



Personal Data Hacking: A Critical Analysis of Islamic Criminal Law and Islamic Jurisprudence

Munifah^{1*}, Mufrod Teguh Mulyo²

^{1,2}Universitas Nahdlatul Ulama Surakarta, l. Dr. Wahidin No.5, Penumping, Kec. Laweyan, Kota Surakarta, Jawa Tengah 57141

*(Corresponding author) e-mail munifah@unu.ac.id

Abstract

This research will examine the rise of social media hacking behaviour from the perspective of Islamic Criminal Law and Islamic Law. The issues discussed in this study include how Islam addresses the laws related to individuals who commit crimes against the right to privacy and personal data, as well as the urgency of personal data protection in social media within the context of Islamic law and the Muslim response to the digital era. This research employs a descriptive-qualitative methodology with in-depth data analysis, incorporating juridical and Islamic criminal law approaches. Primary data is derived from cases and behavioural data pertaining to personal data. Secondary data encompasses primary, secondary, and tertiary legal materials. Primary legal materials include binding legal sources such as legislation, legislative records, and court decisions. The findings of this study indicate that Islam underscores the importance of maintaining the dignity and privacy of individuals through the principles of honour protection (*Hifz al-'Irqi*). Every Muslim is obligated to uphold the security of personal data and to advocate for the implementation of laws that protect individual rights from cyber threats. In order to enhance the security of personal data, it is recommended that Islamic principles be integrated into current laws, ensuring they are based on both positive law and maqashid sharia. Furthermore, improving digital literacy in accordance with Islamic teachings serves as a strategic initiative to raise public awareness of the significance of protecting privacy in the digital age. This study concludes that violations of personal data in the digital realm, such as identity theft and unauthorised information dissemination, can be classified under punishment (*ta'zir*) within Islamic criminal law due to the absence of explicit provisions in *hudud* and *qisas*. It highlights the urgency of protecting personal data in social media and advocates for the application of Islamic legal principles, such as *hifz al-'ird* as a foundation for safeguarding individual privacy in the digital era.

Keywords: Hacking; *Hifz al-'Irqi*; Islamic Law; Personal Data.

Abtrak

Penelitian ini akan mengkaji prevalensi perilaku peretasan media sosial dalam perspektif Hukum Pidana Islam dan Hukum Islam. Permasalahan yang dibahas dalam penelitian ini mencakup bagaimana Islam menyikapi hukum terkait individu yang melakukan kejahatan terhadap hak privasi dan data pribadi, serta urgensi perlindungan data pribadi di media sosial dalam konteks hukum Islam dan respons umat Islam terhadap era digital. Penelitian ini menggunakan metodologi deskriptif-kualitatif dengan analisis data yang mendalam, menerapkan pendekatan yuridis dan hukum pidana Islam. Data primer diperoleh dari kasus-kasus dan data perilaku yang berkaitan dengan data pribadi. Data sekunder meliputi bahan hukum primer, sekunder, dan tersier. Bahan hukum primer mencakup sumber hukum yang mengikat seperti undang-undang, catatan legislatif, dan putusan pengadilan. Temuan dari penelitian ini menunjukkan bahwa Islam menggarisbawahi pentingnya menjaga martabat dan privasi individu melalui prinsip-prinsip perlindungan kehormatan (*Hifz al-'Irqi*). Setiap Muslim berkewajiban untuk menjunjung tinggi keselamatan data pribadi dan mengadvokasi penerapan hukum yang melindungi hak-hak individu daripada ancaman siber. Untuk meningkatkan keselamatan data pribadi, disarankan agar prinsip-prinsip Islam diintegrasikan ke dalam undang-undang yang berlaku pada masa kini, dengan memastikan bahwa undang-undang tersebut berlandaskan hukum positif dan maqashid syariah. Selain itu, meningkatkan literasi digital sesuai dengan ajaran Islam merupakan inisiatif strategis untuk meningkatkan kesadaran masyarakat akan kepentingan melindungi privasi di era digital. Penelitian ini menyimpulkan bahwa pelanggaran data pribadi di ranah digital, seperti pencurian identitas dan penyebaran maklumat tanpa izin, dapat diklasifikasikan sebagai tindak pidana (*ta'zir*) dalam hukum pidana Islam kerana ketiadaan ketentuan eksplisit dalam hukum *hudud* dan *qisas*. Hal ini menyoroti urgensi perlindungan data pribadi di media sosial dan mengadvokasi penerapan prinsip-prinsip hukum Islam, seperti *hifz al-'ird* sebagai asas untuk melindungi privasi individu di era digital.

Kata Kunci: Data Pribadi; *Hifz al-'Irqi*; Hukum Islam; Peretasan.



Introduction

The development of information and communication technology has engendered significant changes in individuals' social and economic lives. However, beneath the convenience afforded by these advancements lies a serious threat to individual privacy, particularly through the practice of personal data hacking.¹ Such hacking not only inflicts financial harm upon victims but also constitutes a violation of the human right to privacy.² In the context of a modern society increasingly reliant on technology, threats to personal data have emerged as a global issue that necessitates serious attention.³ This phenomenon underscores the imperative for robust regulations and an ethical approach to the management of digital information.

Various instances of personal data hacking in Indonesia illustrate the escalation of this threat across multiple sectors. Data from the Ministry of Communication and Information, as cited by the Legal Documentation and Information Network of the General Secretariat of the DPR RI,⁴ indicates that from 2019 to May 14, 2024, there were 111 cases of data leakage that were officially addressed. Furthermore, a report by Surfshark, a Dutch VPN company, ranks Indonesia among the ten countries with the highest incidence of data leaks from January 2020 to January 2024.⁵ These facts reveal that threats to personal data security are becoming increasingly widespread and complex.⁶ Not only individuals but also the education and agrarian sectors have emerged as targets of hacking, as demonstrated in the research conducted by Suhendi and Asmadi.⁷

Several prior studies have investigated the issue of personal data protection from the perspectives of positive law and technology. Dhaval Chudasama and Raj Singh Deora⁸ have highlighted forms of cybercrime such as phishing, online fraud, and identity theft, emphasising the importance of enhancing cybersecurity awareness. The study conducted by Al Sentot Sudarwanto and Dona Budi Budi Kharisma⁹ illustrates that Indonesia still lags behind Hong Kong and Malaysia regarding personal data protection regulations. Setiawati¹⁰

¹ Edi Saputra Hasibuan and Elfirda Ade Putri, "Perlindungan Keamanan Atas Data Pribadi Di Dunia Maya," *Jurnal Hukum Sasana* 10, no. 1 (June 8, 2024): 70–83, <https://doi.org/10.31599/sasana.v10i1.2134>.

² Marta F Arroyabe et al., "Revealing the Realities of Cybercrime in Small and Medium Enterprises: Understanding Fear and Taxonomic Perspectives," *Computers and Security*, March 2024.

³ Theodorus Sendjaja et al., "Cybersecurity In The Digital Age: Developing Robust Strategies To Protect Against Evolving Global Digital Threats And Cyber Attacks," *International Journal of Science and Society* 6, no. 1 (March 1, 2024): 1008–19, <https://doi.org/10.54783/ijssoc.v6i1.1098>.

⁴ DPR RI, "Kebocoran Data Kembali Terjadi, Sukamta: Ini Alarm Keras Buat Pemerintah!," 2024, [ps://jdih.dpr.go.id/berita/detail/id/51640/t/Kebocoran+Data+Kembali+Terjadi%2C+Sukamta%3A+Ini+Alarm+Keras+Buat+Pemerintah%21](https://jdih.dpr.go.id/berita/detail/id/51640/t/Kebocoran+Data+Kembali+Terjadi%2C+Sukamta%3A+Ini+Alarm+Keras+Buat+Pemerintah%21).

⁵ Adi Ahdiat, "Indonesia Is among the Top 10 Countries with the Most Data Leaks," *Databoks*, 2024, [https://www.deepl.com/en/translator#id/en-us/Indonesia Masuk 10 Negara dengan Kebocoran Data Terbesar](https://www.deepl.com/en/translator#id/en-us/Indonesia%20Masuk%2010%20Negara%20dengan%20Kebocoran%20Data%20Terbesar).

⁶ Dadang Suhendi and Erwin Asmadi, "Cyber Laws Related to Prevention of Theft of Information Related to Acquisition of Land and Infrastructure Resources in Indonesia," *International Journal of Cyber Criminology* 15, no. 2 (July 13, 2021): 135–43, <https://doi.org/10.5281/zenodo.4766552>.

⁷ Dadang Suhendi and Erwin Asmadi.

⁸ Dhaval Chudasama and Raj Singh Deora, "Brief Study of Cybercrime on an Internet." *Journal of Communication Engineering & Systems*, *Journal of Communication Engineering & Systems* 21, no. 1 (2021): 22–27.

⁹ Al Sentot Sudarwanto and Dona Budi Budi Kharisma, "Comparative Study of Personal Data Protection Regulations in Indonesia, Hong Kong and Malaysia," *Journal of Financial Crime* 29, no. 4 (September 30, 2022): 1443–57, <https://doi.org/10.1108/JFC-09-2021-0193>.

¹⁰ Diana Setiawati, Hary Abdul Hakim, and Fahmi Adam Hasby Yoga, "Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore," *Indonesian Comparative Law Review* 2, no. 2 (August 7, 2020), <https://doi.org/10.18196/iclr.2219>.

emphasises that strong data protection is essential to support digital innovation amidst the Industrial Revolution 4.0. Meanwhile, Dizon¹¹ advocates for a norm- and value-based approach in the development of technology law to render it more adaptive to societal developments. Suhendi and Asmadi¹² demonstrate how inadequate agricultural data protection creates loopholes for organised crime practices in Indonesia.

Although these studies have made significant contributions, there remains a gap in the examination of personal data protection from the perspective of Islamic law. The majority of existing research tends to favour positive law and technological approaches without delving into the values of maqashid sharia, which prioritise the protection of honour (*Hifz al-'Irḍi*) and life (*Hifz al-Nafs*).¹³ Within the framework of Islamic law, the violation of privacy constitutes a breach of the fundamental principles of a dignified social existence.¹⁴ Consequently, an Islamic normative approach is essential for understanding hacking crimes as both moral and legal transgressions. This article aims to address this gap by investigating the issue through the lens of Islamic law and Islamic criminal law.

This study seeks to analyse the urgency of personal data protection in the digital age from the perspective of Islamic law and Islamic criminal law. Such an inquiry is vital for enriching the discourse surrounding Islamic law by presenting a novel approach grounded in the values of justice, morality, and the protection of individual rights. Furthermore, this study aspires to provide alternative normative solutions to the challenges of personal data protection within Muslim societies. The integration of maqashid sharia principles with the evolution of contemporary digital law is crucial for establishing a more holistic concept of privacy. Therefore, this research is anticipated to contribute to the development of Islamic law that is responsive to the dynamics of contemporary society.

Method

This study employed a qualitative research methodology utilizing a normative juridical approach, with a particular emphasis on Islamic criminal law and positive criminal law. It is classified as a literature-based (library) study. The data sources consisted of both primary and secondary data. Primary data were derived from documented cases and behavioural patterns associated with personal data violations. Secondary data encompassed legal materials, which included (a) primary legal sources such as legislation, court decisions, and official legislative records; (b) secondary legal sources comprising journal articles, theses, and scholarly books; and (c) tertiary sources, including legal encyclopaedias and dictionaries. Data analysis was conducted through three stages: data reduction, data display, and conclusion drawing, thereby ensuring methodological rigor and alignment with the principles of Islamic legal reasoning (maqashid sharia), particularly protection of dignity (*hifz al-'irḍi*).

¹¹ Michael Anthony C. Dizon, "Socio-Legal Study of Technology: A Norms and Values Approach to Hacking and Encryption Law and Policy," *Computer Law & Security Review* 52 (April 2024): 105958, <https://doi.org/10.1016/j.clsr.2024.105958>.

¹² Dadang Suhendi and Erwin Asmadi, "Cyber Laws Related to Prevention of Theft of Information Related to Acquisition of Land and Infrastructure Resources in Indonesia," *International Journal of Cyber Criminology* 15, no. 2 (July 13, 2021): 135–43, <https://doi.org/10.5281/zenodo.4766552>.

¹³ Saibatul Hamdi and Khabib Musthofa, "Menghadirkan Konsep Hifz Al-Irḍi Dalam Bermedia Sosial: Upaya Menyikapi Asusila Abu-Abu Di Youtube," *El Madani : Jurnal Dakwah Dan Komunikasi Islam* 1, no. 02 (January 5, 2021): 141–62, <https://doi.org/10.53678/elmadani.v1i02.129>.

¹⁴ Yusrizal et al., "Defamation and Insult Via Digital Media in Indonesia: The Islamic Law and Human Rights Perspective," *Journal of Law and Sustainable Development* 11, no. 7 (September 25, 2023): e1016, <https://doi.org/10.55908/sdgs.v11i7.1016>.

Protection of personal data

The security of personal data remains a significant issue, leading to ongoing public concerns. The rapid and increasingly complex development of information technology aligns with individuals' constant pursuit of innovation and updates to existing systems.¹⁵ This phenomenon reflects contemporary demands, as nearly every activity in the digital era relies on personal data. The utilisation of personal data necessitates good governance, transparency, and accountability, alongside robust support for the rule of law. However, negligence in personal data protection has precipitated various serious incidents, resulting in recurring challenges.¹⁶ This situation highlights weaknesses in data governance, limited access to recovery for data subjects, and significant obstacles in achieving comprehensive and effective data protection regulations.

In this context, the state bears an obligation to protect its citizens in various domains, including social, economic, legal, and political spheres. This protection encompasses all aspects inherent to individuals, including personal data.¹⁷ With over 221 million internet users in Indonesia, constituting 79.5% of the total population, personal data holds considerable economic, political, and commodity value. Thus, specific regulations are required to govern the protection of personal data. Firman Muhammad Arif asserts that, under these circumstances, the state must take concrete actions, both through the implementation of regulations that serve as a legal framework and through effective law enforcement, with the aim of fostering a competitive, progressive environment that educates the public.¹⁸

Regulations pertaining to personal data protection are enshrined in Law of the Republic of Indonesia Number 27 of 2022, which delineates individual rights to self-protection, family, honour, dignity, and property ownership. This law recognises the protection of personal data as a right of every Indonesian citizen, for which the state is responsible. Such protections are also classified as part of human rights, particularly concerning efforts to maintain individual privacy. A robust legal foundation is essential to ensure the security of personal data in accordance with Law of the Republic of Indonesia Number 27 of 2022. In this framework, a legal umbrella exists that guarantees citizens the right to self-protection, promotes heightened public awareness, and ensures recognition and respect for the importance of maintaining the confidentiality of personal data.¹⁹ Consequently, the pertinent question arises: to what extent does the implementation of the Personal Data Protection Law impact the protection of individual information, and can this law effectively reduce the frequency of user data breaches on social networking platforms?

Social media has become an integral component of digital life, serving as the primary platform for communication, entertainment, and economic transactions. However, despite

¹⁵ Bader Alojaiman, "Technological Modernizations in the Industry 5.0 Era: A Descriptive Analysis and Future Research Directions," *Processes* 11, no. 5 (April 24, 2023): 1318, <https://doi.org/10.3390/pr11051318>.

¹⁶ Hizbul Khootimah Azzaakiyyah, "The Impact of Social Media Use on Social Interaction in Contemporary Society," *Technology and Society Perspectives (TACIT)* 1, no. 1 (August 31, 2023): 1–9, <https://doi.org/10.61100/tacit.v1i1.33>.

¹⁷ Michèle Finck and Frank Pallas, "They Who Must Not Be Identified —Distinguishing Personal from Non-Personal Data under the GDPR," *International Data Privacy Law* 10, no. 1 (February 1, 2020): 11–36, <https://doi.org/10.1093/idpl/ipz026>.

¹⁸ Firman Muhammad Arif, "Mitigasi Resiko Investasi Bodong Dan Aktualisasi Nalar Istislah," *Al-Manahij: Jurnal Kajian Hukum Islam* 14, no. 1 (June 2, 2020): 19–34, <https://doi.org/10.24090/mnh.v14i1.3580>.

¹⁹ Muh Rifqy Hidayatullah Arham and M. Chaerul Risal, "Perlindungan Data Pribadi Bagi Pengguna Media Sosial," *Jurnal Al Tasyri'iyah* 3, no. 2 (December 11, 2023): 109–19.

facilitating easy access and interaction, social media also significantly impacts the exploitation of users' personal data. The We Are Social (2024) report indicates that more than 60% of personal data leakage incidents originate from activities on social media. Personal information collected through interactions on these platforms, such as consumption preferences, geographic location, and daily habits, may be processed and traded without adequate control from individuals. This issue raises substantial questions regarding privacy rights in an increasingly ambiguous digital landscape.

The Cambridge Analytica scandal, which emerged in 2018, serves as a pertinent example of how user data can be misappropriated without consent. Facebook user data was utilised to manipulate political opinion, resulting in significant global political shifts. In Indonesia, a report by the State Cyber and Cryptography Agency (BSSN) in 2023 revealed a 34% increase in doxxing cases compared to the previous year, with most cases arising from the theft of personal data on social media. This practice exemplifies a growing digital injustice, wherein individuals, as data owners, lose control over their data, which is leveraged by third parties in a non-transparent manner.

The phenomenon of data commodification, wherein individual data is treated as a tradable commodity without explicit consent, has become particularly pronounced in today's digital landscape. Social media platforms systematically collect user data through algorithms that not only store information but also utilise it to craft digital experiences that drive specific consumer behaviour.²⁰ This dynamic fosters a growing power imbalance between the technology companies that control the data and the users who lack full control over their information. This condition underscores the necessity for a fairer approach to personal data management, facilitated by stringent regulations and enhanced digital awareness among the public.

The theoretical framework of Surveillance Capitalism, posited by Shoshana Zuboff (2019), provides critical insights into understanding digital economy models that depend on the collection and exploitation of personal data. According to Zuboff, social media not only offers free services but also actively shapes user behaviour for economic gain.²¹ In this context, digital platforms rely on algorithmic systems that collect data to predict and manipulate user behaviour, engendering a dependence on an opaque digital ecosystem.²² This concept is particularly relevant in the realm of social media, where many users remain unaware of how their data is tracked and utilised, as well as the potential dangers associated with this ignorance.

Conversely, the phenomenon of low critical digital literacy poses a significant challenge to personal data protection. Many social media users lack a clear understanding of how algorithms function, how their data is tracked and collected, or how privacy policies are often crafted for corporate benefits rather than to safeguard users. Consequently, most users consent to privacy policies without fully comprehending the implications. Therefore, enhancing digital literacy within society is imperative, encompassing not only a technical understanding of existing systems but also an awareness of individuals' privacy rights.

The implementation of a consent-based privacy model, as adopted by social media platforms, has also proven ineffective. Users frequently provide consent without a thorough

²⁰ Fanny Priscyllia, "Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum," *JATISWARA* 34, no. 3 (November 21, 2019): 239–49, <https://doi.org/10.29303/jtsw.v34i3.218>.

²¹ Shoshana Zuboff, *The Age Of Surveillance Capitalism: The Fight For A Human Future At The New Frontier Of Power* (New York: PublicAffairs, 2019). 12

²² Shoshana Zuboff. 16

understanding of how their data will be utilised or shared. With the proliferation of applications and platforms that utilise personal data, this approach has exacerbated the information inequality between companies and users. Thus, personal data protection should be predicated on a rights-based framework, positioning privacy as a fundamental right of individuals that must be safeguarded by existing regulations.

Stricter regulations, such as the General Data Protection Regulation (GDPR) in the European Union, can serve as an effective model for addressing this issue. The GDPR emphasises the principles of privacy by design, transparency, and clear user consent, which can mitigate the risk of personal data misuse. In Indonesia, Law No. 27 of 2022 concerning Personal Data Protection represents a critical initial step in safeguarding user privacy.²³ However, the primary challenge lies in ensuring consistent implementation and stringent oversight of violations occurring in the digital realm.

In addition to reinforcing regulations, a concerted effort is required to enhance public awareness concerning their rights related to personal data. This effort must encompass not only technical education on individual data protection strategies but also a broader understanding of power dynamics within the digital sphere. Governments, technology companies, and society must collaborate to foster a more transparent environment, wherein individuals possess complete control over their personal data and are equipped to make informed decisions in the face of digital challenges.

To advance personal data protection, robust collaboration among various stakeholders, including the government, the private sector, and the public, is essential. This cooperation is crucial for addressing the challenges that arise in the digital age. The government must enhance regulations concerning personal data protection by crafting laws that are more comprehensive and readily implementable. The private sector, particularly social media platforms, must embrace greater transparency in their data collection and usage policies and assume responsibility for the security of the data they manage. Concurrently, the public must receive in-depth education regarding their personal data rights and how to protect themselves from emerging threats in the digital landscape. Prioritising critical digital literacy is vital, enabling users to better understand the risks associated with social media usage and effectively manage their privacy.

Personal data protection transcends individual interests, serving as a foundation for establishing a fairer and more equitable digital ecosystem. In this context, technology should not solely function to exploit data for the benefit of specific entities; rather, it should reinforce the privacy rights of each individual and ensure that personal data is utilised with transparency and lawful consent. Moving forward, it is imperative to continually update existing regulations, adapt policies to technological advancements, and establish a more effective supervisory framework.²⁴ Absent concrete actions involving all societal elements, social media will persist as a fertile ground for data exploitation, and individual privacy rights will increasingly be disregarded within an unjust digital architecture. Thus, only through a

²³ Guswan Hakim et al., "Analisis Perbandingan Hukum Mengenai Regulasi Perlindungan Data Pribadi Antara Uni Eropa Dan Indonesia," *Halu Oleo Legal Research* 5, no. 2 (August 11, 2023): 443–53, <https://doi.org/10.33772/holresch.v5i2.338>.

²⁴ Debojoyti Chakraborty, "Copyright Challenges in the Digital Age: Balancing Intellectual Property Rights and Data Privacy in India's Online Ecosystem," *SSRN Electronic Journal*, November 29, 2023, <https://doi.org/10.2139/ssrn.4647960>.

more inclusive and human rights-based approach can we cultivate a safer, more transparent, and equitable digital world for every individual.²⁵

The safeguarding of personal data within Islamic values

Personal data is defined as information that can identify a person, either directly or indirectly, such as name, address, identification number, or other sensitive information. Reporting from the Kominfo website, personal data refers to certain individual information that is managed by being stored, maintained, maintained accurate, and protected in its confidentiality. Safeguarding personal data is part of human rights that fall within the protection of a person's privacy. This effort aims to ensure the right of every citizen to maintain their privacy, increase public awareness of the importance of personal data protection, and encourage respect and recognition of such protection. In Islam, personal data is in line with the concept of trust (*amanah*), which is the obligation to maintain individual privacy and honor. Personal information is considered a part of human honor that must be guarded from misuse or infringement.²⁶

The right to privacy in Islam is affirmed through various verses of the Qur'an and hadith that show the importance of maintaining the honor and confidentiality of the individual. The Qur'an, in Q.S. Al-Ḥujurāt 49(12), prohibits *tajassus* (lurking) and gossiping (*ghībah*), which are violations of one's privacy. In addition, Q.S. An-Nūr 24(27-28) teaches Muslims to ask for permission before entering another person's home, as a form of respect for the privacy of private space.²⁷ The hadith of the Prophet PBUH also reinforces this value, such as the prohibition of spreading the secrets of others without permission.²⁸ Meanwhile, Muhammad al-Jauzī explained that stalking or stalking someone without permission is like revealing the disgrace that Allah has covered²⁹. In this context, privacy is a satire that must be maintained between fellow humans. Mulyawan Safwandy said that privacy in Islam does not only include physical aspects, such as home and clothing, but also personal information and the right of individuals not to be misused by others.³⁰ This principle emphasizes that maintaining privacy is part of the noble morals that support a harmonious life in society.

Privacy in Islam is also seen as part of the protection of human honor which is one of the goals of sharia (*maqashid sharia*). Allah SWT prohibits all forms of privacy violations that can damage social relationships, such as spreading slander or looking for faults in others. In the hadith, the Prophet PBUH warned that whoever covers the disgrace of his brother, Allah will cover his disgrace in this world and the hereafter.³¹ Islam also regulates ethics in speaking, conveying information, and maintaining confidentiality, especially when one is entrusted with

²⁵ Abir Al-Harrasi, Abdul Khaliq Shaikh, and Ali Al-Badi, "Towards Protecting Organisations' Data by Preventing Data Theft by Malicious Insiders," *International Journal of Organizational Analysis* 31, no. 3 (April 10, 2023): 875–88, <https://doi.org/10.1108/IJOA-01-2021-2598>.

²⁶ Parida Angriani Baiq, "Perlindungan Hukum Terhadap Data Pribadi Dalam Transaksi E-Commerce: Perspektif Hukum Islam Dan Hukum Positif," *DIKTUM: Jurnal Syariah Dan Hukum* 19, no. 2 (December 2, 2021): 149–65, <https://doi.org/10.35905/diktum.v19i2.2463>.

²⁷ Muḥammad Ṭāhir Ibn 'Asyūr, *Al-Taḥrīr Wa Al-Tanwīr* (Tunis: Al-Dār Al-Tūnisīyah Linasyr, 1984). J.18, 196

²⁸ Abi Husain Muslim bin al-Hajjaj al-Qusyairiyy An-Naisaburry, *Sahih Muslim* (Kairo: Dar al-Hadith, 1991).

²⁹ 'Abdu Al-Raḥman bin 'Alīy bin Muḥammad Al-Jauzī, *Kasyfu Al-Musykil Min Ḥadīth Al-Ṣaḥīḥain* (Riyād: Dār Al-Waṭn, n.d.).

³⁰ Mulyawan Safwandy Nugraha, Didin Kurniadin Maskah, and Ai Rohayani, "Slamic Ethical Concepts Relevant to Digital Technology," in *Islamic Ethical Concepts Relevant to Digital Technology* (Surabaya: The International Conference on Islamic Civilization and Humanities (ICONITIES), 2023), 106–23.

³¹ Aḥmad Bin Ḥanbal, *Musnad Īmām Aḥmad Bin Ḥanbal* (2001: Maktabah al-Risalah, n.d.).

the.³² These values aim to maintain community harmony, prevent rifts, and ensure that each individual feels safe both physically and psychologically. Privacy in Islam is not only a right, but also an obligation to be respected and maintained by every Muslim.³³

The principles of personal data protection in Islam are based on the values of justice, honesty, and responsibility embedded in the teachings of the Qur'an and Hadith. Islam emphasizes the importance of maintaining the honor and privacy of individuals as part of human rights. This principle includes the prohibition of disseminating personal information without the permission of the owner, as affirmed in Q.S. An-Nūr 24(27-28) which commands Muslims to seek permission before entering another person's home.³⁴ The Prophet PBUH also reminded that the act of peeking or looking for the ugliness of others is a sin because it can damage someone's honor.³⁵ This principle is in line with the concept of respect for data privacy and security in the modern era, where personal information must be protected from misuse.

In addition, the principles of transparency and responsibility in the management of personal data are also in accordance with Islamic teachings. Any individual or institution that holds personal data is obliged to use it responsibly and only for permitted purposes.³⁶ From the perspective of sharia, maintaining trust is an absolute obligation, as mentioned in Q.S. Al-Aḥzāb 33(72) which emphasizes the importance of maintaining the trust that has been entrusted to him.³⁷ Misuse of personal data is considered a violation of human rights and divine trust. Therefore, Islam provides a strong moral and ethical foundation for protecting personal data, while encouraging the development of fair and responsible regulations in maintaining individual privacy in modern society.³⁸

Islam has taught that the management of personal data is based on ethical values aimed at safeguarding the honor, privacy, and rights of individuals. This ethics emphasizes the importance of honesty, responsibility, and trust in managing information. This principle is reflected in Q.S. Al-Hujurat 49(12), which prohibits the act of looking for the faults of others or disseminating information without permission. The Prophet PBUH also warned that keeping the secrets and information of others is part of the attitude of trust. Therefore, actions such as disseminating sensitive information without consent are considered to violate Islamic ethical values, as well as injure individuals' right to privacy.

Islamic law provides a strong basic framework for the management of personal data, with the main foundation being maqashid sharia, namely the protection of religion, soul, intellect, heredity, and property³⁹, and honor⁴⁰. In this context, personal data is included in the aspect of honor protection (*Ḥifẓ al-'Irdī*), so the act of misuse or theft of personal data is considered a violation of human rights. (Fad, 2021) Islam also requires the party holding the

³² Abdullah Albaar, M. Yusuf, and Ragwan Albaar, "The Principle of Confidentiality in Islamic Guidance and Counseling: A Review of Hadith," *Jurnal Bimbingan Dan Konseling Islam* 12, no. 2 (December 31, 2022): 184–207, <https://doi.org/10.29080/jbki.2022.12.2.184-207>.

³³ Abdul Karim Abdul Malik Amrullah, *Tafsir Al-Azhar* (Singapura: Pustaka National PTE LTD, 1989).

³⁴ M. Quraish Shihab, *Tafsir Al-Misbah: Pesan, Kesan Dan Keserasian Al-Qur'an* (Jakarta: Lentera Hati, 2012).

³⁵ Muhammad bin Jarīr al-Tabarī, *Jāmi' Al-Bayān 'an Ta'wīl Al-Qur'an* (Mekah: Dar al-Tarbiyah wa al-Turath, n.d.).

³⁶ Sekretariat Negara, "UU Republik Indonesia Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik" (2008).

³⁷ Badru Al-Dīn Al-'Ainī, *Umdah Al-Qārī Bi Syarḥi Ṣaḥīḥ Bukhārī* (Bairut, n.d.).

³⁸ Soediro Soediro, "Prinsip Keamanan, Privasi, Dan Etika Dalam Komunikasi Islam," *Kosmik Hukum* 18, no. 2 (October 1, 2018): 1–14, <https://doi.org/10.30595/kosmikhukum.v18i2.3439>.

³⁹ Abū Ishāq Ibrāhīm Al-Syāṭibī, *Al-Muwāfaqāt* (Mesir: Dār Ibnu 'Affān, 1997).

⁴⁰ Muḥammad Ṭāhir Ibn 'Asyūr, *Maqāṣid Al-Syar'iyah Al-Islāmīyah* (Qatar: Wizārah Al-Awqāf wa Al-Syu'un Al-Islāmīyah, 2004).

data to maintain its security and not use it for unauthorized purposes, in accordance with the principle of prohibition of harming others. For example, selling personal data without the owner's consent can be categorized as a fraudulent act that is prohibited in sharia.⁴¹

Personal data is information that can identify a person, either directly or indirectly, such as name, address, identification number, and other sensitive information. According to Kominfo, personal data refers to individual information that is managed, stored, and kept confidential. The protection of this personal data is in line with human rights, which are closely related to the privacy of individuals. In this context, Islam also teaches the importance of maintaining human privacy and honor as part of a greater moral responsibility. The principle of protection of honor (*Hifz al-'Ird*) is one of the most relevant bases in this context.

Hifz al-'Ird in Islam has a broader meaning than just physical protection of a person. This concept includes the protection of all forms of privacy and personal information related to individuals, including personal data that could reveal a person's identity. This is in line with the teachings of the Qur'an and hadith, which emphasize the importance of safeguarding the honor of individuals from abuse. For example, in Q.S. Al-Ḥujurat 49(12), the Qur'an prohibits stalking (*tajassus*) and gossiping (*ghībah*), which are violations of the privacy of others. In addition, Q.S. An-Nūr 24(27-28) teaches Muslims to ask permission before entering other people's homes, as a form of respect for the privacy of personal space.

The principle of *Hifz al-'Ird* is also affirmed in the hadiths of the Prophet which remind that spreading the secrets of others without permission is a prohibited act. In this context, individual privacy is part of the mandate that must be maintained by everyone. Muhammad al-Jauzī explained that stalking or stalking someone without permission is the same as exposing the disgrace that Allah has covered.⁴² This concept is also expressed by Mulyawan Safwandy, who said that in Islam, privacy is not only limited to the physical aspect, but also includes personal information that must be protected from misuse.

In the perspective of fiqh, the protection of individual honor including *Hifz al-'Ird* is part of maqashid sharia, which is the purpose of Islamic sharia to safeguard the five basic aspects of human life: religion, soul, intellect, descent, and property. The honor and privacy of individuals, in this context, are seen as an integral part of the protection of human rights. Classical scholars such as Al-Ghazālī and Ibn Qayyim⁴³ emphasized the importance of maintaining privacy and honor as part of efforts to create a harmonious and mutually respectful society. Al-Ghazālī in his work *Al-Mustasfa* states that maintaining honor is part of the effort to achieve a just and peaceful social life.⁴⁴

However, in the development of modern times, this protection of honor and privacy is increasingly relevant, especially in the context of digital technology. The rapid dissemination of personal information through social media and online platforms leads to threats against *Hifz al-'Ird*. Contemporary scholars such as Yusuf al-Qaradāwī expanded on this understanding in his work *Fiqh al-Maqāṣid*, asserting that the protection of honor should be seen as one of the basic needs that must be maintained in modern life.⁴⁵ Digital technology and

⁴¹ Abū 'Abdullāh Muḥammad bin Ismā'īl Al-Bukhārī, *Shahih Bukhārī* (Damsyiq: Dār Ibnu Kathīr, 1993). J. 6,2493

⁴² Jasser Auda, *Maqasid Al-Shariah as Philosophy of Islamic Law: A Sistem Approach* (Malaysia: Vinlin Press, 2010).

⁴³ 'Abdu Al-Rahman bin 'Alīy bin Muḥammad Al-Jauzī, *Kasyfu Al-Musykil Min Hadīth Al-Ṣaḥīḥain*.

⁴⁴ Abū Ḥamid Muḥammad ibn Muḥammad al-Ghazālī, *Al-Mustasfā Min 'Ilm Al-Uṣūl* (Beirut: Dār al-Kutub al-'Ilmiyyah, 1993).

⁴⁵ Yusuf Al-Qardāwī, *Ri'āyah Al-Biah Fī Syarī'ah Al-Islām* (Kairo: Dar al-Syuruq, 2001).

social media, according to al-Qaraḍāwī, have created new challenges in maintaining the honor of individuals, especially since personal information can now be easily disseminated and misused.

On the other hand, scholars such as Ṭāhir ibn 'Āshūr⁴⁶ hold to the five basic needs of maqashid sharia, but he also recognizes the importance of the protection of honor as part of the protection of posterity and religion. This shows that there is a development in the perspective of honor protection in the midst of changing times. A more adaptive approach by al-Qaraḍāwī views that *Hifz al-'Ird* should be placed on a par with other protections, given the threat to honor in the increasingly digital world, particularly through social media.

The phenomenon of using social media and disseminating content that has the potential to damage a person's honor further emphasizes the importance of personal data protection in this context. As Saibatul Hamdi and Khabib Musthofa explain, content that can damage a person's dignity even if it does not explicitly violate norms, still has a negative impact on individual honor. Therefore, the protection of personal data must involve stricter management, taking into account the values of *Hifz al-'Ird* in Islam.⁴⁷

In Islamic law, the principle of maqashid sharia provides strict guidelines regarding the protection of individual honor. Fiqh rules such as "*Everything that leads to what is haram is also haram*" supports the prohibition against the dissemination of information that can damage the honor of the individual.⁴⁸ Therefore, in a digital context, the application of *Hifz al-'Ird* through relevant fiqh principles is essential to maintain the privacy and honor of individuals. In this case, the ijtiḥad maqāṣidī approach provides a more adaptive perspective to the challenges that arise due to technological developments.

Overall, the protection of personal data and the honor of individuals should be seen as part of the effort to implement maqashid sharia. In an increasingly digitally connected world, strengthening the values of *Hifz al-'Ird* is key to creating a more dignified and civilized society. This is not only relevant to protect individuals from misuse of personal data, but also to build moral and social resilience in today's information age. The application of these principles in the digital context is crucial to maintain the privacy and honor of individuals in an increasingly connected world through technology.

Islamic perspectives on personal data theft

Personal data theft in the contemporary context refers to the act of accessing, obtaining, or misusing an individual's personal information without valid permission. This encompasses various forms of data misuse, such as identity theft, online fraud, and illegal access to information that should be protected.⁴⁹ In the digital realm, personal data theft frequently occurs through account hacking, unauthorised data collection, or the misuse of access to databases.⁵⁰ Such actions have the potential to adversely affect an individual's personal life, cause financial losses, and even damage their reputation. In Islam, this form of theft is contrary

⁴⁶ Muḥammad Ṭāhir Ibn 'Asyūr, *Maqāṣid Al-Syar'iyah Al-Islāmiyah*.

⁴⁷ Hamdi and Musthofa, "Menghadirkan Konsep Hifz Al-Irdi Dalam Bermedia Sosial: Upaya Menyikapi Asusila Abu-Abu Di Youtube."

⁴⁸ MZ Husamuddin, "Hifzh Al-'Ird Dalam Transformasi Sosial Modern." *Angewandte Chemie International Edition*, *Angewandte Chemie International Edition* 6, no. 11 (January 6, 2020): 119–32, <https://doi.org/10.47498/tasyri.v11i2.298>.

⁴⁹ Philippe Jougoux, "Identity Theft and Internet," *International Journal of Liability and Scientific Enquiry* 5, no. 1 (July 31, 2014): 37–45, <https://doi.org/10.1504/IJLSE.2012.045529>.

⁵⁰ Russel Butarbutar, "Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya," *Jurnal Hukum & Pembangunan* 2, no. 2 (August 24, 2023), <https://doi.org/10.21143/TELJ.vol2.no2.1043>.

to the fundamental principles that safeguard the rights of individuals, particularly with respect to their honour and privacy.⁵¹

Islam teaches the protection of individual privacy as an integral aspect of human rights, which is reflected in various religious teachings. One of the core principles is protection of honour and privacy (*Hifz al-'Irāḍi*), which asserts that every individual has the right to keep their private life free from external interference. The theft of personal data in Islam is regarded as a violation of a person's right to privacy, rendering such acts incompatible with Islamic teachings that emphasise the safeguarding of an individual's honour.

In Islam, any form of misuse of information, including the theft of personal data, is strictly prohibited as it contravenes the principles of justice and the obligation not to harm others. The hadith of the Prophet Muhammad (PBUH) stating "*la ḍarara wa lā ḍirara*" underscores the importance of protecting the rights of others⁵², including their personal information. Islam teaches that every individual should endeavour not to harm or deceive others, and the theft of personal data clearly constitutes a violation of this principle, as it can inflict material, emotional, and social harm upon the victim.

The theft of personal data in Islam can be analogised to theft or fraud, both of which are considered grave sins within the religion.⁵³ Although there is no specific law governing the theft of personal data, such acts remain contrary to Islamic principles that prohibit the unlawful appropriation of others' rights, including actions that exceed legal boundaries (*ta'addi*).⁵⁴ The act of stealing personal data, which involves the capture or utilisation of information without the owner's consent, can be classified as an act of *ghaṣab* from the perspective of Islamic law.

Ghaṣab refers to the act of illegally taking or exploiting another person's property rights, without clear permission, whether in the form of property, honour, or other personal rights.⁵⁵ In the context of personal data theft, an individual who deliberately accesses or uses someone else's data without valid permission has committed an act of illegally appropriating another's property. According to Islamic teachings, any action that violates the rights of others and causes harm, whether material or non-material, falls under the category of *ghaṣab* and is subject to punishment or the obligation to compensate for the harm caused. Therefore, the theft of personal data constitutes not only a violation of individual rights but also a breach of the principles of justice and protection espoused in Islam.

Islam stipulates that each individual bears the responsibility to protect and safeguard the personal data of others with complete trust and integrity. This is connected to the concept of trust (*amānah*), which obligates the maintenance of trust placed in one's care. Any personal data entrusted to an individual or institution must be kept confidential and not misused for personal gain. This principle aligns with Islamic teachings that emphasise the importance of maintaining integrity and trust (*murū'ah*) in all forms of relationships,⁵⁶ whether in business transactions, social interactions, or other engagements. Consequently, both individuals and

⁵¹ Muhammad Taufik and Fatimah Zahara, "Pengaturan Perlindungan Data Pribadi Dalam E-Commerce Menurut Perspektif Maqashid Syariah (Studi Kasus Marketplace Facebook," *Jurnal Ilmu Hukum, Humaniora Dan Politik (JIHHP)* 4, no. 6 (September 14, 2024): 2378–92, <https://doi.org/10.38035/jihhp.v4i6.2744>.

⁵² Majdu Al-Dīn Abū Al-Sa'ādāt Ibnu Al-Athīr, *Al-Syāfi Fī Syarḥ Musnad Al-Syāfi'ī Li Ibnī Al-Athīr* (Riyād: Maktabah Al-Rusyd, 2005).

⁵³ Majmu'at Al-Muallifīn, *Al-Fiqh Al-Manhājīy 'Ala Madzhab Imām Syāfi'īy* (Damsyīq: Dār Al-Qalam, 1992).

⁵⁴ 'Abdu Al-Razāq Al-Ṣan'ānīy, *Muṣannaf 'Abd Al-Razāq* (Beirut: Al-Maktab Al-Islāmīy, 1983).

⁵⁵ Abu Zakariyā Muḥyī Al-Dīn bin Syaraf Al-Nawawīy, *Minhāj Al-Ṭalībīn Wa 'Umdah Al-Muṭṭin Fi Al-* (Beirut: Dār Al-Kutub Al-'Ilmiyah, 2005).

⁵⁶ Abū ḥamid Al-Ghazālīy, *Iḥyā' 'Ulum Al-Dīn* (Beirut: Dār Al-Ma'rifah, n.d.).

institutions possess a moral and ethical obligation to protect the personal data of others from leakage or misuse.

Any form of interaction (*mu'āmalah*), including those involving the collection and use of personal data, must be predicated on clear and valid consent from the parties involved.⁵⁷ The concept of consent (*riḍā*) in Islam affirms that a person should not be compelled to relinquish their personal rights, including personal data, without their consent. This principle promotes transparency and openness in every transaction or data collection endeavour. The theft of personal data or the unauthorised collection of data is regarded as a violation of an individual's right to choose and control their personal information. In this context, Islam teaches that openness and consent form the legitimate foundations of all forms of social and business interaction.

Critical analysis of Islamic criminal law and Islamic principles on personal data protection as *Hifz Al-'Irḍi*

The classification of *maqashid sharia* in traditional discourse is typically divided into three principal levels: basic needs (*ḍarūrīyāt*), secondary needs (*ḥājīyāt*), and perfection (*taḥsīniyāt*). The category of *ḍarūrīyāt* encompasses five critical components, specifically the protection of religion (*Hifz al-Dīn*), the protection of the soul (*Hifz al-Nafs*), the protection of the intellect (*Hifz al-'Aql*), the protection of property (*Hifz al-Māl*), and the protection of offspring (*Hifz al-Nasl*). Some scholars of *fiqh* further include a sixth element, namely the protection of honour (*Hifz Al-'Irḍi*), which complements the five foundational aspects.⁵⁸

Concerning *Hifz Al-'Irḍi*, Al-Juwaini characterises this concept as "the preservation of honour." This notion has deep roots in ancient Arab culture, predating the advent of Islam. For instance, the poet Antarah once engaged in conflict with the tribe of Damdam due to perceived insults to his "honour." Similarly, the Prophet Muhammad underscored that the blood, property, and honour of every Muslim are sacrosanct and must not be violated.⁵⁹ In contemporary contexts, the term "honour" has broadened to include the safeguarding of dignity and human rights. In Indonesia, for example, the right to self-defence is enshrined in the 1945 Constitution. According to Article 28 G, Paragraph (1), citizens possess the right to personal protection, family, honour, dignity, and property. However, in light of advancements in information and communication technology, personal rights should not be limited to property rights as stipulated in that article.⁶⁰

In a hadith, it is revealed, "*kitman (the effort to cover something up) your helper in fulfilling some of your needs, for in every pleasure, there will surely be someone who envies it.*" This hadith indicates that Allah SWT has the right to protect our privacy and requires us to safeguard our secrets to prevent jealousy or exploitation. This highlights how strongly Islam encourages the protection of privacy, despite the absence of specific regulations within Islamic law regarding the rights and obligations of personal data owners. However, the Qur'an addresses *Hifz Al-'Irḍi* in Q.S. an-Nūr, 24(27): "*Do not enter any other house than your own until you have asked permission and greeted the occupants. For you who have believed, it is best to remember this.*"

⁵⁷ Zakariyā Al-Anṣārī, Athū Al-Wahāb Bi Syarḥ Minhāj Al-Ṭullāb (Damaskud: Dār Al-Fikr, 1994). J.1, 186

⁵⁸ Jasser Auda, *Maqasid Al-Shariah as Philosophy of Islamic Law: A Sistem Approach*. 3.

⁵⁹ Hamdi and Musthofa, "Menghadirkan Konsep Hifz Al-Irḍi Dalam Bermedia Sosial: Upaya Menyikapi Asusila Abu-Abu Di Youtube."

⁶⁰ Kadek Rima Anggen Suari and I Made Sarjana, "Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi Di Indonesia," *Jurnal Analisis Hukum* 6, no. 1 (April 25, 2023): 132–42, <https://doi.org/10.38043/jah.v6i1.4484>.

Hifz Al-'Irđi represents a concept in Islam that emphasises the safeguarding of an individual's honour, which encompasses aspects of dignity, privacy, and reputation. As a component of maqashid sharia, this concept is intended to foster social and moral stability within society. The primary objective is to prevent infringements of personal rights, such as defamation, which can damage interpersonal relationships. In Islam, the preservation of honour is a critical element in establishing harmony and justice.

The application of this concept is observable within various legal systems, including both Islamic law and positive law. In Islamic law, *Hifz Al-'Irđi* is reflected in the prohibition of actions such as *ghibah* and slander, as well as the imposition of penalties for offences that harm honour. Conversely, positive law incorporates this principle through data protection legislation, such as the General Data Protection Regulation (GDPR) in Europe and the Personal Data Protection Law in Indonesia, which govern the secure management of data.⁶¹ Advancements in technology further complicate the implementation of this concept, as personal data is now more accessible and susceptible to misuse.⁶² Consequently, measures such as data encryption and access management are essential to safeguard individual information.

The concept of *Hifz Al-'Irđi* in maqashid sharia correlates closely with personal data protection. The principle of preserving one's honour and self-esteem in Islam aligns with the safeguarding of confidential and sensitive personal information.⁶³ Personal data constitutes an integral aspect of an individual's identity; thus, its preservation is vital for respecting individual dignity. In the contemporary digital context, the relevance of this principle is magnified, as personal data can be readily collected, stored, and utilised. Therefore, an understanding of *Hifz Al-'Irđi* can provide a robust moral foundation for the development of personal data protection regulations and practices.

This principle is consistent with the aims of personal data protection, which seeks to shield individual privacy from the misuse of information that could be harmful.⁶⁴ Both *Hifz Al-'Irđi* and personal data protection underscore the significance of maintaining privacy and upholding individual rights. However, a fundamental distinction lies in their respective approaches: *Hifz Al-'Irđi* is grounded in spiritual and moral religious values, whereas personal data protection is legal and technical, governed by positive law and technological regulations. In the digital age, the interpretation of *Hifz Al-'Irđi* is increasingly expansive and relevant, encompassing the protection of dignity and security of personal information in cyberspace.

The protection of personal data, within the framework of *Hifz Al-'Irđi*, entails a stringent prohibition against actions that may compromise an individual's privacy or reputation. In the Qur'an, Allah forbids spying or seeking out the faults of others (*tajassus*), as articulated in Q.S. Hujurat 49(12). This prohibition highlights the high value placed on personal privacy in Islam, including the safeguarding of personal data. This principle can be applied within the context of personal data protection, where maintaining the confidentiality of an individual's

⁶¹ Guswan Hakim et al., "Analisis Perbandingan Hukum Mengenai Regulasi Perlindungan Data Pribadi Antara Uni Eropa Dan Indonesia."

⁶² Trias Palupi Kurnianingrum, "Urgensi Pelindungan Data Pribadi Konsumen Di Era Ekonomi Digital," *Kajian* 25, no. 3 (2020): 197–216, <https://doi.org/10.22212/kajian.v25i3.3893>.

⁶³ Cindy Vania et al., "Tinjauan Yuridis Terhadap Perlindungan Data Pribadi Dari Aspek Pengamanan Data Dan Keamanan Siber," *Jurnal Multidisiplin Indonesia* 2, no. 3 (March 18, 2023): 654–66, <https://doi.org/10.58344/jmi.v2i3.157>.

⁶⁴ Hasanuddin et al., "Jurnal Hukum Islam," *Jurnal Hukum Islam* 22, no. 2 (November 22, 2024): 313–42, 10.28918/jhi.v22i2.3.

information is regarded as a means of preserving their honour. Through *Ḥifẓ Al-'Irḍi*, Islam also advocates for the establishment of legal mechanisms to defend personal data against misuse. Historically, Islamic law has imposed severe sanctions for defamation, underscoring the seriousness with which Islam regards the protection of individual honour. Actions such as the theft of personal data, the unauthorised dissemination of information, or the sale of personal data without the owner's consent can be analogised as violations of the principles of *Ḥifẓ Al-'Irḍi*. Thus, personal data protection may be understood as a modern endeavour to realise the maqāṣid of sharia, particularly in the preservation of an individual's honour, dignity, and privacy.

Within the domain of Islamic criminal law, crimes occurring in the digital sphere, such as identity theft, account hacking, and the unauthorised dissemination of personal information, can be classified as criminal offences under *fiqh al-jināyah*. *Fiqh al-jināyah* is a branch of Islamic law that addresses various offences harming individuals and society. Digital crimes are not merely perceived as violations of social ethics but also as infringements on fundamental individual rights, which are protected by the principles of sharia. Within this framework, violations of personal data that may result in economic and reputational damage should incur equitable sanctions to safeguard these rights.

Generally, criminal offences in *fiqh al-jināyah* are classified into three primary categories: *ḥudūd*, *qisās*, and *ta'zīr*. *Ḥudūd* pertains to crimes with fixed penalties, such as adultery (zina), theft, and false accusations (*qadhḥ*). *Qisās* relates to retributive justice, including capital punishment or corporal punishment.⁶⁵ However, digital crimes, such as data theft and account hacking, do not fall within the categories of *ḥudūd* or *qisās*, as classical texts do not prescribe fixed penalties for such offences. Consequently, these violations are more appropriately classified under *ta'zīr*, which refers to discretionary punishment determined by the judge's *ijtihād*, based on the extent of harm caused and the necessity of protecting public welfare (*al-maslahah al-'āmmah*). Al-Māwardī elucidates that *ta'zīr* sanctions are adaptable, contingent upon circumstances, and enable the law to be applied in a manner that is both contextual and responsive to changing times.⁶⁶

Furthermore, if the violation of personal data involves defamation or slander, it may be classified as *jarimah qadhḥ* or *iftirā'*, as delineated in the Qur'an and the hadith of the Prophet Muhammad. *Qadhḥ* pertains to false accusations that harm an individual's reputation, such as allegations of adultery without substantiating evidence. In the digital realm, the disclosure of personal data that adversely affects an individual's reputation may be construed as a form of *qadhḥ*. Q.S. An-Nūr 24(4) explicitly prohibits defamation, underscoring the importance of protecting the *ḥifẓ al-'irḍ* of individuals.⁶⁷ This reinforces the notion that Islamic law robustly safeguards individuals from harm to their honour, and such violations, whether physical or digital, should be subject to appropriate penalties.

The foundational principles of Islamic law also emphasise the significance of trust and consent in all forms of interaction, including the collection of personal data. Islam mandates that any action involving others must be conducted with lawful consent and transparency, and the misuse of personal data without consent constitutes a violation of these principles. This is closely related to the prohibition of spying, as articulated in Q.S. al-Ḥujurāt 49(12), which forbids any form of intrusion into another's private matters without their consent,

⁶⁵ I-Māwardīy Al-Māwardīy, Al-Ḥawī Al-Kabīr Fī Fiqh Madzhab Al-Syafi'i (Beirut: Dār Al-Kutub Al-'Ilmiyah, 1999). J.13, 57

⁶⁶ Yusuf Al-Qardāwī, Ri'āyah Al-Biah Fī Syarī'ah Al-Islām. 83-85

⁶⁷ Abu Zakariyā Muḥyī Al-Dīn bin Syaraf Al-Nawawīy, Minhāj Al-Ṭalībīn Wa 'Umdah Al-Muftīn Fī Al-.142

including in the digital domain. Therefore, the collection and dissemination of personal data without clear or lawful consent can be regarded as a violation warranting *ta'zīr* sanctions under this principle.

With the evolution of digital technology, *fiqh al-jināyah* presents a flexible approach to emerging forms of crime arising in the digital sphere, such as data-related offences. *Fiqh al-jināyah* not only addresses crimes in the physical realm but also considers the social and economic consequences of violations of individual rights in digital space. *Ta'zīr* sanctions, which are more adaptable, allow for the imposition of just penalties based on the judge's *ijtihād*, taking into account the welfare and harm caused by the offence. This flexibility enables Islamic law to remain pertinent in addressing contemporary challenges and provides legal solutions that are both contextual and suitable for the evolving digital landscape.

In this context, Islamic criminal law, through the framework of *fiqh al-jināyah*, underscores the necessity of upholding justice, privacy, and individual rights in both physical and digital realms. The enforcement of just penalties for violations of personal data aims not only to punish the perpetrator but also to deter similar offences in the future. Thus, *fiqh al-jināyah* offers comprehensive protection for individual and societal rights in the modern socio-technological environment. This illustrates that, although *fiqh al-jināyah* is grounded in classical legal traditions, its core principles can be adapted to address the challenges and dynamics of contemporary digital law.

This study constitutes a significant scholarly contribution to the discourse on personal data protection, both within the national context of Indonesia and from a global perspective. Specifically, the findings enrich the body of legal and public policy scholarship by illuminating the persistent institutional and regulatory deficiencies that impede the effective implementation of Law No. 27 of 2022 on Personal Data Protection (PDP Law). The disparity between the normative framework of the law and the technical realities on the ground underscores the urgent necessity for a more responsive and adaptive data protection system amidst accelerating digital transformation. Globally, this research contributes to comparative policy studies by critically examining the divergent approaches adopted by developed and developing nations in formulating and enforcing data protection policies, with Indonesia serving as a representative case for emerging economies. The study's novelty lies in its interdisciplinary approach, which integrates legal, technological, and socio-political dimensions to provide a comprehensive understanding of the complexities surrounding personal data protection.

Based on these findings, several academic recommendations are proposed. It is essential to strengthen the role of an independent supervisory authority endowed with adequate technical and legal capacity to ensure effective law enforcement. Second, enhancing public digital literacy should become a national priority to raise awareness regarding individual data rights and the risks associated with misuse. Third, Indonesia is encouraged to engage in deeper international collaboration to align its data protection policies with global standards, such as the European Union's General Data Protection Regulation (GDPR). Fourth, regulatory frameworks must undergo regular reviews and updates in response to technological advancements, including big data analytics, artificial intelligence, and cloud computing systems. Fifth, educational and professional training curricula in the field of information technology should incorporate data ethics as a core component in developing human capital committed to digital justice. Consequently, this study not only provides descriptive and analytical insights but also offers normative and strategic solutions for the establishment of a more inclusive and sustainable data protection system.

Conclusion

This study indicates that *maqashid sharia*, including the concept of *Ḥifẓ Al-'Irḍi*, which underscores the importance of preserving individual privacy and honour, provides the foundation for the Islamic protection of personal data. *Tajassus* (spying) and the sharing of information without authorisation are prohibited in Islam, as stated in Q.S. Al-Ḥujurāt 49(12) and Q.S. An-Nūr 24(27-28). However, Islamic law necessitates reinterpretation within a contemporary context, as it currently lacks specific provisions regarding the security of digital data. Furthermore, it is evident from a sociological-legal perspective that public awareness and regulations are both essential for data protection. Many individuals are vulnerable to data breaches due to their low level of digital literacy. Consequently, to develop a more efficient and equitable framework for personal data protection, Islamic principles and contemporary regulations must be harmonised.

To enhance the security of personal data, it is recommended that Islamic principles be integrated into current laws, establishing a foundation based on both positive law and *maqashid sharia*. Increasing digital literacy in accordance with Islamic teachings also serves as a strategic initiative to elevate public understanding of the importance of privacy protection in the digital age. Educational institutions and religious organisations can provide instruction on digital ethics in Islam. Additionally, the government must intensify its oversight of digital service providers to ensure greater accountability and transparency in their use of user data. Building a secure digital ecosystem based on the principle of *ḥifẓ al-'irḍ* necessitates collaboration among academics, legal professionals, scholars, and regulators to ensure more effective and equitable protection of personal data.

Within the context of Islamic criminal law (*fiqh al-jināyah*), violations of personal data in the digital realm, such as identity theft, account hacking, and the unauthorised dissemination of information, can be categorised as crimes (*jarimah*) falling under discretionary punishment (*ta'zīr*). This classification arises from the absence of explicit provisions within the categories of fixed punishments (*ḥudūd*) and retributive justice (*qisās*) concerning digital crimes in classical legal literature. Through the *ta'zīr* approach, Islam permits legal authorities the flexibility to impose sanctions commensurate with the severity of the crime and the public benefit (*al-maṣlahah al-'āmmah*). Principles of Shariah, such as *ḥifẓ al-'irḍ* (protection of honour), *amanah* (trust), *riḍā* (consent), and the prohibition of *tajassus* (spying), form the normative foundation for defining personal data violations as infringements on fundamental individual rights that must be safeguarded. In cases that result in defamation, such violations may even be classified as false accusation (*qadhf*) or slander (*iftirā'*) according to Qur'anic and Sunnah guidelines. Thus, *fiqh al-jināyah* demonstrates conceptual and methodological flexibility to respond to the dynamics of contemporary digital crimes, offering a just, contextual, and human rights-oriented legal framework within the modern social landscape.

References

- 'Abdu Al-Raḥman bin 'Alīy bin Muḥammad Al-Jauzī. *Kasyfu Al-Musykil Min Ḥadīth Al-Ṣaḥīḥain*. Riyād: Dār Al-Waṭn, n.d.
- 'Abdu Al-Razāq Al-Ṣan'ānīy. *Muṣannaf 'Abd Al-Razāq*. Beirut: Al-Maktab Al-Islāmīy, 1983.
- Abdul Karim Abdul Malik Amrullah. *Tafsir Al-Azhar*. Singapura: Pustaka National PTE LTD, 1989.
- Abi Husain Muslim bin al-Hajjaj al-Qusyairiyy An-Naisaburry. *Sahih Muslim*. Kairo: Dar al-Hadith, 1991.

- Abū ‘Abdullāh Muḥammad bin Ismā‘īl Al-Bukhārī. *Shahih Bukhārī*. Damsyiq: Dār Ibnu Kathīr, 1993.
- Abū ḥāmid Al-Ghazālīy. *Iḥyā` ‘Ulum Al-Dīn*. Beirut: Dār Al-Ma‘rifah, n.d.
- Abū Ḥāmid Muḥammad ibn Muḥammad al-Ghazālī. *Al-Mustaṣfā Min ‘Ilm Al-Uṣūl*. Beirut: Dār al-Kutub al-‘Ilmiyyah, 1993.
- Abū Ishāq Ibrāhīm Al-Syāṭibīy. *Al-Muwāfaqāt*. Mesir: Dār Ibnu ‘Affān, 1997.
- Abu Zakariyā Muḥyī Al-Dīn bin Syaraf Al-Nawawīy. *Minḥāj Al-Ṭalībīn Wa ‘Umdah Al-Muṣṭafīn Fi Al-*. Beirut: Dār Al-Kutub Al-‘Ilmiyyah, 2005.
- Adi Ahdiat. “Indonesia Is among the Top 10 Countries with the Most Data Leaks.” Databoks, 2024. [https://www.deepl.com/en/translator#id/en-us/Indonesia Masuk 10 Negara dengan Kebocoran Data Terbesar](https://www.deepl.com/en/translator#id/en-us/Indonesia%20Masuk%2010%20Negara%20dengan%20Kebocoran%20Data%20Terbesar).
- Aḥmad Bin Ḥanbal. *Musnad Īmām Aḥmad Bin Ḥanbal*. 2001: Maktabah al-Risalah, n.d.
- Albaar, Abdullah, M. Yusuf, and Ragwan Albaar. “The Principle of Confidentiality in Islamic Guidance and Counseling: A Review of Hadith.” *Jurnal Bimbingan Dan Konseling Islam* 12, no. 2 (December 31, 2022): 184–207. <https://doi.org/10.29080/jbki.2022.12.2.184-207>.
- Al-Harrasi, Abir, Abdul Khalique Shaikh, and Ali Al-Badi. “Towards Protecting Organisations’ Data by Preventing Data Theft by Malicious Insiders.” *International Journal of Organizational Analysis* 31, no. 3 (April 10, 2023): 875–88. <https://doi.org/10.1108/IJOA-01-2021-2598>.
- Alojaiman, Bader. “Technological Modernizations in the Industry 5.0 Era: A Descriptive Analysis and Future Research Directions.” *Processes* 11, no. 5 (April 24, 2023): 1318. <https://doi.org/10.3390/pr11051318>.
- Anggen Suari, Kadek Rima, and I Made Sarjana. “Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi Di Indonesia.” *Jurnal Analisis Hukum* 6, no. 1 (April 25, 2023): 132–42. <https://doi.org/10.38043/jah.v6i1.4484>.
- Arif, Firman Muhammad. “Mitigasi Resiko Investasi Bodong Dan Aktualisasi Nalar Istislah.” *Al-Manahij: Jurnal Kajian Hukum Islam* 14, no. 1 (June 2, 2020): 19–34. <https://doi.org/10.24090/mnh.v14i1.3580>.
- Azzaakiyyah, Hizbul Khootimah. “The Impact of Social Media Use on Social Interaction in Contemporary Society.” *Technology and Society Perspectives (TACIT)* 1, no. 1 (August 31, 2023): 1–9. <https://doi.org/10.61100/tacit.v1i1.33>.
- Badru Al-Dīn Al-‘Ainī. *‘Umdah Al-Qārī Bi Syarḥi Ṣaḥīḥ Bukhārī*. Bairut, n.d.
- Butarbutar, Russel. “Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya.” *Jurnal Hukum & Pembangunan* 2, no. 2 (August 24, 2023). <https://doi.org/10.21143/TELJ.vol2.no2.1043>.
- Chakraborty, Debojoyti. “Copyright Challenges in the Digital Age: Balancing Intellectual Property Rights and Data Privacy in India’s Online Ecosystem.” *SSRN Electronic Journal*, November 29, 2023. <https://doi.org/10.2139/ssrn.4647960>.
- Dadang Suhendi, and Erwin Asmadi. “Cyber Laws Related to Prevention of Theft of Information Related to Acquisition of Land and Infrastructure Resources in Indonesia.” *International Journal of Cyber Criminology* 15, no. 2 (July 13, 2021): 135–43. <https://doi.org/10.5281/zenodo.4766552>.
- Dhaval Chudasama, and Raj Singh Deora. “Brief Study of Cybercrime on an Internet.” *Journal of Communication Engineering & Systems* 21, no. 1 (2021): 22–27.
- Dizon, Michael Anthony C. “Socio-Legal Study of Technology: A Norms and Values Approach to Hacking and Encryption Law and Policy.” *Computer Law & Security Review* 52 (April 2024): 105958. <https://doi.org/10.1016/j.clsr.2024.105958>.

- DPR RI. "Kebocoran Data Kembali Terjadi, Sukamta: Ini Alarm Keras Buat Pemerintah!," 2024. [ps://jdih.dpr.go.id/berita/detail/id/51640/t/Kebocoran+Data+Kembali+Terjadi%2C+Sukamta%3A+Ini+Alarm+Keras+Buat+Pemerintah%21](https://jdih.dpr.go.id/berita/detail/id/51640/t/Kebocoran+Data+Kembali+Terjadi%2C+Sukamta%3A+Ini+Alarm+Keras+Buat+Pemerintah%21).
- Finck, Michèle, and Frank Pallas. "They Who Must Not Be Identified — Distinguishing Personal from Non-Personal Data under the GDPR." *International Data Privacy Law* 10, no. 1 (February 1, 2020): 11–36. <https://doi.org/10.1093/idpl/ipz026>.
- Guswan Hakim, Jabalnur, Oheo Kaimuddin Haris, Ruliah, Sukring, and Muthaharry Mohammad. "Analisis Perbandingan Hukum Mengenai Regulasi Perlindungan Data Pribadi Antara Uni Eropa Dan Indonesia." *Halu Oleo Legal Research* 5, no. 2 (August 11, 2023): 443–53. <https://doi.org/10.33772/holresch.v5i2.338>.
- Hamdi, Saibatul, and Khabib Musthofa. "Menghadirkan Konsep Hifz Al-Irdi Dalam Bermedia Sosial: Upaya Menyikapi Asusila Abu-Abu Di Youtube." *El Madani : Jurnal Dakwah Dan Komunikasi Islam* 1, no. 02 (January 5, 2021): 141–62. <https://doi.org/10.53678/elmadani.v1i02.129>.
- Hasanuddin, Mowafg Masuwd, Muhammad Ridwan, Siti Walida Mustamin, Muhammad Saleh, and Fitriyani. "Jurnal Hukum Islam." *Jurnal Hukum Islam* 22, no. 2 (November 22, 2024): 313–42. [10.28918/jhi.v22i2.3](https://doi.org/10.28918/jhi.v22i2.3).
- Hasibuan, Edi Saputra, and Elfirda Ade Putri. "Perlindungan Keamanan Atas Data Pribadi Di Dunia Maya." *Jurnal Hukum Sasana* 10, no. 1 (June 8, 2024): 70–83. <https://doi.org/10.31599/sasana.v10i1.2134>.
- Jasser Auda. *Maqasid Al-Shariah as Philosophy of Islamic Law: A Sistem Approach*. Malaysia: Vinlin Press, 2010.
- Jougleux, Philippe. "Identity Theft and Internet." *International Journal of Liability and Scientific Enquiry* 5, no. 1 (July 31, 2014): 37–45. <https://doi.org/10.1504/IJLSE.2012.045529>.
- l-Māwardīy Al-Māwardīy. *Al-Ḥāwī Al-Kabīr Fī Fiqh Madzhab Al-Syāfi'ī*. Beirut: Dār Al-Kutub Al-'Ilmiyah, 1999.
- M. Quraish Shihab. *Tafsir Al-Misbah: Pesan, Kesan Dan Keserasian Al-Qur'an*. Jakarta: Lentera Hati, 2012.
- Majdu Al-Dīn Abū Al-Sa'ādāt Ibnu Al-Athīr. *Al-Syāfi Fī Syarḥ Musnad Al-Syāfi'ī Li Ibni Al-Athīr*. Riyād: Maktabah Al-Rusyd, 2005.
- Majmu'at Al-Muallifin. *Al-Fiqh Al-Manhājīy 'Ala Madzhab Imām Syāfi'īy*. Damsyīq: Dār Al-Qalam, 1992.
- Marta F Arroyabe, Carlos F.A. Arranz, Ignacio Fernandez De Arroyabe, and Juan Carlos Fernandez de Arroyabe. "Revealing the Realities of Cybercrime in Small and Medium Enterprises: Understanding Fear and Taxonomic Perspectives." *Computers and Security*, March 2024.
- Muh Rifqy Hidayatullah Arham, and M. Chaerul Risal. "Perlindungan Data Pribadi Bagi Pengguna Media Sosial." *Jurnal Al Tasyri'iyah* 3, no. 2 (December 11, 2023): 109–19.
- Muhammad bin Jarīr al-Tabarī. *Jāmi' Al-Bayān 'an Ta'wīl Al-Qur'ān*. Mekah: Dar al-Tarbiyah wa al-Turath, n.d.
- Muḥammad Ṭāhir Ibn 'Asyūr. *Al-Taḥrīr Wa Al-Tanzwīr*. Tunis: Al-Dār Al-Tūnisīyah Linasyr, 1984. — — —. *Maqāshid Al-Syar'iyah Al-Islāmīyah*. Qatar: Wizārah Al-Awqāf wa Al-Syu'ūn Al-Islāmīyah, 2004.
- Muhammad Taufik, and Fatimah Zahara. "Pengaturan Perlindungan Data Pribadi Dalam E-Commerce Menurut Perspektif Maqashid Syariah (Studi Kasus Marketplace Facebook)." *Jurnal Ilmu Hukum, Humaniora Dan Politik (JIHHP)* 4, no. 6 (September 14, 2024): 2378–92. <https://doi.org/10.38035/jihhp.v4i6.2744>.

- Mulyawan Safwandy Nugraha, Didin Kurniadin Maskah, and Ai Rohayani. "Slamic Ethical Concepts Relevant to Digital Technology." In *Islamic Ethical Concepts Relevant to Digital Technology*, 106–23. Surabaya: The International Conference on Islamic Civilization and Humanities (ICONITIES), 2023.
- MZ Husamuddin. "Hifzh Al-'Ird Dalam Transformasi Sosial Modern." *Angewandte Chemie International Edition*. "Angewandte Chemie International Edition 6, no. 11 (January 6, 2020): 119–32. <https://doi.org/10.47498/tasyri.v11i2.298>.
- Parida Angriani Baiq. "Perlindungan Hukum Terhadap Data Pribadi Dalam Transaksi E-Commerce: Perspektif Hukum Islam Dan Hukum Positif." *DIKTUM: Jurnal Syariah Dan Hukum* 19, no. 2 (December 2, 2021): 149–65. <https://doi.org/10.35905/diktum.v19i2.2463>.
- Priscyllia, Fanny. "Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum." *JATISWARA* 34, no. 3 (November 21, 2019): 239–49. <https://doi.org/10.29303/jtsw.v34i3.218>.
- Sekretariat Negara. UU Republik Indonesia Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik (2008).
- Sendjaja, Theodorus, Irwandi, Erwan Prastiawan, Yunita Suryani, and Endang Fatmawati. "Cybersecurity In The Digital Age: Developing Robust Strategies To Protect Against Evolving Global Digital Threats And Cyber Attacks." *International Journal of Science and Society* 6, no. 1 (March 1, 2024): 1008–19. <https://doi.org/10.54783/ijssoc.v6i1.1098>.
- Setiawati, Diana, Hary Abdul Hakim, and Fahmi Adam Hasby Yoga. "Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore." *Indonesian Comparative Law Review* 2, no. 2 (August 7, 2020). <https://doi.org/10.18196/iclr.2219>.
- Shoshana Zuboff. *The Age Of Surveillance Capitalism: The Fight For A Human Future At The New Frontier Of Power*. New York: PublicAffairs, 2019.
- Soediro Soediro. "Prinsip Keamanan, Privasi, Dan Etika Dalam Komunikasi Islam." *Kosmik Hukum* 18, no. 2 (October 1, 2018): 1–14. <https://doi.org/10.30595/kosmikhukum.v18i2.3439>.
- Sudarwanto, Al Sentot, and Dona Budi Budi Kharisma. "Comparative Study of Personal Data Protection Regulations in Indonesia, Hong Kong and Malaysia." *Journal of Financial Crime* 29, no. 4 (September 30, 2022): 1443–57. <https://doi.org/10.1108/JFC-09-2021-0193>.
- Trias Palupi Kurnianingrum. "Urgensi Pelindungan Data Pribadi Konsumen Di Era Ekonomi Digital." *Kajian* 25, no. 3 (2020): 197–216. <https://doi.org/10.22212/kajian.v25i3.3893>.
- Vania, Cindy, Markoni Markoni, Horadin Saragih, and Joko Widarto. "Tinjauan Yuridis Terhadap Perlindungan Data Pribadi Dari Aspek Pengamanan Data Dan Keamanan Siber." *Jurnal Multidisiplin Indonesia* 2, no. 3 (March 18, 2023): 654–66. <https://doi.org/10.58344/jmi.v2i3.157>.
- Yusrizal, Adwani, Rizanizarli, and Yanis Rinaldi. "Defamation and Insult Via Digital Media in Indonesia: The Islamic Law and Human Rights Perspective." *Journal of Law and Sustainable Development* 11, no. 7 (September 25, 2023): e1016. <https://doi.org/10.55908/sdgs.v11i7.1016>.
- Yusuf Al-Qardâwî. *Ri'āyah Al-Biah Fī Syarī'ah Al-Islām*. Kairo: Dar al-Syuruq, 2001.
- Zakariyā Al-Anṣārīy. *Aṭḥu Al-Wahāb Bi Syarḥ Minhāj Al-Ṭullāb*. Damaskud: Dār Al-Fikr, 1994.