Al-Manāhij: Jurnal Kajian Hukum Islam
Vol. 17 No. 1, January-June 2023, 53-68
DOI: https://doi.org/10.24090/mnh.v17i1.7633

Published by Sharia Faculty of State Islamic University of Prof. K.H. Saifuddin Zuhri, Purwokerto

Al-Manāhij
Jurnal Kajian Hukum Islam

P-ISSN: 1978-6670 | E-ISSN: 2579-4167

Sharia E-Wallet: The Issue of Sharia Compliance and Data Protection

Muhammad Khaeruddin Hamsin[1*], Abdul Halim[2], Rizaldy Anggriawan[3], Hilda Lutfiani[4]

*[1*3]Universitas Muhammadiyah Yogyakarta*
Jl. Brawijaya, Daerah Istimewa Yogyakarta 55183

[2]Universitas Islam Negeri Sunan Kalijaga
Jl. Laksda Adisucipto, Daerah Istimewa Yogyakarta 55281

[4]Universiti Islam Sultan Sharif Ali
347, Jalan Pasar Gadong, Bandar Seri Begawan, Brunei Darussalam

Email: *[1*]khaeruddin@umy.ac.id, [2]abd.halim@uin-suka.ac.id, [3]rizaldy.ipols@umy.ac.id, [4]18mr902@siswa.unissa.edu.bn*

Submitted	: 09-01-2023	Accepted	: 04-04-2023
Revision	: 24-03-2023	Publish	: 17-04-2023

Abstract: Sharia digital payments have lately emerged as one of the most significant innovations and breakthroughs in the field of Islamic economics in Indonesia. However, behind the positive side of the use of sharia e-wallets, there is one thing that all parties involved need to pay attention to, which if ignored can become a double-edged sword for its users, namely compliance, security, and personal data protection. The paper aims to investigate how the Indonesian government governs data privacy for Islamic e-wallet users. It also investigates the potential risks and challenges of Islamic digital payments particularly in regard to data protection. Besides, it also investigates whether or not the sharia e-wallet has complied with the Fatwa of DSN-MUI. The study used normative research methods employing statutory, case, and conceptual approaches. This study reveals that the use of sharia e-wallets in Indonesia is essentially in compliance with Islamic principles as stated in the Fatwa of the National Sharia Council. As for the protection of personal data, in fact, this has been regulated in a comprehensive manner by the government and related state institutions such as Bank Indonesia and the Financial Services Authority. However, the government still has work that must be considered in regard to the compliance of sharia digital payment operators with established laws and regulations, where in the event of the operators violated the use of data privacy, thus they will face a severe sanctions stipulated by the prevailed rule.

Keywords : Sharia E-wallet, Data Privacy, Sharia Compliance

***Abstrak*:** *Pembayaran digital syariah akhir-akhir ini muncul sebagai salah satu inovasi dan terobosan paling signifikan di bidang ekonomi syariah di Indonesia. Namun, di balik sisi positif penggunaan e-wallet syariah, ada satu hal yang perlu diperhatikan oleh semua pihak yang terlibat, yang jika diabaikan bisa menjadi pedang bermata dua bagi penggunanya, yaitu kepatuhan, keamanan, dan perlindungan data pribadi. Artikel ini bertujuan untuk menyelidiki bagaimana pemerintah Indonesia mengatur privasi data untuk pengguna e-wallet Syariah. Studi ini juga menyelidiki potensi risiko dan tantangan pembayaran digital Syariah khususnya*

dalam hal perlindungan data. Di samping itu, penelitian ini juga melihat apakah penggunaan dompet digital syariah telah memenuhi kepatuhan syariah sebagaimana ditetapkan oleh Fatwa DSN-MUI. Penelitian ini menggunakan metode penelitian normatif dengan pendekatan perundang-undangan, kasus, dan konseptual. Kajian ini mengungkapkan bahwa penggunaan e-wallet syariah di Indonesia pada dasarnya telah sesuai dengan prinsip Islam sebagaimana tertuang dalam Fatwa Dewan Syariah Nasional. Adapun perlindungan data pribadi sebenarnya sudah diatur secara komprehensif oleh pemerintah dan lembaga negara terkait seperti Bank Indonesia dan Otoritas Jasa Keuangan. Namun, pemerintah masih memiliki pekerjaan yang harus diperhatikan terkait kepatuhan operator pembayaran digital syariah terhadap peraturan perundang-undangan yang ditetapkan, dimana dalam hal operator melakukan pelanggaran data privasi, maka akan menghadapi hukuman yang berat sebagaimana ditetapkan dalam peraturan.

Kata Kunci : *E-wallet Syariah, Data Privasi, Kepatuhan Syariah*

Introduction

According to the 2019/2020 Global Islamic Economy Report, Indonesia is the nation with the strongest sharia financial indicators in the world, coming in at number five, up from number ten in 2018.[1] The 2019-2024 Halal Economic Masterplan, which was developed, calls for strengthening the halal economy across all sectors.[2] Given that Indonesia has the biggest proportion of Muslims roughly 87 percent of its 273 million people this is plausible.[3] This is a possible market share for sharia-based goods and services, such as digital payment methods based on the religion, including e-wallets or e-money.

Similar to other nations that have gone before it, Indonesia is beginning to transition to a cashless society by maximizing the use of digital payment systems to cut down on cash payments.[4] According to information released by the Bank Indonesia (BI), 51 businesses issued electronic money in 2020, with the average value of all transactions from January to May being IDR 15 trillion.[5] E-money transactions in Indonesia are increasing significantly year over year, with a notable jump in 2019 of about 400 percent, or four times the prior year.[6] According to the data, Indonesian society is on the path to become a cashless society like that of other nations. The majority of Indonesians, particularly those who reside in cities, are also said to make less cash payments.

With producing electronic money based on sharia, Islamic finance has the potential to spread the message of Islamic economics in Indonesia using the data as explained above. This prevents the riba (interest) that is currently present in electronic money.[7] At the end of 2019, Indonesia's first and only

1 Yudho Taruno Muryanto, Dona Budi Kharisma, and Anjar Sri Ciptorukmi Nugraheni, "Prospects and Challenges of Islamic Fintech in Indonesia: A Legal Viewpoint," *International Journal of Law and Management*, 2021.

2 A Yusup et al., "Halal Industry Certification in Bandung, Indonesia: Opportunities and Challenges," *Islam, Media and Education in the Digital Era*, 2022, 70–81.

3 Vita Briliana and Nurwanti Mursito, "Exploring Antecedents and Consequences of Indonesian Muslim Youths' Attitude towards Halal Cosmetic Products: A Case Study in Jakarta," *Asia Pacific Management Review* 22, no. 4 (2017): 176–84.

4 Zahrotur Rusyda Hinduan, Adilla Anggraeni, and Muhamad Irfan Agia, "Generation Z in Indonesia: The Self-Driven Digital," in *The New Generation Z in Asia: Dynamics, Differences, Digitalisation* (Emerald Publishing Limited, 2020).

5 Marvello Yang et al., "Cashless Transactions: A Study on Intention and Adoption of e-Wallets," *Sustainability* 13, no. 2 (2021): 831.

6 Augi Ciptarianto and Yudo Anggoro, "E-Wallet Application Penetration for Financial Inclusion in Indonesia," *International Journal of Current Science Research and Review* 5, no. 2 (2022): 319–32.

7 Muhammad Syarif Hidayatullah and Rahmat Fadillah, "Economic and Legal Dimensions of Collateral Existence in Modern Mudhârabah Contracts: Understanding the Relationship between Risk Management, National Law, and Contemporary Fiqh," *Al-Manahij: Jurnal Kajian Hukum Islam*, November 25, 2022, 223–38, https://doi.org/10.24090/mnh.v16i2.6860.

sharia payment service, LinkAja Syariah, was launched by a state-owned company.[8] The presence of this digital wallet has largely replaced the need to carry a physical wallet. A wallet that can store all user payment information safely and practically. The use of digital wallets is also a potential advantage for companies to collect consumer data.[9] The more a company knows about the buying habits of its customers, the more effective it will be in marketing to its customers.[10] Conversely, on the consumer side, there is a loss, namely the potential loss of privacy if it is misused.[11] The widespread use of digital wallets today sometimes makes people not pay attention to how their personal data is when registering to become digital wallet users.

Several studies reveal the importance of paying attention to consumer data protection. This is in line with research conducted by Spiekermann, where it stated that until now there is still uncertainty about the protection of privacy and personal data in the digital era.[12] In addition, Rauschnabel and Ro discussed in their article related to the abuse of data protection in e-hailing transportation, it stated that sometimes drivers easily take advantage of consumers' personal data for matters outside the service process by sending threats because they do not accept the rating they receive given by consumers to drivers.[13] Meanwhile, regarding Islamic digital payments, Razali et al show that the use of e-wallets as a medium for electronic transactions to purchase products or services is in line with the *hifz mal* concept.[14] However, Zulkefli et al argues that e-wallet implementation can involve several transactions and concepts that can trigger Sharia problems. Therefore, it is necessary to study the concept and its application by looking at the requirements of Sharia principles regarding the use of e-wallets for Muslim users.[15]

Although there were numerous studies conducted related to the issue of sharia digital payment and consumer data protection. However, the study that particularly discusses on the issue of sharia compliance and the consumer data protection of sharia e-wallet or Islamic digital payment is difficult to be found primarily in the context of Indonesia where the authors considered it important to be discussed and examined in order to provide a comprehensive analysis on the issue and for the sake of development of existing knowledge in sharia digital payment. Based on the aforementioned background, in order to provide a novel study on such an issue, this paper seeks to examine how the Indonesian government regulates data protection for Islamic e-wallet consumers. Furthermore, it looks into the current practice of Islamic digital payments, focusing on the issues of data protection and consumer privacy. Besides, it also observes the Islamic perspective on the use of digital payment whether or not the current practice has complied with the Fatwa of the National Sharia Council-Indonesian Ulema Council (DSN-MUI).

---

8 Muryanto, Kharisma, and Nugraheni, "Prospects and Challenges of Islamic Fintech in Indonesia: A Legal Viewpoint."

9 Shasha Teng and Kok Wei Khong, "Examining Actual Consumer Usage of E-Wallet: A Case Study of Big Data Analytics," *Computers in Human Behavior* 121 (2021): 106778.

10 Su Jung Kim, Rebecca Jen-Hui Wang, and Edward C Malthouse, "The Effects of Adopting and Using a Brand's Mobile Application on Customers' Subsequent Purchase Behavior," *Journal of Interactive Marketing* 31 (2015): 28–41.

11 Yosra Miaoui, Noureddine Boudriga, and Ezzeddine Abaoub, "Economics of Privacy: A Model for Protecting against Cyber Data Disclosure Attacks," *Procedia Computer Science* 72 (2015): 569–79.

12 Sarah Spiekermann et al., "The Challenges of Personal Data Markets and Privacy," *Electronic Markets* 25, no. 2 (2015): 161–67.

13 Philipp A Rauschnabel and Young K Ro, "Augmented Reality Smart Glasses: An Investigation of Technology Acceptance Drivers," *International Journal of Technology Marketing* 11, no. 2 (2016): 123–48.

14 Mastura Razali et al., "Maqasid Shariah HIFZ MAL in E-Wallet Application.," *Islamiyyat: International Journal of Islamic Studies* 43, no. 1 (2021).

15 Adlin Zulkefli, Hanum Rusmadi, and Akhtarzaite Abdul Aziz, "Application of E-Wallet: A Preliminary Analysis from the Shariah Perspective: Taṭbīq al-Muḥaffaḍah al-Elektrūniyyah: Taḥlīl Ūlā min Manḍūr al-Syarīʿah al-Islamiyyah," *International Journal of Fiqh and Usul Al-Fiqh Studies* 3, no. 2 (2019): 98–105.

The study uses normative research methods to examine the regulatory framework related to data protection in Islamic e-wallets in Indonesia. This study uses the case approach, statutory approach, and conceptual approach. The data studied consisted of primary sources, secondary sources, and tertiary sources. Primary sources include applicable laws and regulations. While secondary sources include scientific articles from reputable journals, research results, books, and results of conferences or seminars. Furthermore, tertiary sources are taken from legal dictionaries and encyclopedias related to the topic of discussion. Furthermore, a number of data and facts that have been collected will be identified and systematized according to the object of the problem under study. Furthermore, a series of data and facts will be analyzed and studied systematically in a descriptive-qualitative manner with several approaches that have been selected.

E-Wallet in Islamic Perspective

A digital wallet called a "e-wallet" can be used to conduct authorized, quick, secure, and integrated transactions.[16] In general, e-wallets are described as server-based programs and the usage procedure necessitates a connection with the publisher first. E-wallets are a type of financial technology (fintech) designed to make transactions easier.[17] In Indonesia, e-wallets are frequently used for a variety of activities, including paying for power, multi-finance installment loans, credit or data packages, and other transactions that can be completed using e-wallets.

Through the National Non-Cash Movement (GNNT) campaign, Bank Indonesia (BI) has urged the public to use cashless payment methods since 2014.[18] E-wallet usage has increased substantially during the epidemic period and has seen significant developments in Indonesia. PT Dompet Anak Bangsa (GoPay), PT Espay Debit Indonesia Koe (Dana), PT Visionet Internasional (OVO), and PT Fintek Karya Nusantara (LinkAja) are among the registered organizations issuing electronic money that have gained official licenses in 2020, according to BI (Bank Indonesia).[19]

In the Islamic perspective, e-wallets are essentially lawful as long as they comply with Allah's provisions, namely that they do not contain usury, gharar, maysir, tadlis, risywah, and israf, and that there is no argument from the Quran and Hadits against them.[20] Thus, in the Islamic perspective, the law of e-wallets is permitted because the creation of e-wallets serves to expedite transactions and provide convenience for humans. Furthermore, it is emphasized that Islamic electronic money is electronic money that complies with sharia principles in accordance with the Fatwa of the National Sharia Council-Indonesian Ulema Council No: 116/DSN-MUI/IX/2017 Concerning Sharia Electronic Money. A wadi'ah or qardh contract governs the relationship between the electronic money issuer and the holder. Sharia-compliant e-wallets are ones that do not violate any laws. Sharia-based

[16] Md Mahmudul Alam, Ala Eldin Awawdeh, and Azim Izzuddin Bin Muhamad, "Using E-Wallet for Business Process Development: Challenges and Prospects in Malaysia," *Business Process Management Journal*, 2021.

[17] Bob Foster, Ratih Hurriyati, and Muhamad Deni Johansyah, "The Effect of Product Knowledge, Perceived Benefits, and Perceptions of Risk on Indonesian Student Decisions to Use E-Wallets for Warunk Upnormal," *Sustainability* 14, no. 11 (2022): 6475.

[18] Dini Safitri and Martomu Buttu Nainggolan, "Implementation of Campaign Strategy For National Non Cash Movement From Bank of Indonesia," in *3rd International Conference on Transformation in Communications 2017 (IcoTiC 2017)* (Atlantis Press, 2017), 13–17.

[19] Hendy Mustiko Aji, Izra Berakon, and Maizaitulaidawati Md Husin, "COVID-19 and e-Wallet Usage Intention: A Multigroup Analysis between Indonesia and Malaysia," *Cogent Business & Management* 7, no. 1 (2020): 1804181.

[20] Muhammad Aunurrochim and Muhammad Adib bin Saharudin, "E-Wallet: A Study On Contracts Involved Within Its Operational Mechanism," *Journal of Fatwa Management and Research*, 2021, 1–16.

e-wallets are therefore required because in practice, traditional e-wallets still include items that are against sharia principles.[21]

According to the Fatwa of the National Sharia Council-Indonesian Ulema Council No: 116/DSN-MUI/IX/2017 Concerning Sharia Electronic Money, the nominal amount of electronic money in the issuer must be placed in the sharia bank as opposed to conventional e-wallets, where the funds that settle are kept in conventional banks. Additionally, if the contract used in the e-wallet is a qardh contract, as is the case with most traditional e-wallets, it can contain usury even if cashback is authorized as long as it is used for benefit.[22] As of now, Indonesia only has one sharia-based e-wallet, Linkaja Syariah, which was launched on April 14, 2020. Following the publication of DSN-MUI Fatwa No. 116/DSN-MUI/IX/2017, Linkaja Syariah has been issued a DSN-MUI certificate. Because it forgoes usury, gharar, maysir, tadlis, risywah, and israf as well as accumulated balances in sharia banks, this sharia-based Linkaja is also regarded as adhering to sharia norms. Furthermore, it is envisaged that there would be a large number of e-wallets that are based on sharia, as these can comfort Muslims because they follow Islamic laws and values.

Sharia Digital Economy Innovation: Prospectives and Challenges

Digital payments, held by banks and start-up enterprises, are rapidly evolving in Indonesia. According to the 2018 Fintech survey performed by Daily Social and Financial Services Authority (OJK), Go-Pay and OVO are the most popular e-payment services in Indonesia. According to the study results, 79.4% of the 1,419 respondents used Go-Pay, while 58.4% utilized OVO. In 2018, the total number of Go-Pay transactions hit IDR 87 trillion. Meanwhile, OVO claimed a 400% rise in total users and a 75-fold increase in total transactions, or around one billion transactions.[23]

The public is attracted to the existence of digital payments because of the comfort and convenience they offer. Being a customer of the bank might benefit from the allure of digital payments in the banking field. Through the provision of low-cost money, this tool helps banks increase earnings. Nevertheless, Indonesia still has extremely few of these facilities. The presence of sharia digital payments could be a solution to lower the cost of funds for sharia banking,[24] making it clear that the Indonesian sharia banking sector needs and must offer this service to its customers. In addition, sharia-based digital payments are certainly required to fulfill the needs of the Muslim community, which composes 87% of Indonesia's total population.

In order to realize this sharia digital payment, the National Sharia Economy and Finance Committee (KNEKS) held a series of discussion events with stakeholders on March 18 and 29, 2019 that included Bank Mandiri Syariah, BNI Syariah, BRI Syariah, and BTN Syariah. In addition, a meeting with PT Finarya, the organization in charge of overseeing State-Owned Enterprises's sole digital payment system, LinkAja, was also held on March 22, 2019. KNEKS, Sharia Banks, and LinkAja are expected to work together to develop a sharia-based digital payment application supported by

[21] Mohd Zakhiri Md Noor et al., "Legal Issues In E-Wallet Practices," *Uum Journal Of Legal Studies* 12, no. 2 (2021): 229–52.
[22] Nafis Alam, Lokesh Gupta, and Abdolhossein Zameni, *Fintech and Islamic Finance* (Springer, 2019).
[23] Yulius Koesworo, Ninuk Muljani, and Lena Ellitan, "Fintech in the Industrial Revolution Era 4.0," *International Journal of Research Culture Society* 3, no. 9 (2019): 53–56.
[24] Nafis Alam, Lokesh Gupta, and Abdolhossein Zameni, "Emergence of Shariah-Tech and Its Landscape," in *Fintech and Islamic Finance* (Springer, 2019), 63–79.

Sharia Banks functioning as Custodian Banks.[25] This partnership is anticipated to enhance Islamic financial services and support in the financial sector's development of a halal lifestyle in Indonesian society.

The aforementioned prospect is supported by the fact that the use of digital wallet applications (e-wallets) has also become part of the lifestyle of the millennial generation and generation Z in Indonesia. Thus, slowly, the hope for a cashless society is getting brighter. Ipsos Media research explains that as much as 68 percent of this generation use a digital wallet at least once a week. This usage is dominated by online transportation service payment transactions by 40 percent and food and beverage purchases by 32 percent. The research involved 500 respondents in five major cities in Indonesia, namely Jakarta, Semarang, Yogyakarta, Palembang, and Manado. Ipsos said that there are four main digital wallet players in Indonesia, namely Go-Pay, OVO, Dana, and LinkAja. Go-Pay, which is a pioneer in the industry, is the brand most widely known by the younger generation, namely 58 percent, then OVO 29 percent, Dana 9 percent, and LinkAja 4 percent.[26]

In order to attract the consumers, digital wallets must first entice consumers to use them through a variety of promotions, but as time goes on, users come to trust and feel safe utilizing the system.[27] As a result, it is possible to anticipate that consumers of digital wallets will keep increasing even while promotional expenses would decline. The majority of users will still make transactions even if there are no promotions because they consider it practical and safe, so they do not need to carry a lot of money and it is safe because it is not easy to steal. This means that digital wallet companies no longer need to burn money to create loyal customers. The viability of the business will be built on these loyal consumers or organic users. They will serve as a solid indicator or filter for businesses to determine if the services they employ are appropriate or not, in addition to being the foundation of revenue. Menne et al then offers another method for e-wallet companies to attract more devoted clients without spending more money. They contend that businesses must exercise creativity to pamper customers through the creation of innovative service ideas. According to Menne's research, e-wallet providers can provide customers new functionalities that are not currently available.[28] Ipsos Media research claimed that while 36 percent of generation Z preferred installment payment alternatives, 48 percent of millennials desired a digital wallet that was linked to savings.[29] This generation can easily assimilate new technologies. This generation thus has the capacity to influence change in the digital financial sector in addition to being the largest section.

On the other hand, according to Buil et al, they argued that the incentives offered in the form of a variety of promotions, discounts, and cashback in order to attract new customers are insufficient to develop loyal consumers.[30] In order to tacke this, Gobble contends that businesses should create

[25] Firsty Izzata Bella and Nadya Fira Efendi, "Strengthening the Islamic Digital Payment System Through Sharia Electronic Wallet (E-Wallet)," *El Dinar: Jurnal Keuangan Dan Perbankan Syariah* 9, no. 2 (2021): 94–107.

[26] Riyanti Teresa Tedja, Yanti Tjong, and Kevin Deniswara, "Factors Affecting The Behavioral Intention of E-Wallet Use during Covid-19 Pandemic in DKI Jakarta," in *2021 International Conference on Information Management and Technology (ICIMTech)*, vol. 1 (IEEE, 2021), 574–79.

[27] Hendy Mustiko Aji and Wiwiek Rabiatul Adawiyah, "How E-Wallets Encourage Excessive Spending Behavior among Young Adult Consumers?," *Journal of Asia Business Studies*, 2021.

[28] Firman Menne et al., "Optimizing the Financial Performance of Smes Based on Sharia Economy: Perspective of Economic Business Sustainability and Open Innovation," *Journal of Open Innovation: Technology, Market, and Complexity* 8, no. 1 (2022): 18.

[29] Ipsos, "Penelitian Ipsos: Evolusi Dompet Digital Menuju Keberlanjutan Bisnis," 2020, https://www.ipsos.com/sites/default/files/ct/news/documents/2020-02/ipsos_-_press_release_-_indonesian.pdf.

[30] Isabel Buil, Leslie De Chernatony, and Eva Martínez, "Examining the Role of Advertising and Sales Promotions in Brand Equity Creation," *Journal of Business Research* 66, no. 1 (2013): 115–22.

products in accordance with ecosystems that are close to daily needs,[31] particularly in the financial industry where ecosystems and products must be developed constantly. Financial requirements take on more significance and unavoidably require cooperation. This serves as a launchpad for the financial industry's growth. Additionally, there are numerous prospects for this digital wallet to enable micro but considerable financial service transactions, making it a significant industry and the future of financial institutions.

Apart from all the prospects and advantages of using e-wallets, there are also challenges and threats that all parties need to pay attention to. Teng and Khong explained that consumer transaction data is a strategic key factor for optimizing the digital wallet business. According to them, this digital data can become a map of financial system services in the future. Individual data is something that is very strategic and it determines how the life cycle of financial needs is very important.[32] This data is key for the wider financial sector, including insurance and investment. Forbes writes that in 2022, data and artificial intelligence will become a trend for financial technology companies.[33] Data that contains a history of customer behavior can provide convenience to the marketing function which will become more specific and personal. On the other hand, the use of personal data for marketing analysis is considered to violate privacy because it is used without consumer consent. Responding to this, Jin et al stated, the issue of data privacy will be a major issue in the future, particularly regarding national security and crime.[34] Thus, according to Poltak, the government must also be present to guarantee the confidentiality of each citizen's data because the digital financial sector is a business that depends on trust.[35] The financial sector can only operate based on trust, so the key is how to treat consumer data.

Vulnerability to Cybercrime: The Absence of Pertinent Legislation

Technological developments that are increasingly advanced, both devices and their utilization, provide positive value to people's lives such as the presence of sharia e-wallets. Sharia e-wallet is a program service that has the function of archiving and monitoring user online shopping information, such as user login data, passwords, shipping addresses, and information about user credit cards. With the existence of a sharia e-wallet, of course, it will make it easier for everyone when they want to make transactions. Technology does not only offer advantages by facilitating people's lives, but also has weaknesses, namely making it easier for criminals to commit crimes. Over time, the forms of crime are increasingly diverse. Technological development is one of the factors that can trigger crime. Along with the development of technology, the types of crime also developed and varied. Many new crimes have sprung up along with technological developments, especially internet technology. Cybercrime is a form of crime caused by technological developments.[36] This crime has become an

[31] MaryAnne M Gobble, "Charting the Innovation Ecosystem," *Research-Technology Management* 57, no. 4 (2014): 55–59.
[32] Teng and Khong, "Examining Actual Consumer Usage of E-Wallet: A Case Study of Big Data Analytics."
[33] Forbes, "Artificial Intelligence Will Become An Indispensable, Trusted Enterprise Coworker," *Forbes*, November 2022, https://www.forbes.com/sites/forrester/2022/11/10/artificial-intelligence-will-become-an-indispensable-trusted-enterprise-coworker/?sh=4f66eb20d686.
[34] Xiaolong Jin et al., "Significance and Challenges of Big Data Research," *Big Data Research* 2, no. 2 (2015): 59–64.
[35] Marijn Janssen and Jeroen van den Hoven, "Big and Open Linked Data (BOLD) in Government: A Challenge to Transparency and Privacy?," *Government Information Quarterly* (Elsevier, 2015).
[36] Adam M Bossler and Tamar Berenblum, "Introduction: New Directions in Cybercrime Research," *Journal of Crime and Justice* (Taylor & Francis, 2019).

international concern. Cybercrime is one of the dark sides of technological progress which has a negative impact on every area of modern life today. In essence, Cybercrime is an illegal action carried out by using the internet, technological sophistication, and telecommunications in carrying out a crime.

According to David S. Wall, the term 'cybercrime' has come to represent danger and insecurity online and broadly defines crimes that take place there.[37] E-wallet user data theft cases might happen as a result of scams or phishing attacks by criminals. In this instance, it might be said that the person who perpetrated the data breach committed a crime, necessitating the application of criminal law. Public law includes criminal law, which is described as laws that are acts of legal subjects that specify what people are allowed and not allowed to do as well as the consequences for doing so. The legality concept, according to which the perpetrator of an act may face penalties depending on the relevant written regulations, is the foundation of the Indonesian legal system for determining whether an act qualifies as a crime. In Article 1(1) of the Penal Code, which is currently in effect, the legality concept is spelled out in explicit terms. These crimes typically begin with phishing, where the attackers trick the victim into giving them their One Time Password (OTP) so they can quickly access the victim's e-wallet account.

Phishing is the deceptive practice of pretending to be a reliable website in electronic interactions in order to steal sensitive data, such as usernames, passwords, and credit card numbers. Phishing frequently involves directing the user to enter website login information via email or instant messaging, while it has also frequently used telephone contact.[38] According to Indonesian law, the perpetrator's actions in forcibly accessing the victim's account can be considered a violation of Article 30 paragraphs (1) and (2) of Law No. 11 of 2008 concerning Information and Electronic Transactions, which states that anyone who intentionally accesses another person's computer or electronic system in any way while acting illegally or without authorization is in violation of the law. Then, in paragraph (2), it is stated that anybody who purposefully accesses computers and/or electronic systems without authorization or in violation of the law in any way with the objective of collecting electronic documents and/or information. In addition, Article 46 stipulates that violator of Article 30 paragraphs (1) or (2) may be sentenced to a maximum of 7 years in jail and/or a maximum fine of IDR 700 million.[39]

Consumer Data Protection: What Do The Laws Say?

Privacy rights include the protection of personal information, which indicates that one's right to privacy includes the freedom from all types of intrusion into one's private life. Personal rights also include the freedom to communicate with others without being spied on. Additionally, the right to privacy includes the freedom from restrictions on who can access data and information about a person's private life. As a result, if someone's personal information is used without their consent,

[37] David S Wall, "Crime, Security and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and Its Implications for Regulation and Policing," *Security and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and Its Implications for Regulation and Policing (July 20, 2017)*, 2017.

[38] Brij B Gupta, Nalin A G Arachchilage, and Kostas E Psannis, "Defending against Phishing Attacks: Taxonomy of Methods, Current Issues and Future Directions," *Telecommunication Systems* 67, no. 2 (2018): 247–67.

[39] Gomgom Siregar and Muhammad Ridwan Lubis, "Juridical Analysis of Religious Blasphemy Crimes through Smartphone Applications Based on the Information and Electronic Transactions (Ite)," *Journal of Contemporary Issues in Business and Government* 27, no. 2 (2021): 1006–12.

that person's rights have been infringed, and they may now initiate a lawsuit to recover their losses.[40] According to Article 26 paragraph (1) of Law No. 19 of 2016 concerning Amendments to Law Number 11 of 2008 on Information and Electronic Transactions, which refers to the Information and Electronic Transactions Act (IET Act) and its amendments, the use of any information via electronic media that relates to a person's personal data must be done with that person's consent, unless specified otherwise by laws and regulations.

Furthermore, the Indonesian Parliament recently passed a special law that addresses the protection of personal data. On October 17, 2022, President Joko Widodo signed Law Number 27 of 2022 Concerning Protection of Personal Data (PDP Act). The objective of this initiative is to safeguard the personal information of users that is under the control of operators of electronic systems and to stop irresponsible people from abusing it. The Indonesian Parliament has been working on the PDP Act since 2016. According to Johnny G. Plate, the Minister of Communication and Information, the passage of the Law heralded a new era in the management of people's personal data, particularly in relation to digital affairs.[41] According to Article 1 Point 1 of the PDP Act, personal data are details about people who can be directly or indirectly identified, either alone or in combination with other information, using electronic or non-electronic means. Furthermore, it is stated in Article 1 Paragraph 2 that the protection of personal data refers to all measures taken to safeguard personal data in the personal data processing sequence in order to uphold the constitutional rights of individuals whose personal data are being processed. In accordance with Article 4 of the Law, public personal data are divided into two categories: generic information that may be shared and specific information that, if given without authorization, may result in legal repercussions. Full name, gender, nationality, religion, and marital status are among the general information. Health data, biometric and genetic data, criminal histories, child data, financial data, and other data in line with laws and regulations are examples of particular data. The PDP Act controls, among other things, the issue of criminal threats made against behaviors that are forbidden when utilizing personal data, such as stealing, disseminating, and exploiting other people's personal data, including misrepresenting personal data. According to Articles 67 to 69 of the Personal Data Protection Law, this behavior is punished by a term of imprisonment of up to 4 years and/or a fine of billions of rupiah. The PDP Act also governs activities that are forbidden in the use of personal data. For instance, it is forbidden to use or disclose someone else's personal information. Additionally, it is forbidden to injure others by gathering personal information that is not one's own. Articles 65 and 66 of the Personal Data Protection Law go into depth on how these practices are prohibited.

Although the PDP Act ushers in a new era of personal data management in Indonesia, it is like a breath of "fresh air." The PDP Act, on the other hand, is not final. In fact, the legislation assigns the government with some "task." The PDP Act requires that personal data security be provided by the government. The government is challenged to keep bringing up the need for all sharia e-wallet operators to enhance security measures (firewalls and encryption), adhere to obligations, and secure the personal data they manage in both general and specific ways as a condition of compliance.[42] This

[40] William A Parent, "Privacy, Morality, and the Law," in *Privacy* (Routledge, 2017), 105–24.
[41] Muhammad Firdaus, "A Review of Personal Data Protection Law in Indonesia" (OSF Preprints, 2020), file:///C:/Users/rizaldyanggriawan/Downloads/Muhammad Firdaus_A Review of Personal Data Protection Law in Indonesia (1).pdf.
[42] Neetu Kumari and Jhanvi Khanna, "Cashless Payment: A Behaviourial Change to Economic Growth," *Qualitative and Quantitative Research Review* 2, no. 2 (2017).

means that if there is a data breach or event involving personal information, it will be determined whether the operator complied with the PDP Act or not. If not, the operator will face a range of PDP Act-mandated punishments, including administrative penalties, incarceration, fines, and criminal penalties.

Additionally, in accordance with Article 1(1) of the Regulation No. 20 of 2016 on the Protection of Personal Data in Electronic Systems issued by the Minister of Communication and Information, Personal Data is defined as particular individual data that is stored, maintained, and protected by confidentiality as well as truthfulness. Legal protection, in the opinion of Philipus M. Hadjon, comprises both the protection of dignity and the defense of human rights that are related to a legal matter.[43] The protection of the larger population is the goal of the law. The best weapon for controlling social change is the law, which allows for existing changes to also develop the nation and state. Although the goal of the law in the case of electronic transactions is to protect consumers, laws can provide solutions for utilizing science and technology to the fullest extent feasible for the benefit and survival of humanity. Since consumers are the general public, defending customers also means defending society. One way to give users of Islamic e-wallets legal protection is to maintain the security of their personal information. The general population is given legal protection so they can exercise all of the legal rights that have been granted to them. It defends human rights when they are trampled upon by others. The right to privacy may also extend to data about an individual that is obtained and used by others, according to the idea of privacy from data about a person. This notion highlights the significance of preserving the privacy of personal information as a symbol of that right.[44]

Two different sorts of legal protection preventive and repressive can be offered, according to Philipus M. Hadjon. When receiving and obtaining user data, processing, analyzing, storing, and displaying that data, as well as when storing and displaying that data after it has been received, the provider must protect personal data. If there is an interest in disseminating and destroying the user's personal data, the provider must ensure the security of the data process.[45] This is further supported by the explanation of Article 26 of the IET Act, which states that a person's right to their personal information. The rights mentioned in this article include the right to data confidentiality, the right to file complaints in the event that electronic system operators fail to protect the privacy of personal data, and the right to access, change, or update their personal data without interfering with the system for managing personal data. It is necessary to seek the consent and approval of the individual concerned before using any information collected by electronic means that relates to that person's personal data.[46] A party who disobeys this rule may be held liable for the damages that ensue. According to Article 26 of the IET Act, it is unlawful to engage in activities that include the gathering, use, or disclosure of a person's personal information because that person's right to privacy includes the choice of whether or not to disclose that information. Data protection guarantees are governed

[43] Wilma Silalahi, "Violations of Human Rights by Criminal Acts of Misappropriation of Social Assistance Funds," in *2nd International Conference on Law and Human Rights 2021 (ICLHR 2021)* (Atlantis Press, 2021), 514–24.
[44] Neil M Richards, "The Dangers of Surveillance," *Harvard Law Review* 126, no. 7 (2013): 1934–65.
[45] Dinda Dinanti et al., "Politics of Law for the Protection of Debtors as Consumers in Fintech Based Loaning Services," *Unnes Law Journal* 6, no. 2 (2020): 427–44.
[46] Alyson Leigh Young and Anabel Quan-Haase, "Privacy Protection Strategies on Facebook: The Internet Privacy Paradox Revisited," *Information, Communication & Society* 16, no. 4 (2013): 479–500.

by Article 15 paragraph (1) of the IET Act, which mandates that every electronic system operator maintain platform security. Electronic system users are required to maintain the confidentiality of personal data that is obtained, collected, processed, and analyzed as well as to protect personal data and documents containing personal data from misuse.

To ensure the effectiveness and security of the payment system, Bank Indonesia (BI), which is responsible for monitoring operations related to the payment system in Indonesia, must monitor payment transactions using established policies.[47] This can be achieved by keeping an eye on current systems while they are still in the design stages and by evaluating how each operator will carry out payment system operations based on compliance with the objectives, security, and efficiency of each payment system. In order to effectively implement a payment system in Indonesia that is characterized by the principles of efficiency, fluidity, security, and reliability, Bank Indonesia Regulation (PBI) Number 18/40/PBI/2016's Article 20 Paragraph (2) contains provisions regarding the application of information system security standards. The implementation of a policy requiring the party operating as an operator to first seek a permit from BI by completing the general requirements and eligibility aspects following the adoption of PBI No. 20/6/PBI/2018 concerning Electronic Money. According to Article 34 of the PBI, operators must follow information system security requirements and put consumer protection, anti-money laundering, and anti-terrorist financing principles into practice in order to give customers legal assurance.

Furthermore, OJK's role as a custodian in the financial services sector will protect consumers from financial service business operators that are regarded to be harmful to consumers' interests. Protecting the interests of consumers and the public so that consumers feel comfortable when using financial services is one of the key aims of the OJK, as stated in Article 4 of Law No. 21 of 2011 on the Financial Services Authority.[48] Since OJK is an entity with the capacity to oversee company activities in the financial services sector, it must be able to protect the financial services that clients utilize when they deposit money or use services provided by financial service institutions. OJK states in OJK Circular Letter Number 18/SEOJK.02/2017 Concerning Information Technology Governance and Risk Management in Information Technology-Based Money Lending Services that the following categories of personal information must be kept secure: user names, residential addresses, identity cards, dates of birth, emails, IP addresses, user's phone numbers, account numbers, the name of the user's biological mother, credit card numbers, and digital identity information. However, there are still a lot of people who receive information but are unable to properly interpret and process it; as a result, a lot of people continue to look at erroneous data.

Preventive actions must be taken to protect against negative effects and technology misuse in order to keep personal data in e-wallets secured. The Ministry of Communication and Information Technology (Kominfo) asserts that providing the OTP code at random will not stop cybercrime from occurring. The OTP code is the most important component of modern technology security since it functions like a house key and cannot be distributed to just anybody. One must be cautious if they get an OTP code request from an official institution or e-wallet provider by SMS, phone call, email, or even

[47] Reka Dewantara and Moch Munir, "Supervision of Banking Institutions in Achieve Sound Banking in Indonesia," *JL Pol'y & Globalization* 41 (2015): 97.
[48] Kevin Davis, Rodney Maddock, and Martin Foo, "Catching up with Indonesia's Fintech Industry," *Law and Financial Markets Review* 11, no. 1 (2017): 33–40.

chat, as legitimate institutions never do so.[49] In addition, Zingerle and Kronman also urged people to be on the lookout for fraudulent phone forwarding schemes and fake websites.[50] Thus, it is essential to contact the appropriate m-banking or electronic money call center for complaints and processing, then reporting the incident to the appropriate authorities, including Bank Indonesia, the Police, OJK, and associated organizations to conduct reports and investigations. In addition to refraining from providing arbitrary OTP codes, individuals can raise their awareness of the significance of personal data protection in order to lower the frequency of cybercrime.[51] Data security awareness among the public will help to lessen the community's concern with cybercrime. Personal data security is a problem that can never be solved if preventative and punitive measures are implemented but people choose to disregard them.[52]

Conclusion

E-wallet is essentially acceptable in Islam as long as it follows sharia principles, meaning it does not contain usury, *gharar, maysir, tadlis, risywah,* or *israf*, and there is no evidence from the Quran or Hadith to argue against it. The National Sharia Council-Indonesian Ulema Council's Fatwa No. 116/DSN-MUI/IX/2017 Concerning Sharia Electronic Money regulates the adherence of Islamic rules and principles, particularly as they relate to the use of Sharia e-wallets. One of the differences, according to the Fatwa, is that unlike conventional e-wallets where the funds that settle are maintained in conventional banks, the nominal amount of electronic money issued by an issuer must be placed in a sharia bank. Furthermore, given that the number of Muslim society's enthusiasm on halal lifestyle and the increasing number of e-wallet users, eventually the first sharia-based e-wallet in Indonesia, Linkaja Syariah, was launched on April 14, 2020, after a series number of meetings between KNKS, Sharia Banks, and PT. Finarya. Moreover, Linkaja Syariah was also granted a DSN-MUI certificate following the issuance of DSN-MUI Fatwa No. 116/DSN-MUI/IX/2017.

However, along with all the opportunities and benefits of using sharia e-wallets, there are also risks and threats that need to be addressed by every stakeholder, particularly when it comes to data security. Moreover, crime types evolved and varied as well. Many new crimes have emerged alongside technical advancements, particularly internet technology. Besides, personal information also plays a crucial strategic role in determining how the life cycle of financial needs should be managed. The marketing function can benefit from data that has a history of customer behavior as it becomes increasingly specialized and personalized. In addition, since it is utilized without the consumer's agreement, the use of personal data for marketing analysis is regarded as a violation of privacy. Nevertheless, generally speaking, the current regulatory framework provided by Government, Parliament, Bank Indonesia, and Financial Services Authority has thoroughly addressed this issue from upstream to downstream, beginning with how to obtain personal data, managing personal data,

[49] Rahel Octora, P Lindawaty S Sewu, and Jason Arnold Sugiono, "Regulation on Electronic System Security for E-Wallet in Order to Protect Consumers from Financial Loss Due to Cyber Fraud Based on Indonesian Law," *International Journal of Social Science And Human Research* 4, no. 09 (2021).

[50] Andreas Zingerle and Linda Kronman, "Internet Crime and Anti-Fraud Activism: A Hands-On Approach," in *Security and Privacy Management, Techniques, and Protocols* (IGI Global, 2018), 322–36.

[51] Lennon Y C Chang and Nicholas Coppel, "Building Cyber Security Awareness in a Developing Country: Lessons from Myanmar," *Computers & Security* 97 (2020): 101959.

[52] Sinchul Back and Rob T Guerette, "Cyber Place Management and Crime Prevention: The Effectiveness of Cybersecurity Awareness Training Against Phishing Attacks," *Journal of Contemporary Criminal Justice* 37, no. 3 (2021): 427–51.

and in the event of a breach of personal data, including the imposition of penalties in the form of imprisonment and fines as these provisions are stipulated in several forms of legislations. In addition, PDP Act particularly requires the government to provide personal data security. As total compliance, the government is tasked to continuously oversee and remind all sharia e-wallet operators to strengthen security systems, comply with regulations, and secure the personal data they manage, both general and specific.

References

Aji, Hendy Mustiko, and Wiwiek Rabiatul Adawiyah. "How E-Wallets Encourage Excessive Spending Behavior among Young Adult Consumers?" *Journal of Asia Business Studies*, 2021.

Aji, Hendy Mustiko, Izra Berakon, and Maizaitulaidawati Md Husin. "COVID-19 and e-Wallet Usage Intention: A Multigroup Analysis between Indonesia and Malaysia." *Cogent Business & Management* 7, no. 1 (2020): 1804181.

Alam, Md Mahmudul, Ala Eldin Awawdeh, and Azim Izzuddin Bin Muhamad. "Using E-Wallet for Business Process Development: Challenges and Prospects in Malaysia." *Business Process Management Journal*, 2021.

Alam, Nafis, Lokesh Gupta, and Abdolhossein Zameni. "Emergence of Shariah-Tech and Its Landscape." In *Fintech and Islamic Finance*, 63–79. Springer, 2019.

———. *Fintech and Islamic Finance*. Springer, 2019.

Aunurrochim, Muhammad, and Muhammad Adib bin Saharudin. "E-Wallet: A Study On Contracts Involved Within Its Operational Mechanism." *Journal of Fatwa Management and Research*, 2021, 1–16.

Back, Sinchul, and Rob T Guerette. "Cyber Place Management and Crime Prevention: The Effectiveness of Cybersecurity Awareness Training Against Phishing Attacks." *Journal of Contemporary Criminal Justice* 37, no. 3 (2021): 427–51.

Bella, Firsty Izzata, and Nadya Fira Efendi. "Strengthening the Islamic Digital Payment System Through Sharia Electronic Wallet (E-Wallet)." *El Dinar: Jurnal Keuangan Dan Perbankan Syariah* 9, no. 2 (2021): 94–107.

Bossler, Adam M, and Tamar Berenblum. "Introduction: New Directions in Cybercrime Research." *Journal of Crime and Justice*. Taylor & Francis, 2019.

Briliana, Vita, and Nurwanti Mursito. "Exploring Antecedents and Consequences of Indonesian Muslim Youths' Attitude towards Halal Cosmetic Products: A Case Study in Jakarta." *Asia Pacific Management Review* 22, no. 4 (2017): 176–84.

Buil, Isabel, Leslie De Chernatony, and Eva Martínez. "Examining the Role of Advertising and Sales Promotions in Brand Equity Creation." *Journal of Business Research* 66, no. 1 (2013): 115–22.

Chang, Lennon Y C, and Nicholas Coppel. "Building Cyber Security Awareness in a Developing Country: Lessons from Myanmar." *Computers & Security* 97 (2020): 101959.

Ciptarianto, Augi, and Yudo Anggoro. "E-Wallet Application Penetration for Financial Inclusion in Indonesia." *International Journal of Current Science Research and Review* 5, no. 2 (2022): 319–32.

Davis, Kevin, Rodney Maddock, and Martin Foo. "Catching up with Indonesia's Fintech Industry." *Law and Financial Markets Review* 11, no. 1 (2017): 33–40.

Dewantara, Reka, and Moch Munir. "Supervision of Banking Institutions in Achieve Sound Banking in Indonesia." *JL Pol'y & Globalization* 41 (2015): 97.

Dinanti, Dinda, Muthia Sakti, Indira Putri Irfani, and Sinta Ana Pramita. "Politics of Law for the Protection of Debtors as Consumers in Fintech Based Loaning Services." *Unnes Law Journal* 6, no. 2 (2020): 427–44.

Firdaus, Muhammad. "A Review of Personal Data Protection Law in Indonesia." OSF Preprints, 2020. file:///C:/Users/rizaldyanggriawan/Downloads/Muhammad Firdaus_A Review of Personal Data Protection Law in Indonesia (1).pdf.

Forbes. "Artificial Intelligence Will Become An Indispensable, Trusted Enterprise Coworker." *Forbes*, November 2022. https://www.forbes.com/sites/forrester/2022/11/10/artificial-intelligence-will-become-an-indispensable-trusted-enterprise-coworker/?sh=4f66eb20d686.

Foster, Bob, Ratih Hurriyati, and Muhamad Deni Johansyah. "The Effect of Product Knowledge, Perceived Benefits, and Perceptions of Risk on Indonesian Student Decisions to Use E-Wallets for Warunk Upnormal." *Sustainability* 14, no. 11 (2022): 6475.

Gobble, MaryAnne M. "Charting the Innovation Ecosystem." *Research-Technology Management* 57, no. 4 (2014): 55–59.

Gupta, Brij B, Nalin A G Arachchilage, and Kostas E Psannis. "Defending against Phishing Attacks: Taxonomy of Methods, Current Issues and Future Directions." *Telecommunication Systems* 67, no. 2 (2018): 247–67.

Hidayatullah, Muhammad Syarif, and Rahmat Fadillah. "Economic and Legal Dimensions of Collateral Existence in Modern Mudhârabah Contracts: Understanding the Relationship between Risk Management, National Law, and Contemporary Fiqh." *Al-Manahij: Jurnal Kajian Hukum Islam*, November 25, 2022, 223–38. https://doi.org/10.24090/mnh.v16i2.6860.

Hinduan, Zahrotur Rusyda, Adilla Anggraeni, and Muhamad Irfan Agia. "Generation Z in Indonesia: The Self-Driven Digital." In *The New Generation Z in Asia: Dynamics, Differences, Digitalisation*. Emerald Publishing Limited, 2020.

Ipsos. "Penelitian Ipsos: Evolusi Dompet Digital Menuju Keberlanjutan Bisnis," 2020. https://www.ipsos.com/sites/default/files/ct/news/documents/2020-02/ipsos_-_press_release_-_indonesian.pdf.

Janssen, Marijn, and Jeroen van den Hoven. "Big and Open Linked Data (BOLD) in Government: A Challenge to Transparency and Privacy?" *Government Information Quarterly*. Elsevier, 2015.

Jin, Xiaolong, Benjamin W Wah, Xueqi Cheng, and Yuanzhuo Wang. "Significance and Challenges of Big Data Research." *Big Data Research* 2, no. 2 (2015): 59–64.

Kim, Su Jung, Rebecca Jen-Hui Wang, and Edward C Malthouse. "The Effects of Adopting and Using a Brand's Mobile Application on Customers' Subsequent Purchase Behavior." *Journal of Interactive Marketing* 31 (2015): 28–41.

Koesworo, Yulius, Ninuk Muljani, and Lena Ellitan. "Fintech in the Industrial Revolution Era 4.0." *International Journal of Research Culture Society* 3, no. 9 (2019): 53–56.

Kumari, Neetu, and Jhanvi Khanna. "Cashless Payment: A Behaviourial Change to Economic Growth." *Qualitative and Quantitative Research Review* 2, no. 2 (2017).

Menne, Firman, Batara Surya, Muhammad Yusuf, Seri Suriani, Muhlis Ruslan, and Iskandar Iskandar. "Optimizing the Financial Performance of Smes Based on Sharia Economy: Perspective of Economic Business Sustainability and Open Innovation." *Journal of Open Innovation: Technology, Market, and Complexity* 8, no. 1 (2022): 18.

Miaoui, Yosra, Noureddine Boudriga, and Ezzeddine Abaoub. "Economics of Privacy: A Model for Protecting against Cyber Data Disclosure Attacks." *Procedia Computer Science* 72 (2015): 569–79.

Muryanto, Yudho Taruno, Dona Budi Kharisma, and Anjar Sri Ciptorukmi Nugraheni. "Prospects and Challenges of Islamic Fintech in Indonesia: A Legal Viewpoint." *International Journal of Law and Management*, 2021.

Noor, Mohd Zakhiri Md, Asmadi Mohamed Naim, Nurul Aini Muhamed, Azrul Azlan Iskandar Mirza, Azuan Ahmad, Shahrul Ridhwan S Ali, and Abdul Rahman A Shukor. "Legal Issues In E-Wallet Practices." *Uum Journal Of Legal Studies* 12, no. 2 (2021): 229–52.

Octora, Rahel, P Lindawaty S Sewu, and Jason Arnold Sugiono. "Regulation on Electronic System Security for E-Wallet in Order to Protect Consumers from Financial Loss Due to Cyber Fraud Based on Indonesian Law." *International Journal of Social Science And Human Research* 4, no. 09 (2021).

Parent, William A. "Privacy, Morality, and the Law." In *Privacy*, 105–24. Routledge, 2017.

Rauschnabel, Philipp A, and Young K Ro. "Augmented Reality Smart Glasses: An Investigation of Technology Acceptance Drivers." *International Journal of Technology Marketing* 11, no. 2 (2016): 123–48.

Razali, Mastura, Nurul'Ain Mohd, Nurhanisah Hadigunawan, and Rafeah Saidon. "Maqasid Shariah HIFZ MAL in E-Wallet Application." *Islamiyyat: International Journal of Islamic Studies* 43, no. 1 (2021).

Richards, Neil M. "The Dangers of Surveillance." *Harvard Law Review* 126, no. 7 (2013): 1934–65.

Safitri, Dini, and Martomu Buttu Nainggolan. "Implementation of Campaign Strategy For National Non Cash Movement From Bank of Indonesia." In *3rd International Conference on Transformation in Communications 2017 (IcoTiC 2017)*, 13–17. Atlantis Press, 2017.

Silalahi, Wilma. "Violations of Human Rights by Criminal Acts of Misappropriation of Social Assistance Funds." In *2nd International Conference on Law and Human Rights 2021 (ICLHR 2021)*, 514–24. Atlantis Press, 2021.

Siregar, Gomgom, and Muhammad Ridwan Lubis. "Juridical Analysis of Religious Blasphemy Crimes through Smartphone Applications Based on the Information and Electronic Transactions (Ite)." *Journal of Contemporary Issues in Business and Government* 27, no. 2 (2021): 1006–12.

Spiekermann, Sarah, Alessandro Acquisti, Rainer Böhme, and Kai-Lung Hui. "The Challenges of Personal Data Markets and Privacy." *Electronic Markets* 25, no. 2 (2015): 161–67.

Tedja, Riyanti Teresa, Yanti Tjong, and Kevin Deniswara. "Factors Affecting The Behavioral Intention of E-Wallet Use during Covid-19 Pandemic in DKI Jakarta." In *2021 International Conference on Information Management and Technology (ICIMTech)*, 1:574–79. IEEE, 2021.

Teng, Shasha, and Kok Wei Khong. "Examining Actual Consumer Usage of E-Wallet: A Case Study of Big Data Analytics." *Computers in Human Behavior* 121 (2021): 106778.

Wall, David S. "Crime, Security and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and Its Implications for Regulation and Policing." *Security and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and Its Implications for Regulation and Policing (July 20, 2017)*, 2017.

Yang, Marvello, Abdullah Al Mamun, Muhammad Mohiuddin, Noorshella Che Nawi, and Noor Raihani Zainol. "Cashless Transactions: A Study on Intention and Adoption of e-Wallets." *Sustainability* 13, no. 2 (2021): 831.

Young, Alyson Leigh, and Anabel Quan-Haase. "Privacy Protection Strategies on Facebook: The Internet Privacy Paradox Revisited." *Information, Communication & Society* 16, no. 4 (2013): 479–500.

Yusup, A, E M Bayuni, Z F Nuzula, Y Haryati, M R N Alfiani, and N A Lesmana. "Halal Industry Certification in Bandung, Indonesia: Opportunities and Challenges." *Islam, Media and Education in the Digital Era*, 2022, 70–81.

Zingerle, Andreas, and Linda Kronman. "Internet Crime and Anti-Fraud Activism: A Hands-On Approach." In *Security and Privacy Management, Techniques, and Protocols*, 322–36. IGI Global, 2018.

Zulkefli, Adlin, Hanum Rusmadi, and Akhtarzaite Abdul Aziz. "Application of E-Wallet: A Preliminary Analysis from the Shariah Perspective: Taṭbīq al-Muḥaffaḍah al-Elektrūniyyah: Taḥlīl Ūlā min Manḍūr al-Syarīʿah al-Islamiyyah." *International Journal of Fiqh and Usul Al-Fiqh Studies* 3, no. 2 (2019): 98–105.