy frameworks that integrate Islamic values with cyber regulations.

The study highlights a general lack of digital ethics awareness among Muslim users, as reported in existing literature despite high levels of online engagement. Many respondents expressed concern over issues such as cyberbullying and privacy breaches but lacked understanding of how Islamic teachings relate to digital behavior. This finding aligns with the Qur'anic emphasis on knowledge and reflection: "Are those who know equal to those who do not know?" (Qur'an Surah Az-Zumar 39:9).

The gap between ethical ideals and actual digital behavior implies that Muslim communities require structured digital citizenship education. Such programs should integrate legal literacy (knowing rights and obligations under cyber laws) with Islamic moral teachings (such as Amanah (trust), tawhid "unity of purpose", and ihsan "ethical excellence"). This dual literacy strengthens both compliance and ethical motivation, shaping responsible digital conduct.

Finally, the discussion highlights the necessity of developing an integrated cyber governance framework rooted in maqasid al-shari'ah. The objectives of Shariah—preserving faith, life, intellect, lineage, and property—map naturally onto contemporary digital challenges. Protecting intellect aligns with combating misinformation; protecting property aligns with cybersecurity against hacking; protecting lineage aligns with regulating deepfakes and online exploitation; and protecting honor aligns with cyberbullying laws. By integrating these objectives with global cyber standards such as GDPR, Budapest Convention principles, and national cybercrime statutes, governments in Muslim-majority countries can craft policies that are both technologically relevant and morally grounded. This harmonized framework ensures that digital systems do not merely punish wrongdoing, but also cultivate digital environments that honor human dignity, prevent harm, and uphold justice.

Table 2: Cyber Law Enforcement vs Islamic Ethical Accountability

Dimension	Cyber Law	Islamic Ethics
Nature	Regulatory & punitive	Moral & spiritual
Motivation	Fear of sanctions	Accountability before Allah
Scope	Jurisdiction-bound	Universal
Orientation	Reactive	Preventive

5. Conclusion

This study examined the intersection of cyber laws and Islamic digital ethics to understand how modern regulatory frameworks can be strengthened through Shariah-based moral principles. The findings show that contemporary cyber laws, while increasingly sophisticated, remain largely reactive and focused on enforcement mechanisms against threats such as hacking, cyberbullying, identity theft, misinformation, surveillance abuse, and data breaches. However, these legal systems often lack the deeper ethical grounding needed to guide responsible digital behavior. In contrast, Islamic ethical principles—rooted in the Qur'an, Sunnah, and maqasid al-shari'ah—offer a more holistic foundation by integrating moral responsibility, accountability, justice, and the sanctity of human dignity into discussions of digital life. The Qur'anic emphasis on privacy (Qur'an 49:12), verification of information (Qur'an 49:6), and justice (Qur'an 16:90), as well as the Prophetic principle of la darar wa la dirar ("there should be neither harming nor reciprocating harm"), provide comprehensive guidance that complements and enriches modern legal provisions.

The literature indicates that while Muslim digital users express awareness of online risks, their understanding of Islamic digital ethics remains limited. This highlights an urgent need for enhanced digital citizenship programs that combine legal literacy with Islamic moral education. The study also found significant gaps in Islamic scholarly engagement with emerging technologies such as AI, blockchain, predictive analytics, and biometric surveillance. These gaps underscore the necessity of contemporary ijtihad to ensure that Shariah remains relevant and responsive in guiding Muslims through new technological realities.

Ultimately, the study concludes that effective cyber governance in Muslim-majority societies must move beyond mere legal compliance toward a hybrid model that integrates global cyber standards with Shariah-based ethics. By doing so, policymakers can better uphold human dignity, prevent harm, strengthen trust, and ensure justice in digital environments. This integrated approach is not only technologically necessary but also aligns with the Islamic vision of a morally grounded and socially responsible digital society.

These findings also have practical implications for policymakers, particularly in integrating ethical considerations into cyber governance frameworks.

REFERENCES

[1] K. Komaruddin et al, "Islamic Perspectives on Cybersecurity and Data Privacy: Legal and Ethical Implications," vol. 1 no 04 (2023), https://doi.org/10.58812/wslhr.v1i04.323.

[2] J. N. Inayah and T. Nugroho, "Criminal Implementation of Cyberbullying Based on Electronic Information and Transaction Law and Islamic Law," vol. 7, no. 1, pp. 252–268, 2024.

[3] A. Maghaireh, "Shariah Law and Cyber-Sectarian Conflict: How can Islamic Criminal Law respond to cyber crime ?," vol. 2, no. 2, pp. 337–345, 2008.

[4] J. Notariil et al., "Digital Ethics and Citizenship Challengers in Cyberspace: An Overview from Perspective Morals," vol. 9, no. 1, pp. 33–39, 2024. Doi: https://doi.org/10.22225/jn.9.1.2024.33-39.

[5] M. Y. Chaudhary, "Initial Considerations for Islamic Digital Ethics," Philos. Technol., vol. 33, no. 4, pp. 639–657, 2020, doi: 10.1007/s13347-020-00418-3.

[6] Arrozy & Zarman 2024, "Philosophical Underpinnings of Artificial Intelligence and the Concept of Human Soul in Islam: Some Issues at the Interface", vol. 17 no 1 (2024), https://doi.org/10.56389/tafhim.vol17no1.2.

[7] N. Allahrakha, "Balancing Cyber-security and Privacy: Legal and Ethical Considerations in the Digital Age," vol. 4, no. 2, pp. 78–121, 2023, doi: 10.17323/2713-2749.2023.2.78.121.

[8] E. Implications, "Cybersecurity and Moral Responsibility: A Philosophical-Islamic Approach to Digital Trus," vol. 1, no. 2, pp. 68–82, 2024. https://doi.org/10.70063/techcompinnovations.v2i1.93..