



ISLAMIC LEGAL STRATEGIES IN INDONESIAN CONTEXTS TO COMBAT CYBERCRIME AND THE SPREAD OF ILLEGAL DATA DISSEMINATION

Muhammad Sibawaihi¹, Devika Rosa Guspita², Badriyah³

¹ Faculty of Sharia UIN Sulthan Thaha Saifuddin Jambi, Indonesia

² UIN Sunan Gunung Djati Bandung, Indonesia

³ Master of TESOL, Monash University, Australia

Email: msibawaihi@uinjambi.ac.id¹, devikarosagustipa@gmail.com²,
badr0001@student.monash.edu³

*Corresponding Author

DOI: 10.21154/justicia.v21i2.9587

Received: July 4, 2024

Revised: September 22, 2024

Approved: November 6, 2024

Abstract: This research examines Islamic law strategies in Indonesia to combat cybercrime and illegal data dissemination. The main focus is to identify and analyze relevant Islamic law approaches in cybercrime in Indonesia and assess their effectiveness in addressing illegal data dissemination. Qualitative methodology was used to collect data, including document analysis and expert interviews. The results show that applying Islamic law principles such as justice, transparency, and accountability can strengthen law enforcement policies and practices in addressing cybercrime. The findings also emphasize the importance of improving education and awareness about Islamic law in preventing cybercrime. As a practical contribution, this research offers a legal framework that policymakers and law enforcement can integrate to address cybercrime and illegal data dissemination more effectively. By referring to principles such as justice (*al-'adl*) and the protection of individual rights (*huquq al-insan*), the article proposes preventive and enforcement measures that can be applied in the context of legal product formulation, policy drafting and more flexible law enforcement.

Keywords: cybercrime; Islamic law; legal strategy; spread of illegal data.

Abstrak: Penelitian ini mengkaji strategi hukum Islam di Indonesia untuk memerangi kejahatan siber dan penyebaran data ilegal. Fokus utamanya adalah mengidentifikasi dan menganalisis pendekatan hukum Islam yang relevan dalam kejahatan siber di Indonesia dan menilai efektivitasnya dalam menangani penyebaran data ilegal. Metodologi kualitatif digunakan untuk mengumpulkan data, termasuk analisis dokumen dan wawancara ahli. Hasil penelitian menunjukkan bahwa penerapan prinsip-prinsip hukum Islam seperti keadilan, transparansi, dan akuntabilitas dapat memperkuat kebijakan dan praktik penegakan hukum dalam menangani kejahatan siber. Temuan ini juga menekankan pentingnya meningkatkan pendidikan dan

kesadaran tentang hukum Islam dalam mencegah kejahatan siber. Sebagai kontribusi praktis, penelitian ini menawarkan kerangka hukum yang dapat diintegrasikan oleh pembuat kebijakan dan penegak hukum untuk menangani kejahatan siber dan penyebaran data ilegal secara lebih efektif. Dengan mengacu pada prinsip-prinsip seperti keadilan (*al-'adl*) dan perlindungan hak-hak individu (*huquq al-insan*), artikel ini mengusulkan langkah-langkah pencegahan dan penegakan hukum yang dapat diterapkan dalam konteks perumusan produk hukum, penyusunan kebijakan maupun penegakan hukum yang lebih fleksibel.

Kata Kunci: Kejahatan dunia maya; Hukum Islam; strategi hukum; Penyebaran Data Ilegal.



Copyright: © 2024 by author (s). This work is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/).

INTRODUCTION

In the increasingly advanced digital era, information technology's evolution has significantly altered how humans live and interact.¹ The internet, mobile devices, and related technologies have revolutionized numerous aspects of life, influencing how we work, communicate, and engage with our environment.² This transformation has brought immense benefits but has also introduced severe challenges, notably cybercrime.

Cybercrime, encompassing activities such as identity theft, online fraud, network attacks, and data breaches, has escalated into a critical threat to individuals, corporations, and nations.³ For instance, in Indonesia, the National Data Center recently suffered a cyberattack orchestrated by malicious hackers, compromising the security of citizens' personal data and vital state information. This incident highlights the need for comprehensive cybersecurity measures to protect sensitive data.⁴

¹ Herman et al., "Kejahatan Carding Sebagai Bentuk Cyber Crime Dalam Hukum Pidana Indonesia," *Halu Oleo Legal Research* 5, no. 2 (August 31, 2023): 633–46, <https://doi.org/10.33772/holresch.v5i2.286>.

² Ardiansyah, M Rafi, and Pahmi Amri, "The Importance of Strengthening Legal Concepts in Overcoming Cybercrime During the Covid-19 Pandemic in Indonesia," in *International Conference on Human-Computer Interaction* (Springer, 2022), 469–79.

³ Muammar Bakry et al., "Strengthening the cyber terrorism law enforcement in Indonesia: Assimilation from Islamic jurisdiction," *International Journal of Criminology and Sociology* 10 (2021): 1267–76.

⁴ Saiful Aris Munandar, Arifin Abdullah, and Rispalman Rispalman, "The Offense of Using Pirated Computer Software in Law Nomor 28 of 2014 on Copyright Based on Islamic Criminal Law [Tindak Pidana Penggunaan Software Komputer Bajakan dalam Undang-Undang Nomor 28 Tahun 2014 Tentang Hak Cipta Perspektif Hukum Pidana Islam]," *Legitimasi: Jurnal Hukum Pidana dan Politik Hukum* 10, no. 2 (December 26, 2021): 238–55, <https://doi.org/10.22373/legitimasi.v10i2.11342>.

The repercussions of cybercrime are extensive, leading to substantial financial losses, significant disruptions in daily life, and the compromise of personal information and critical infrastructure. Addressing this issue requires a robust legal framework.⁵ However, the existing legal systems often struggle to keep pace with the rapid advancements and the complex nature of cybercrime. In response to these challenges, Islamic law offers a compelling and relevant approach, providing a set of principles that can be adapted to address the unique aspects of cybercrime.⁶

In recent years, cybercrime has become increasingly complex and disruptive worldwide. One prominent example is ransomware attacks targeting institutions, including hospitals, large corporations, and governments. In these attacks, cybercriminals use malicious software to encrypt victims' data and demand a hefty ransom for the decryption key.⁷ In addition, online fraud has become increasingly common, with modes ranging from investment to identity fraud. In addition, the spread of illegal content such as child pornography and radicalism also poses severe threats in the digital world.

In the face of these increasingly sophisticated cybercrimes, Islamic legal strategies offer a unique framework for addressing and preventing such crimes. Research has shown that Islamic law, with its principles emphasizing justice, responsibility, and protection of individual rights, can provide vital guidance in formulating legal responses to cybercrime.⁸ For example, in Islamic law, protecting five fundamental values—religion, life, intellect, lineage, and property—is a priority, which can be applied in cybercrime to protect individuals and society from such threats. In addition, Malaysia and Indonesia have demonstrated a solid commitment to strict Islamic law to protect against cybercrime.

The Islamic legal approach to cybercrime is limited to the application of punishment, prevention, and education. For example, the concept of 'ta'zir' in Islamic law allows judges to determine the appropriate sentence based on specific circumstances, including preventive measures such as blocking access to harmful

⁵ Rahmida Erliyani, "Examining Religious and Justice System in Indonesia to Prevent Cyberbullying," *International Journal of Cyber Criminology* 15, no. 2 (2022): 112-23.

⁶ Jastin Nurul Inayah and Taufiq Nugroho, "Criminal Implementation of Cyberbullying Based on Electronic Information and Transaction Law and Islamic Law," *Jurnal Usm Law Review* 7, no. 1 (March 14, 2024): 252-68, <https://doi.org/10.26623/julr.v7i1.8665>.

⁷ Sahat Maruli Tua Situmeang, "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber," *Sasi* 27, no. 1 (2021): 38-52.

⁸ Tim Hall et al., "Economic geographies of the illegal: the multiscalar production of cybercrime," *Trends in Organized Crime* 24 (2021): 282-307.

sites or distributing illegal content.⁹ In addition, education on digital ethics in the Islamic context can help raise awareness about the dangers of cybercrime and encourage responsible behavior online. Considering the perspective of Islamic law, this study aims to develop an Islamic legal strategy to address cybercrime and the distribution of illegal data.¹⁰ This strategy will include an in-depth analysis of Islamic legal principles, applying laws appropriate to the modern digital context, and collaboration between legal institutions and technology to create a resilient system to combat cybercrime. As such, this study is relevant to Muslim communities and provides insights for the global community in formulating effective legal responses to the ever-growing challenge of cybercrime.

In Islamic law, cyber operational theory can be interpreted as applying sharia principles in activities that occur in digital space. This includes various aspects such as buying and selling transactions, social interactions, and information dissemination.¹¹ For example, in online buying and selling, principles such as honesty, transparency, and fulfilling promises are highly emphasized in Islam, and these principles must be operationalized in the form of policies and practices that are fair to all parties involved. Apart from that, in social interactions, Islam teaches us to maintain manners and communication ethics, which prohibit bullying or insulting other people, including in cyberspace.¹²

Islamic law encourages fair and proportional law enforcement in responding to crime. In cybercrime, this means providing appropriate sanctions to the perpetrator in criminal penalties or restitution to the victim.¹³ Not only that, the principle of justice in Islamic law also requires the protection of individual rights, including the right to privacy and security. Therefore, efforts to prevent the spread of illegal content and protect victims of online fraud can be seen as part of

⁹ Venkat Ram Reddy Minampati and Jyoti Singh, "Cyber Crime-Diffusion, Effects, and Framework towards More Secure Cyber Security Network Governance in India'What Is Illegal Offline Is Illegal Online'," *Liberal Stud.* 8 (2023): 19.

¹⁰ Lutvy Priambono, Sudirman Sudirman, and Wahyudi Umar, "Kebocoran Data Pribadi Akibat Penagihan Utang Pinjaman Online Ilegal," *UNES Law Review* 6, no. 4 (2024): 11238-43.

¹¹ Rahmayati Rahmayati, "Competition Strategy In The Islamic Banking Industry: An Empirical Review," *International Journal Of Business, Economics, And Social Development* 2, no. 2 (2021): 65-71.

¹² Masriyani Masriyani, Nella Octaviany Siregar, and Tresya Tresya, "Tinjauan Yuridis Terhadap Penyebaran Data Pribadi Yang Dilakukan Oleh Aplikasi Pinjaman Online Ilegal," *Wajah Hukum* 8, no. 1 (2024): 249-58.

¹³ Fina Rahmawati, "Analisis Hukum Dan Syariah Dalam Budaya Digital: Tantangan Dan Peluang Di Era Teknologi," *Al-Hiwalah: Journal Syariah Economic Law* 2, no. 1 (June 28, 2023): 37-53, <https://doi.org/10.47766/alhiwalah.v2i1.1473>.

implementing these values. Islamic law, or Sharia, includes a set of ethical and legal principles that guide the lives of Muslims.¹⁴

These principles cover justice, security, and protection of individuals and society. Therefore, understanding and applying Islamic law principles in the context of cybercrime can provide a solid foundation for overcoming cybersecurity challenges. Ahmed Al-Dawoody, an Islamic law expert from the International Islamic University Malaysia, explained that Islamic law has great potential in dealing with cybercrime because of its inclusive and holistic principles.¹⁵ In Al-Dawoody's view, the principles of Islamic law, which include aspects of justice, security, and protection of individuals and society, can provide a solid foundation for overcoming cyber security challenges. However, despite its great potential, Dr. Sarah Qadeer, a legal researcher at the Center for Islamic Legislation and Ethics, Qatar, highlighted the need for Islamic legal experts to understand the context of modern technology and apply Islamic legal principles in a rapidly evolving situation such as cybercrime. This research explores relevant Islamic legal concepts and analyzes applicable legal strategies in this context. It builds upon a foundation of prior research, which includes:

The first research was written by Bakry, Abu Bakar, Risal Ahmad, and Amiruddin, and it was titled *Strengthening Cyber Terrorism Law Enforcement in Indonesia: Assimilation of Islamic Jurisdiction*.¹⁶ This research aims to strengthen legal action against cyberterrorism. This strengthening is obtained by assimilating Islamic law through normative juridical methods. Data comes from related news and updated journals. Researchers found that this was an assimilation of Islamic law products into positive law in Indonesia through Hirabah, Rebel Punishment, or Takzir. It is hoped that this idea can be taken into consideration by policymakers in updating their laws so that they can further suppress terrorist crimes, especially in cyberspace.

The following research is entitled *Globalization of Law in Preventing Cyber Crime*, and Sirega and Sinaga wrote it.¹⁷ Globalization makes the world without borders; countries compete freely in various fields, sometimes even crossing the

¹⁴ Hall et al., "Economic geographies of the illegal: the multiscalar production of cybercrime." 287.

¹⁵ Suud Sarim Karimullah, "Pursuing Legal Harmony: Indonesianization of Islamic Law Concept and Its Impact on National Law," *Mazahib* 21, no. 2 (2022): 213-44.

¹⁶ Mayada Afriga Arum Dari and Nadya Melinda Oktarina, "Islamic Criminal Law Principles in Regulation of Misuse Information on Social Media Victims," *Rechtenstudent* 4, no. 1 (2023): 15-25.

¹⁷ Russel Butarbutar, "Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya," *Technology and Economics Law Journal* 2, no. 2 (2023): 3.

boundaries of a country's jurisdiction, so overcoming cybercrime in legal regulations is necessary. Regarding the jurisdiction of this global crime, there needs to be a separate law that regulates cyber crimes. The approach method uses normative juridical. The results of the research and discussion state that the globalization of law and politics provides efforts to overcome cybercrime where the application of legal norms between nations plays an increasingly important role, especially in regulating all forms of advances in information, communication, and transportation technology.

The difference between this article and the previous research above is that this research focuses on overcoming cybercrime from an Islamic legal perspective using applicable legal strategies and approaches. Additionally, several academic concerns have emerged regarding how Islamic law principles can be applied effectively in the increasingly complex context of cybercrime. Challenges such as limited understanding of Islamic law in the context of modern technology, differences of opinion among Islamic legal scholars regarding applying these principles, and issues of compliance with international law are significant concerns. By considering the complexity and urgency of this problem, this article aims to examine legal strategies and approaches in dealing with cybercrime from an Islamic legal perspective. Therefore, this article provides insight into how Islamic law responds to the challenges of modern cybercrime and explores potential effective solutions to protect society from this growing threat.¹⁸

This study seeks to enhance the comprehension of Islamic legal principles' role in safeguarding individuals and society against cybercrime threats. Through careful document analysis and detailed interviews with experts in Islamic law and cybersecurity, this study seeks to understand how Islamic legal principles can be applied to address contemporary issues arising from information technology. By considering various cybercrime cases and comparing them with the existing Islamic legal framework, this study attempts to identify gaps and challenges and propose practical solutions by Islamic law.¹⁹

To achieve these objectives, this study identifies the basic principles of Islamic law relevant to cybercrime, such as the principles of justice, protection of privacy,

¹⁸ Putri Avini Azzahra -, "Cyber Crime 'Phishing' In Islamic Law," *Tawazuna* 3, no. 2 (June 28, 2024): 20-24, <https://doi.org/10.35747/twz.v3i2.999>.

¹⁹ Tegar Islami Putra, Akbar Jihadul Islam, and Abdullah Mufti Abdul Rahman, "Integrating Islamic Laws into Indonesian Data Protection Laws: An Analysis of Regulatory Landscape and Ethical Considerations," *Contemporary Issues on Interfaith Law and Society* 3, no. 1 (January 31, 2024): 85-118, <https://doi.org/10.15294/ciils.v3i1.78690>.

and the prohibition of spreading slander. It then continues by analyzing how these principles can be applied in specific cybercrime cases, including phishing, hacking, and the spread of malware. This analysis is enriched by interviews with experts who provide different perspectives on implementing Islamic law in the context of cybercrime.

This study uses a descriptive qualitative method to gain an in-depth understanding of Islamic legal strategies in the Indonesian context to combat cybercrime and the spread of illegal data. This method involves collecting qualitative data, such as interviews, observations, and document analysis, which are then analyzed descriptively to identify patterns, themes, and relationships. Data were obtained through extensive literature studies, including reviews of relevant legal regulations and expert interviews. After the data was collected, the analysis was done by categorizing information, interpreting meaning, and arranging it in a coherent framework to build a comprehensive understanding of the research subject. The results of this analysis were then used to formulate effective legal strategies for addressing cybercrime problems using the principles of Islamic law and the socio-cultural context of Indonesia.

ISLAMIC LEGAL STRATEGIES IN PREVENTING CYBERCRIMES

In the context of cybercrime, this may involve the application of Sharia law to determine appropriate punishments or preventive measures. For example, Cybercrime, a term encompassing a wide range of illegal activities conducted through digital media, has become a significant global issue with far-reaching implications.²⁰ The phenomenon encompasses various criminal acts such as data breaches, financial fraud, identity theft, and cyber espionage.²¹ With the rapid expansion of digital technology, cybercrime has evolved into a complex and sophisticated enterprise, often crossing national borders and challenging traditional law enforcement methods.²²

The Islamic legal strategy for preventing cybercrime in Indonesia involves the application of Sharia principles to address cybercrime. Although Indonesia does not yet have a specific law regulating cybercrime, several existing favorable laws have

²⁰ Cheng Chen and Bin Dong, "Digital Forensics Analysis Based on Cybercrime and the Study of the Rule of Law in Space Governance," *Open Computer Science* 13, no. 1 (May 25, 2023): 20220266, <https://doi.org/10.1515/comp-2022-0266>.

²¹ Naila Nur Izzah, "Law Enforcement Against Scampage at Polda Jatim: Perspectives of Positive Law and Islamic Criminal Law," *Peradaban Journal of Law and Society* 3, no. 1 (2024): 63-76.

²² Putra, Islam, and Rahman, "Integrating Islamic Laws into Indonesian Data Protection Laws."

been used to address this issue. According to Islamic law, preventive measures and punishments for cybercrime can include ta'zir, with various methods such as imprisonment, exile, flogging, and the death penalty. Ta'zir punishments based on Islamic law are significant because they provide an alternative to controlling cybercrime. In addition, with the discussion of cybercrime in Islamic law, this becomes one alternative and way to prevent this criminal act. The prevention strategy also involves educating the public about the dangers of cybercrime and the importance of maintaining ethics and morality in cyberspace through Islamic teachings.²³ This education aims to increase public awareness and understanding of cybercrime's legal consequences and negative impacts. Cooperation between law enforcement agencies and religious institutions is also needed to strengthen the prevention and handling of cybercrime. Thus, the strategy of Islamic law in preventing cybercrime in Indonesia combines positive law, public education, and inter-institutional cooperation to create a safe cyber environment based on Sharia values.²⁴

In response to this growing threat, Islamic legal strategies offer a unique perspective based on Sharia law principles, emphasizing the protection of five fundamental values: religion, life, intellect, lineage, and property. Applying Islamic legal principles to cybercrime prevention involves a multifaceted approach that includes establishing a clear legal framework, promoting ethical online behavior, and implementing robust cybersecurity measures. For example, Sharia law can guide appropriate sanctions and fines for cyberattacks threatening these core values, deterring potential cyber criminals.

Islamic legal strategies can contribute to international efforts to combat cybercrime by offering insights into digital behavior's ethical and moral dimensions. As the digital landscape evolves, integrating Islamic legal principles with contemporary cybercrime laws can help create a more holistic approach to prevention and enforcement. This integration should address the technical aspects of cybersecurity and consider the ethical implications, ensuring that the digital world aligns with the moral values and social norms held dear by the Islamic community.

²³ Sri Jaya Lesmana, Inas Sofia, and Felina Felina, "Law Enforcement in Efforts to Combat Cyber Crime in Indonesia Building Future Digital Security," *The International Journal of Law Review and State Administration* 1, no. 3 (2023): 120-28.

²⁴ Ita Musarrofa and Holilur Rohman, "'Urf of Cyberspace: Solutions to the Problems of Islamic Law in the Digital Age," *Al-Ahkam* 33, no. 1 (April 30, 2023): 63-88, <https://doi.org/10.21580/ahkam.2023.33.1.13236>.

The importance of discussing Islamic legal strategies in cybercrime prevention lies in the potential to bridge the gap between modern technological challenges and traditional legal and ethical frameworks. Drawing on the rich legacy of Islamic jurisprudence, these strategies can provide a foundation for developing comprehensive laws and policies that effectively address the complexities of cybercrime while remaining steadfast to the values of justice, accountability, and protection of the common good. In a world of increasingly widespread cyber threats, the contribution of Islamic legal thought to the discourse on cybercrime prevention is relevant and essential to fostering a safe and ethical digital environment.

Research by Mansoor Al-A'ali from the University of Bahrain explored 'Adellah' (Shariah evidence from the Quran, Hadith, and sayings of the Imams) to verify the Islamic view on computer crimes.²⁵ Second, "cybercrime" is an illegal activity that uses computer facilities or computer networks without permission and is against the law. According to Islamic law, the punishment for cybercrime is ta'zir with various methods, such as imprisonment, exile, flogging, and the death penalty, which shows the importance of Islamic law in dealing with this crime, especially since some countries do not yet have specific regulations governing cybercrime.²⁶ Third, "illegal data dissemination" refers to distributing information prohibited by law, including copyrighted material, pornographic content, or stolen personal data. In Islam, the protection of individual property and privacy rights is highly emphasized, and violation of this can be considered an act that is detrimental to society.

This article explores how Islamic legal principles can be applied to address cybercrime in Indonesia. By identifying and analyzing relevant approaches, this article seeks to understand how Islamic law can effectively solve the problem of illegal data dissemination. This includes assessing the various aspects of Islamic law that may contribute to preventing and handling cybercrime and evaluating how these principles can be integrated into the existing legal framework to enhance national cybersecurity. In doing so, this article provides insight into the application of Islamic law and how it can interact with contemporary challenges such as cybercrime.

²⁵ Indra Rahmatullah, "The Legal Protection of Sharia Financial Technology in Indonesia (Analysis of Regulation, Structure and Law Enforcement)," 2020.

²⁶ Mohammed I Alghamdi, "A Descriptive Study on the Impact of Cybercrime and Possible Measures to Curtail Its Spread Worldwide," *International Journal of Engineering Research and Technology* 9 (2020): 731-35.

These goals underscore the need to safeguard individuals' digital rights and privacy. Islamic law's emphasis on the sanctity of contracts and the prohibition of fraud and harm aligns with modern legal frameworks that seek to protect individuals from fraudulent online activities.²⁷ The application of 'Qawaid Fiqhiyyah' (Islamic legal principles) further provides a dynamic tool to interpret Islamic law in a manner that is relevant to the prevention and resolution of cybercrime.²⁸ For example, the principle of 'al-Darar yuzal' (harm must be removed) can be used to justify the removal of harmful online content and support for victims.

In addition, the concept of 'tazkiyah' (purification) in Islam relates to the individual's spiritual growth and the purification of society from injustices such as cybercrime.²⁹ This holistic approach encourages the development of a moral and ethical online environment. The narrative can also explore the role of 'Hisbah' (accountability) in Islam, which advocates a community-based approach to monitoring and preventing unethical practices, including those in the digital realm.

By combining the principles of 'adl' (justice) and 'Ihsan' (righteousness), the narrative can articulate how Islamic teachings promote justice and compassion in dealing with victims of cybercrime. The integration of 'Shura' (consultation) into the Islamic governance system illustrates the collaborative efforts required to formulate effective strategies against cybercrime. By drawing parallels between traditional Islamic and modern cyber governance, the narrative can highlight the proactive role of Islamic legal strategy in combating cybercrime and supporting victims.

Islamic legal strategies offer a comprehensive approach to combating cybercrime, deeply rooted in the principles of justice, compassion, and shared responsibility.³⁰ These strategies are theoretical constructs and practical tools that can be effectively applied in the digital realm. For example, the law enforcement process under Islamic law can involve the application of 'Ta'zir,' a form of discretionary punishment, which can be tailored to the severity and nature of the cybercrime committed. Islamic courts, guided by the principles of Shariah, will handle cybercrime cases by considering the evidence within the framework of

²⁷ Saida Dita Hanifawati, "Urgensi Penegakan Hukum Pidana Pada Penerima Pinjaman Kegiatan Peer to Peer Lending Fintech Ilegal Dan Perlindungan Data Pribadi," *Jurnal Penegakan Hukum Dan Keadilan* 2, no. 2 (2021): 162-72.

²⁸ Miftakhur Rokhman Habibi and Isnatul Liviani, "Kejahatan Teknologi Informasi (Cyber Crime) Dan Penanggulangannya Dalam Sistem Hukum Indonesia," *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam* 23, no. 2 (2020): 400-426.

²⁹ Fatkhul Muin, "Hukum Islam Dan Teknologi: Adaptasi Hukum Islam Dengan Perkembangan Teknologi," *IDRIS: InDonesian Journal of Islamic Studies* 1, no. 1 (2023): 107-23.

³⁰ Rahmayati, "Competition Strategy in The Islamic Banking Industry: An Empirical Review."

Islamic jurisprudence, ensuring that punishment not only upholds justice but also aims to reform the perpetrator.

The role of Islamic legal institutions is crucial, as they are responsible for interpreting the 'Adellah' (evidence from the Quran, Hadith, and sayings of the Imams) to formulate laws that address the challenges posed by cybercrime while upholding the protection of the five essential values: religion, life, intellect, progeny and property. This holistic approach demonstrates the adaptability of Islamic teachings in providing solutions to contemporary problems such as cybercrime, thereby safeguarding individual rights and maintaining social harmony by the universal principles of human dignity and the rule of law.

ISLAMIC LEGAL STRATEGY TO COMBAT ILLEGAL DATA DISTRIBUTION

In the face of the growing challenge of cybercrime, one major issue is the distribution of illegal data. This challenge includes ensuring data security, maintaining privacy, and addressing data interoperability issues. In addition, the large volume of data and the need to maintain data accuracy and integrity add to the issue's complexity.³¹ From an Islamic legal perspective, the approach protects core values such as religion, life, intellect, progeny, and property. Islamic law imposes sanctions and fines on cyberattacks that threaten these values to protect society from cybercrime. Thus, Islamic law can significantly contribute to resolving the problem of the distribution of illegal data, which aligns with the values and norms respected in society.³²

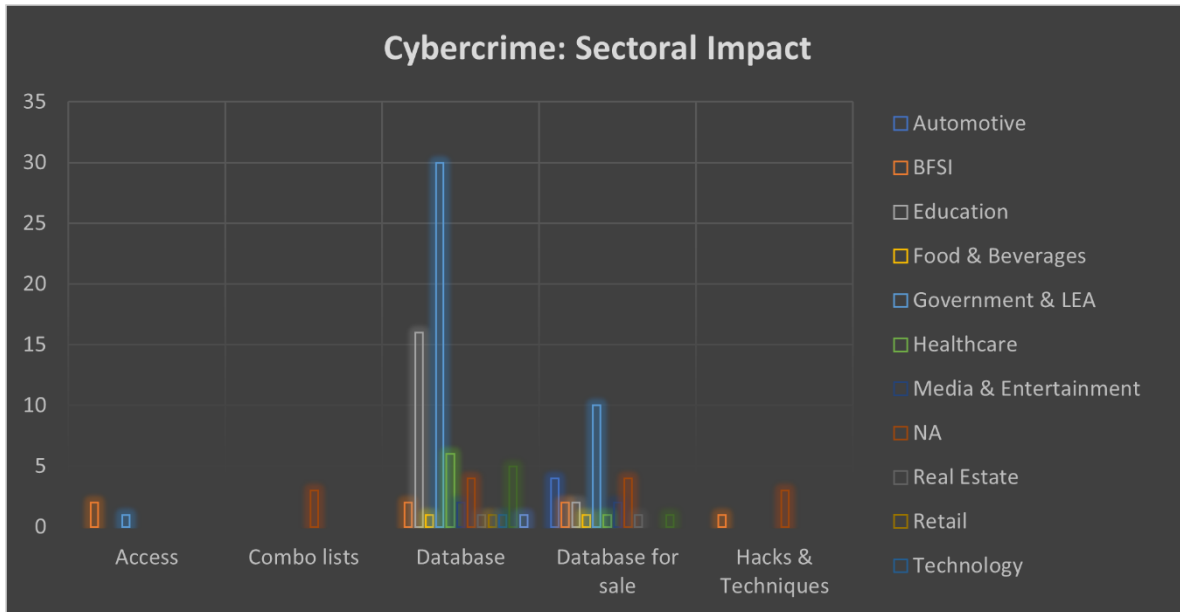
Integrating Islamic legal principles into law enforcement policies offers a unique and potentially effective perspective. Justice, one of the main pillars of Islamic law, demands that everyone be treated fairly and equally before the law, including in cybercrime cases.³³ Transparency in the legal process ensures that all parties can see and understand how decisions are made, thereby increasing public trust in the legal system. Responsibility, both individual and collective, underscores the importance of everyone in preventing and combating cybercrime. The following are the types of cybercrime in Indonesia that Cybel managed to collect in the 2022 period:

³¹ Fajar Kurniawan, Didik Suhariyanto, and Hartana Hartana, "Perlindungan Konsumen Terhadap Pinjaman Online Atas Penyebaran Data Pribadi," *Innovative: Journal Of Social Science Research* 4, no. 1 (2024): 2817–29.

³² Dari and Oktarina, "Islamic Criminal Law Principles in Regulation of Misuse Information on Social Media Victims."

³³ Deni Kamaludin Yusup, "Cyber Security Sharing Platform: Indonesia Approach in Law Enforcement of Financial Transaction Crimes," *J. Legal Ethical & Regul. Issues* 25 (2022): 1.

Figure 1. Types of Cybercrime in Indonesia



The most common cybercrime data found is database hacking, related to data taken or distributed illegally. Researchers try to examine this further by discussing it with one of the academics focusing on technology, Ade Irfan. He explained that cybercrime that has occurred in Indonesia lately is a very dangerous alarm for the State and its citizens themselves. Therefore, a clear legal umbrella for protecting personal data and the embodiment of state cyber security must be created and thought through carefully to suppress crimes still occurring in this cyber world. Education about Islamic law and cybercrime is essential to increase public awareness and understanding. Effective teaching can be done in several ways, such as holding seminars and workshops that discuss the principles of Islamic law related to cybercrime and ways to identify and protect yourself from cyber threats.

Educational materials should include real-life case studies, prevention strategies, and the importance of ethics and morals in using the internet. In addition, collaboration with information technology experts can enrich the material with the latest technical knowledge.³⁴ Thus, individuals will not only become more vigilant but can also actively contribute to efforts to prevent cybercrime, which aligns with the moral and ethical values taught in Islamic law.

The strategy of Islamic law in dealing with cybercrime and the spread of illegal

³⁴ Hadi Prasetyo, "Penegakan Hukum Terhadap Debt Collector Yang Melakukan Penyebaran Data Pribadi Pengguna Fintech Ditinjau Dari Pasal 26 UU No 19 Tahun 2016 Tentang Informasi Teknologi Elektronik," in *Bandung Conference Series: Law Studies*, vol. 2, 2022, 615-21.

data involves a multidisciplinary approach that includes legal, technological, social, and educational aspects. Applying Islamic law consistent with its principles can provide a robust framework for fair and effective cyber law.³⁵ This includes creating clear rules, strict law enforcement, and solid international cooperation in dealing with transnational crimes. Amid rapid technological advances, cybercrime has become a global threat that impacts various aspects of life. The impacts are severe and far-reaching, from identity theft to attacks on critical infrastructure.

Islamic law also offers a strong concept of (legal) responsibility in dealing with cybercrime. Individuals involved in cybercrime must be held accountable for their actions before human law and Allah SWT. Sanctions and consequences regulated in Islamic law must be applied fairly and proportionally by Islamic law principles. Not only that, Islamic law also encourages the prevention of cybercrime through education and public awareness. Through its emphasis on moral and ethical values in the use of technology, Islam seeks to create an environment where cybercrime can be minimized.

Implementing legal strategies that comply with Islamic law principles is crucial in dealing with increasing cybercrime.³⁶ In this context, discussing legal strategies that can be implemented becomes very important. One strategy that has emerged is law enforcement based on Islamic legal values. This includes developing a legal system that integrates Islamic law principles in regulations and law enforcement related to cybercrime. Sarah Qadeer, Islamic law researcher at the Center for Islamic Legislation and Ethics, Qatar, emphasized the importance of understanding the context of modern technology in applying Islamic law principles in handling cyber. According to Qadeer, a deep understanding of the dynamics and development of digital technology is very important so that the principles of Islamic law can be applied effectively. Professor Ahmed Al-Dawoody, an Islamic law expert from the International Islamic University Malaysia, highlighted the relevance of Islamic legal principles in addressing cybercrime.³⁷

Al-Dawoody emphasized that Islamic law has excellent potential to provide

³⁵ Raj Singh Deora and Dhaval Chudasama, "Brief Study of Cybercrime on an Internet," *Journal of Communication Engineering & Systems* 11, no. 1 (2021): 1-6.

³⁶ Erliyani, "Examining Religious and Justice System in Indonesia to Prevent Cyberbullying."

³⁷ Siti Aura Fadhillah, Michelle Sharon Anastasia Matakupan, and Britney Wilhelmina Berlian Minggu, "Peran Interpol Dalam Penyelesaian Kasus Kejahatan Siber Berdasarkan Konvensi Budapest On Cybercrimes," *Journal on Education* 5, no. 4 (2023): 16553-64.

practical solutions to cybercrime because of its inclusive and holistic principles.³⁸ According to him, Islamic law principles of justice, security, and protection can provide a solid framework for facing cyber security challenges. In law enforcement, Professor Jonathan AC Brown, an Islamic law expert from Georgetown University, highlighted the importance of cooperation between security authorities and religious institutions in dealing with cybercrime.³⁹ Brown stressed that effective law enforcement requires close collaboration between authorities and religious leaders to identify, prevent, and prosecute cybercriminals. In addition, Dr Asma Uddin, an Islamic law researcher from the Al-Madinah Institute, highlighted the critical role of education and public awareness in preventing cybercrime.⁴⁰

Uddin emphasized that knowledge about the risks and consequences of cybercrime and understanding ethical and moral values in Islamic law can help individuals and society not become victims or perpetrators of cybercrime. Therefore, handling cybercrime from an Islamic legal perspective requires a holistic and integrated approach.⁴¹ Strategies that involve understanding modern technology, effective law enforcement, collaboration between institutions, and public education and awareness are key to effectively addressing the threat of cybercrime within the framework of Islamic law. Additionally, efforts to prevent cybercrime should be made through education and public awareness. By strengthening understanding of the ethical and moral values that underlie Islamic law, it is hoped that individuals and society can be more alert to the threat of cybercrime and take appropriate preventative steps.

Cybercrime prevention is a series of proactive actions to prevent crimes or law violations from occurring in cyberspace.⁴² The goal is to reduce the risk and vulnerability to cyberattacks and protect individuals, organizations, and infrastructure from threats arising from the digital environment.⁴³ Cybercrime

³⁸ Thomas Paterson, "Indonesian Cyberspace Expansion: A Double-Edged Sword," *Journal of Cyber Policy* 4, no. 2 (2019): 216–34.

³⁹ Marta Pomykała, "The Central Cybercrime Bureau as a New Police Service Established to Combat Cybercrime," *Humanities and Social Sciences quarterly* 31, no. 2 (30 Juni 2024): 131–41, <https://doi.org/10.7862/rz.2024.hss.24>.

⁴⁰ Sindy Ariyaningsih et al., "Korelasi Kejahatan Siber dengan Percepatan Digitalisasi di Indonesia," *Justisia: Jurnal Ilmu Hukum* 1, no. 1 (2023): 1–11.

⁴¹ Muhammad Ridha Iswardhana, "Cyber Diplomacy And Protection Measures Against Threats Of Information Communication Technology In Indonesia," *Journal of Islamic World and Politics* 5, no. 2 (2021): 343–67.

⁴² Wadha Abdullah Al-Khater et al., "Comprehensive review of cybercrime detection techniques," *IEEE access* 8 (2020): 137293–311.

⁴³ Václav Jirovský et al., "Cybercrime and organized crime," dalam *Proceedings of the 13th international conference on availability, reliability and security*, 2018, 1–5.

prevention involves various strategies and actions to reduce the potential harm caused by cyberattacks.⁴⁴ Education and training on Islamic law can play a significant role in preventing and addressing cybercrime.⁴⁵ By understanding Islamic law principles, individuals can be more aware of their online actions' legal and moral consequences.⁴⁶ For example, education on the concept of 'Adellah' in Islam, which refers to the evidence of Sharia from the Quran, Hadith, and the sayings of the Imams, can provide ethical solid guidance in interacting online. In addition, training in Islamic law can help develop an appropriate legal framework to address cybercrime, aligning with Muslim societies' values and norms. It can also encourage the development of policies and best practices that are effective, fair, and just, taking into account aspects such as privacy, security, and human rights. The following are several aspects that need to be considered in efforts to prevent cybercrime:⁴⁷

1. Policies and Procedures: Implementing strict policies and procedures at the individual, corporate, and government levels can help reduce vulnerability to cyber attacks. This includes information security policies, procedures for handling sensitive data, and good cybersecurity practices.
2. Security Technology: Security technology such as firewalls, antivirus, and encryption software can help protect systems and data from cyber threats. Regular security assessments and system updates are also crucial for maintaining digital security.
3. Cooperation and Collaboration: Collaboration between the parties involved, including governments, law enforcement agencies, the private sector, and civil society, is necessary to confront cyber threats effectively. This includes information exchange, cybercrime reporting, and cooperation in law enforcement.

In cybercrime, the Shariah protects five values: religion, human life, reason, progeny, and property. Therefore, sanctions and fines are applied to cyberattacks that threaten any of these values. For example, Malaysia and Indonesia have firmly

⁴⁴ Ardiansyah, Rafi, and Amri, "The Importance of Strengthening Legal Concepts in Overcoming Cybercrime During the Covid-19 Pandemic in Indonesia."

⁴⁵ Suharyadi Suharyadi, Said Sampara, and Kamri Ahmad, "Kejahatan Dunia Maya (Cyber Crime) Dalam Prespektif Hukum Islam," *Journal of Lex Generalis (JLG)* 1, no. 5 (2020): 761-73.

⁴⁶ R Arif Muljohadi, "Analisis Yuridis Kejahatan Online Berbasis Gender Dalam Perspektif Hukum Positif Dan Hukum Pidana Islam," *The Jure: Journal of Islamic Law* 1, no. 2 (2024): 47-63.

⁴⁷ Nurbaiti Marufah, Hayatul Khairul Rahmat, dan I Dewa Ketut Kerta Widana, "Degradasi moral sebagai dampak kejahatan siber pada generasi millennial di Indonesia," *Nusantara: Jurnal Ilmu Pengetahuan Sosial* 7, no. 1 (2020): 191-201.

committed to strict Islamic law to protect against cybercrime. Furthermore, a critical analysis of Pakistan's cybercrime legislation from an Islamic legal perspective shows that the Standing Committee also made some sections too broad, such as the clause to remove content, if necessary, that is inappropriate or inconsistent with Islam.

CONCLUSIONS

This study explores Indonesia's Islamic legal approach to cybercrime and illegal data dissemination. The study seeks to assess their effectiveness in a local context by identifying and analyzing relevant Islamic legal strategies. The novelty of this study lies in the specific application of Islamic legal principles to address contemporary issues, such as cybercrime, which pose new challenges to society and the law. This study is significant because it provides insight into how Islamic law can be adapted to address modern legal issues while also providing practical solutions to the problem of illegal data dissemination. In conclusion, this study significantly contributes to our understanding of Islamic law and its application in combating cybercrime. It demonstrates the potential of Islamic law as a practical framework for combating illegal data dissemination in Indonesia.

REFERENCES

- Alghamdi, Mohammed I. "A Descriptive Study on the Impact of Cybercrime and Possible Measures to Curtail Its Spread Worldwide." *International Journal of Engineering Research and Technology* 9 (2020): 731-35.
- Al-Khater, Wadha Abdullah, Somaya Al-Maadeed, Abdulghani Ali Ahmed, Ali Safaa Sadiq, and Muhammad Khurram Khan. "Comprehensive Review of Cybercrime Detection Techniques." *IEEE Access* 8 (2020): 137293-311.
- Ardiansyah, M Rafi, and Pahmi Amri. "The Importance of Strengthening Legal Concepts in Overcoming Cybercrime During the Covid-19 Pandemic in Indonesia." In *International Conference on Human-Computer Interaction*, 469-79. Springer, 2022.
- Ariyaningsih, Sindy, A Ari Andrianto, Adri Surya Kusuma, and Rina Arum Prastyanti. "Korelasi Kejahatan Siber Dengan Percepatan Digitalisasi Di Indonesia." *Justisia: Jurnal Ilmu Hukum* 1, no. 1 (2023): 1-11.
- Azzahra -, Putri Avini. "Cyber Crime 'Phishing' In Islamic Law." *Tawazuna* 3, no. 2 (June 28, 2024): 20-24. <https://doi.org/10.35747/twz.v3i2.999>.
- Bakry, Muammar, Abdul Syatar, Achmad Abubakar, Chaerul Risal, Ahmad Ahmad, and Muhammad Majdy Amiruddin. "Strengthening the Cyber Terrorism Law Enforcement in Indonesia: Assimilation from Islamic

- Jurisdiction." *International Journal of Criminology and Sociology* 10 (2021): 1267-76.
- Butarbutar, Russel. "Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya." *Technology and Economics Law Journal* 2, no. 2 (2023): 3.
- Chen, Cheng, and Bin Dong. "Digital Forensics Analysis Based on Cybercrime and the Study of the Rule of Law in Space Governance." *Open Computer Science* 13, no. 1 (May 25, 2023): 20220266. <https://doi.org/10.1515/comp-2022-0266>.
- Dari, Mayada Afriga Arum, and Nadya Melinda Oktarina. "Islamic Criminal Law Principles in Regulation of Misuse Information on Social Media Victims." *Rechtenstudent* 4, no. 1 (2023): 15-25.
- Deora, Raj Singh, and Dhaval Chudasama. "Brief Study of Cybercrime on an Internet." *Journal of Communication Engineering & Systems* 11, no. 1 (2021): 1-6.
- Erliyani, Rahmida. "Examining Religious and Justice System in Indonesia to Prevent Cyberbullying." *International Journal of Cyber Criminology* 15, no. 2 (2022): 112-23.
- Fadhillah, Siti Aura, Michelle Sharon Anastasia Matakupan, and Britney Wilhelmina Berlian Mingga. "Peran Interpol Dalam Penyelesaian Kasus Kejahatan Siber Berdasarkan Konvensi Budapest On Cybercrimes." *Journal on Education* 5, no. 4 (2023): 16553-64.
- Habibi, Miftakhur Rokhman, and Isnatul Liviani. "Kejahatan Teknologi Informasi (Cyber Crime) Dan Penanggulangannya Dalam Sistem Hukum Indonesia." *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam* 23, no. 2 (2020): 400-426.
- Hall, Tim, Ben Sanders, Mamadou Bah, Owen King, and Edward Wigley. "Economic Geographies of the Illegal: The Multiscalar Production of Cybercrime." *Trends in Organized Crime* 24 (2021): 282-307.
- Hanifawati, Saida Dita. "Urgensi Penegakan Hukum Pidana Pada Penerima Pinjaman Kegiatan Peer to Peer Lending Fintech Ilegal Dan Perlindungan Data Pribadi." *Jurnal Penegakan Hukum Dan Keadilan* 2, no. 2 (2021): 162-72.
- Herman, Handrawan, Oheo Kaimuddin Haris, Sabrina Hidayat, Zahrowati, and Riski Dwitasari. "Kejahatan Carding Sebagai Bentuk Cyber Crime Dalam Hukum Pidana Indonesia." *Halu Oleo Legal Research* 5, no. 2 (August 31, 2023): 633-46. <https://doi.org/10.33772/holresch.v5i2.286>.
- Inayah, Jastin Nurul, and Taufiq Nugroho. "Criminal Implementation of Cyberbullying Based on Electronic Information and Transaction Law and Islamic Law." *JURNAL USM LAW REVIEW* 7, no. 1 (March 14, 2024): 252-68. <https://doi.org/10.26623/julr.v7i1.8665>.
- Iswardhana, Muhammad Ridha. "Cyber Diplomacy And Protection Measures Against Threats Of Information Communication Technology In Indonesia." *Journal of Islamic World and Politics* 5, no. 2 (2021): 343-67.

- Izzah, Naila Nur. "Law Enforcement Against Scampage at Polda Jatim: Perspectives of Positive Law and Islamic Criminal Law." *Peradaban Journal of Law and Society* 3, no. 1 (2024): 63-76.
- Jirovský, Václav, Andrej Pastorek, Max Mühlhäuser, and Andrea Tundis. "Cybercrime and Organized Crime." In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, 1-5, 2018.
- Karimullah, Suud Sarim. "Pursuing Legal Harmony: Indonesianization of Islamic Law Concept and Its Impact on National Law." *Mazahib* 21, no. 2 (2022): 213-44.
- Kurniawan, Fajar, Didik Suhariyanto, and Hartana Hartana. "Perlindungan Konsumen Terhadap Pinjaman Online Atas Penyebaran Data Pribadi." *Innovative: Journal Of Social Science Research* 4, no. 1 (2024): 2817-29.
- Lesmana, Sri Jaya, Inas Sofia, and Felina Felina. "Law Enforcement in Efforts to Combat Cyber Crime in Indonesia Building Future Digital Security." *The International Journal of Law Review and State Administration* 1, no. 3 (2023): 120-28.
- Marufah, Nurbaiti, Hayatul Khairul Rahmat, and I Dewa Ketut Kerta Widana. "Degradasi Moral Sebagai Dampak Kejahatan Siber Pada Generasi Millennial Di Indonesia." *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial* 7, no. 1 (2020): 191-201.
- Masriyani, Masriyani, Nella Octaviany Siregar, and Tresya Tresya. "Tinjauan Yuridis Terhadap Penyebaran Data Pribadi Yang Dilakukan Oleh Aplikasi Pinjaman Online Ilegal." *Wajah Hukum* 8, no. 1 (2024): 249-58.
- Minampati, Venkat Ram Reddy, and Jyoti Singh. "Cyber Crime-Diffusion, Effects, and Framework towards More Secure Cyber Security Network Governance in India'What Is Illegal Offline Is Illegal Online'." *Liberal Stud.* 8 (2023): 19.
- Muin, Fatkhul. "Hukum Islam Dan Teknologi: Adaptasi Hukum Islam Dengan Perkembangan Teknologi." *IDRIS: InDonesian Journal of Islamic Studies* 1, no. 1 (2023): 107-23.
- Muljohadi, R Arif. "Analisis Yuridis Kejahatan Online Berbasis Gender Dalam Perspektif Hukum Positif Dan Hukum Pidana Islam." *The Jure: Journal of Islamic Law* 1, no. 2 (2024): 47-63.
- Munandar, Saiful Aris, Arifin Abdullah, and Rispalman Rispalman. "The Offense of Using Pirated Computer Software in Law Nomor 28 of 2014 on Copyright Based on Islamic Criminal Law [Tindak Pidana Penggunaan Software Komputer Bajakan dalam Undang-Undang Nomor 28 Tahun 2014 Tentang Hak Cipta Perspektif Hukum Pidana Islam]." *Legitimasi: Jurnal Hukum Pidana dan Politik Hukum* 10, no. 2 (December 26, 2021): 238-55. <https://doi.org/10.22373/legitimasi.v10i2.11342>.

- Musarrofa, Ita, and Holilur Rohman. "Urf of Cyberspace: Solutions to the Problems of Islamic Law in the Digital Age." *Al-Ahkam* 33, no. 1 (April 30, 2023): 63–88. <https://doi.org/10.21580/ahkam.2023.33.1.13236>.
- Paterson, Thomas. "Indonesian Cyberspace Expansion: A Double-Edged Sword." *Journal of Cyber Policy* 4, no. 2 (2019): 216–34.
- Pomykala, Marta. "The Central Cybercrime Bureau As a New Police Service Established to Combat Cybercrime." *Humanities and Social Sciences Quarterly* 31, no. 2 (June 30, 2024): 131–41. <https://doi.org/10.7862/rz.2024.hss.24>.
- Prasetyo, Hadi. "Penegakan Hukum Terhadap Debt Collector Yang Melakukan Penyebaran Data Pribadi Pengguna Fintech Ditinjau Dari Pasal 26 UU No 19 Tahun 2016 Tentang Informasi Teknologi Elektronik." In *Bandung Conference Series: Law Studies*, 2:615–21, 2022.
- Priambono, Lutvy, Sudirman Sudirman, and Wahyudi Umar. "Kebocoran Data Pribadi Akibat Penagihan Utang Pinjaman Online Ilegal." *UNES Law Review* 6, no. 4 (2024): 11238–43.
- Putra, Tegar Islami, Akbar Jihadul Islam, and Abdullah Mufti Abdul Rahman. "Integrating Islamic Laws into Indonesian Data Protection Laws: An Analysis of Regulatory Landscape and Ethical Considerations." *Contemporary Issues on Interfaith Law and Society* 3, no. 1 (January 31, 2024): 85–118. <https://doi.org/10.15294/ciils.v3i1.78690>.
- Rahmatullah, Indra. "The Legal Protection of Sharia Financial Technology in Indonesia (Analysis of Regulation, Structure and Law Enforcement)," 2020.
- Rahmawati, Fina. "Analisis Hukum Dan Syariah Dalam Budaya Digital: Tantangan Dan Peluang Di Era Teknologi." *Al-Hiwalah : Journal Syariah Economic Law* 2, no. 1 (June 28, 2023): 37–53. <https://doi.org/10.47766/alhiwalah.v2i1.1473>.
- Rahmayati, Rahmayati. "Competition Strategy In The Islamic Banking Industry: An Empirical Review." *International Journal of Business, Economics, and Social Development* 2, no. 2 (2021): 65–71.
- Situmeang, Sahat Maruli Tua. "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber." *Sasi* 27, no. 1 (2021): 38–52.
- Suharyadi, Suharyadi, Said Sampara, and Kamri Ahmad. "Kejahatan Dunia Maya (Cyber Crime) Dalam Prespektif Hukum Islam." *Journal of Lex Generalis (JLG)* 1, no. 5 (2020): 761–73.
- Yusup, Deni Kamaludin. "Cyber Security Sharing Platform: Indonesia Approach in Law Enforcement of Financial Transaction Crimes." *J. Legal Ethical & Regul. Isses* 25 (2022): 1.

