UQUBAH
Journal of Islamic Criminal Law

Uqubah: Journal of Islamic Criminal Law

Vol. 1, No. 1, 2026, 31–51

Reconceptualizing Islamic criminal policy for QRIS payment fraud: Toward an adaptive framework for contemporary digital financial crime

RESEARCH ARTICLE

Muhammad Guntur
Sekolah Tinggi Ilmu Ekonomi Syariah Nahdhatul Ulama Bengkulu, Indonesia

Bahjatun Mahmudah
Al-Azhar University, Cairo, Egypt

Denmas Azkal Basyari Arsyad
Al-Ahgaff University, Mukalla, Yemen

ABSTRACT

The rapid expansion of digital payment systems has generated new forms of financial fraud, including Quick Response Code Indonesian Standard (QRIS) payment manipulation, which threatens property rights, transaction security, and public trust in digital financial systems. This study examines criminal liability for QRIS payment fraud under Indonesian positive law and Islamic criminal law and develops an adaptive framework for Islamic criminal policy. Employing normative legal research, the study uses statutory, conceptual, and comparative approaches to analyze legislation, regulatory instruments, Islamic legal sources, and relevant scholarly literature. The findings demonstrate that QRIS payment manipulation constitutes a *jarīmah ta'zīr* because it entails deception, unlawful appropriation of property, and harm to the public interest. Accordingly, its criminalization and sanctioning may be determined through the discretionary authority of the *ulī al-amr* in accordance with *maslahah* and *maqāsid al-sharī'ah*. The study further finds that Indonesian positive law and Islamic criminal law can operate complementarily in addressing digital payment fraud. On this basis, it proposes an adaptive *ta'zir* framework integrating preventive protection, proportional punishment, restorative recovery, and adaptive governance. The framework extends *ta'zīr* beyond the classification of offences by positioning it as a normative basis for adaptive Islamic criminal policy in responding to emerging forms of contemporary digital financial crime.

CORRESPONDING AUTHOR:

Muhammad Guntur
gunturmuhammad708@gmail.com

KEYWORDS:

Islamic criminal law; QRIS; digital payment fraud; criminal policy.

TO CITE THIS ARTICLE:

Guntur, Muhammad, Bahjatun Mahmudah, and Denmas Azkal Basyari Arsyad. "Reconceptualizing Islamic criminal policy for QRIS payment fraud: Toward an adaptive framework for contemporary digital financial crime." *Uqubah: Journal of Islamic Criminal Law* 1, no. 1 (2026): 31–51. https://jurnal.stain-madina.ac.id/index.php/uqubah/article/3327

Introduction

The digital transformation of payment systems has fundamentally reshaped the landscape of financial transactions while simultaneously introducing new challenges, particularly the growing risk of technology-enabled financial crime.[1] The digitalization of payment systems is no longer viewed merely as a technological innovation. Rather, it has become an integral component of national economic development strategies aimed at improving transaction efficiency, expanding financial inclusion, and strengthening the competitiveness of the digital economy.[2] In Indonesia, this transformation has been realized through the development of the Quick Response Code Indonesian Standard (QRIS), introduced by Bank Indonesia in 2019 as the national standard for QR code-based payment systems. This standardization has successfully integrated diverse payment service providers into a single interoperable ecosystem, thereby facilitating faster and more seamless transactions for both consumers and business actors.[3]

This development has been accompanied by a substantial increase in the adoption of QRIS. According to the Indonesian Payment System Association (ASPI), the number of QRIS users reached approximately 58 million in the third quarter of 2025, representing an increase of approximately 9.4% compared with the corresponding period of the previous year.[4] This sustained growth indicates that QRIS has become one of the most widely adopted digital payment instruments in Indonesia, playing an increasingly central role in the country's day-to-day economic activities.

The increasing adoption of digital payment technologies has also been accompanied by the emergence of various forms of emerging financial crime that exploit system vulnerabilities and inadequate levels of digital literacy among users.[5] One growing form of criminal activity involves QRIS payment manipulation, including the replacement of merchants' legitimate QR codes, the use of fraudulent QRIS codes to redirect payment funds, and the deployment of modified QR codes that lead victims to phishing websites designed to obtain banking credentials. These practices demonstrate that perpetrators no longer rely solely on conventional fraudulent schemes; instead, they exploit public trust in digital payment systems and their associated infrastructure.[6]

The development of these fraudulent schemes has drawn serious attention from Bank Indonesia, the Directorate General of Digital Ecosystem of the Ministry of Communication and Digital Affairs of the Republic of Indonesia (*Kementerian Komunikasi dan Digital Republik*

---

1 Arnesh Telukdarie and Aviksha Mungar, "The Impact of Digital Financial Technology on Accelerating Financial Inclusion in Developing Economies," *Procedia Computer Science* 217 (2023): 670–78, https://doi.org/10.1016/j.procs.2022.12.263.

2 Alfonz Lawrenz Kilay, Bachtiar H. Simamora, and Danang Pinardi Putra, "The Influence of E-Payment and E-Commerce Services on Supply Chain Performance: Implications of Open Innovation and Solutions for the Digitalization of Micro, Small, and Medium Enterprises (MSMEs) in Indonesia," *Journal of Open Innovation: Technology, Market, and Complexity* 8, no. 3 (2022): 119, https://doi.org/10.3390/joitmc8030119.

3 Evan Hamzah Muchtar et al., "Quick Response Code Indonesia Standard (QRIS) E-Payment Adoption: Customers Perspective," *Cogent Business & Management* 11, no. 1 (2024): 2316044, https://doi.org/10.1080/23311975.2024.2316044.

4 Agnes Z. Yonathan, "Nilai Transaksi QRIS Tembus Rp128 Triliun Q3 2025," GoodStats Data, December 12, 2025, https://goodstats.id/article/nilai-transaksi-qris-tembus-rp128-triliun-q3-2025-vPpbG. Accessed 2 August 2026.

5 Vishnu Laxman et al., "Emerging Threats in Digital Payment and Financial Crime: A Bibliometric Review," *Journal of Digital Economy* 3 (2024): 205–22, https://doi.org/10.1016/j.jdec.2025.04.002.

6 Ali Gunawan, Alifia Farrah Fatikasari, and Selva Aisah Putri, "The Effect of Using Cashless (QRIS) on Daily Payment Transactions Using the Technology Acceptance Model," *Procedia Computer Science* 227 (2023): 548–56, https://doi.org/10.1016/j.procs.2023.10.557; Angelique Aurielle Alpaullivarez and Ahmad Nurul Fajar, "Exploring Factors Influencing User Avoidance Behavior Toward QR-Based Payment Scams," *Journal of Information Systems Engineering and Business Intelligence* 12, no. 2 (2026): 458–73, https://doi.org/10.20473/jisebi.12.2.458-473.

Indonesia/Komdigi RI), and the Financial Services Authority (*Otoritas Jasa Keuangan*/OJK), which have periodically issued warnings regarding QRIS misuse and emphasized the importance of verifying merchant identities before completing transactions.[7] Research by Alpaullivarez and Fajar further demonstrates that the increasing adoption of QR-based technologies has created opportunities for the proliferation of QR phishing (quishing) attacks, which are becoming increasingly difficult for ordinary users to detect.[8]

This development has not yet been fully accompanied by the formulation of a dedicated legal framework specifically regulating QRIS-based payment manipulation. Law enforcement efforts continue to rely on a combination of provisions dispersed across several legal instruments, including Law Number 1 of 2023 concerning the Criminal Code (National Criminal Code), Law Number 1 of 2024 on the Second Amendment to the Electronic Information and Transactions Law (ITE Law), and Regulation of Members of the Board of Governors of Bank Indonesia Number 3 of 2025 concerning the implementation of the national QRIS standard. This situation demonstrates that the advancement of digital payment technologies has progressed more rapidly than the development of legal frameworks capable of comprehensively addressing the distinctive characteristics of such crimes. Consequently, criminal liability for these offenses continues to be constructed through the interplay of multiple legal regimes with different regulatory scopes and objectives.

The adaptive nature of Islamic criminal law provides a distinct perspective in responding to the emergence of new forms of criminality. Through the concept of *jarīmah ta'zīr*, Islamic law grants authority to *ulī al-amr* (legitimate authorities) to establish penal policies against any conduct that causes harm (*mafsadah*) and undermines public welfare (*maslahah*).[9] QRIS-based payment manipulation essentially constitutes an unlawful appropriation of another person's property through electronic means, thereby contradicting the prohibition of *akl al-māl bi al-bātil* (consuming or acquiring wealth through wrongful means), the principle of trust (*amānah*), and the objectives of Islamic law in protecting property (*hifz al-māl*).[10] Therefore, the analysis of digital payment crimes cannot be confined solely to the perspective of positive law. It also requires a construction of Islamic criminal law capable of explaining the foundations of criminal liability, the objectives of punishment, and the protection of public welfare through the *maqāsid al-syarī'ah* approach.[11]

Research on QRIS has expanded significantly in recent years; however, existing studies remain predominantly focused on consumer protection, Islamic economic law, payment system security, and positive criminal law perspectives. Ramdhani and Luthfi examined consumer legal protection in QRIS transactions from the perspectives of both positive law and

---

7 Erwin Haryono, "BI Terus Edukasi Masyarakat Dan Pedagang/Merchant Agar Terhindar Dari Upaya Penyalahgunaan QRIS," Bank Indonesia, April 11, 2023, https://www.bi.go.id/id/publikasi/ruang-media/news-release/Pages/sp_259323.aspx; Komdigi RI, "Waspada Modus Kejahatan Lewat QRIS," Direktorat Jenderal Ekosistem Digital, December 30, 2025, https://djed.komdigi.go.id/news/waspada-modus-kejahatan-lewat-qris; OJK Indonesia, "Modus Layanan Keuangan Ilegal Masih Mengintai," X (Twitter), June 25, 2026, https://x.com/ojkindonesia/status/2070046016242606347. All online sources were accessed on 2 August 2026.

8 Alpaullivarez and Fajar, "Exploring Factors Influencing User Avoidance Behavior Toward QR-Based Payment Scams."

9 Muhammad Mawardi Djalaluddin et al., "The Implementation of Ta'zīr Punishment as an Educational Reinforcement in Islamic Law," *Samarah: Jurnal Hukum Keluarga Dan Hukum Islam* 7, no. 1 (2023): 399–417, https://doi.org/10.22373/sjhk.v7i1.15101.

10 Hisam Ahyani et al., "Fraud in the Digital Space: A Comparative Study of Jinayah Fiqh and Indonesian Criminal Law," *Jurnal Hukum Islam* 23, no. 1 (2025): 37–72, https://doi.org/10.28918/jhi.v23i1.02.

11 Imroatul Azizah et al., "Reconstructing Islamic Criminal Liability for Economic Crimes: A Maqasid-Based Framework for Indonesia's Sharia Finance," *El-Mashlahah* 16, no. 1 (2026): 41–64, https://doi.org/10.23971/el-mashlahah.v16i1.11254.

Islamic economic law.[12] Ariyanto et al. investigated the application of the principle of consensualism in QRIS-based electronic payment transactions.[13] Herryani analyzed fraudulent activities involving QRIS barcode counterfeiting from the perspective of positive criminal law, without incorporating an Islamic criminal law framework.[14] Meanwhile, Yalda et al. proposed a blockchain-based solution to prevent QRIS-related fraud,[15] Hamka et al. focused their study on QRIS misuse as a means of personal data theft,[16] while Muttaqin examined the practice of merchant discount rates (MDR) from the perspective of *fiqh muamalah*.[17]

A review of previous studies reveals three primary research gaps. *First*, no existing study has specifically constructed QRIS payment manipulation as a form of contemporary digital payment fraud from the perspective of Islamic criminal law. *Second*, prior research has tended to examine positive law, Islamic economic law, and cybersecurity issues separately, thereby failing to establish an integrated analytical framework for addressing criminal liability. *Third*, the concepts of *jarīmah ta'zīr*, *maqāsid al-syarī'ah*, *hifz al-māl*, and *maṣlaḥah* have not yet been sufficiently utilized as foundations for developing criminal policy responses to digital payment crimes.

Based on these gaps, this study aims to analyze criminal liability for QRIS payment manipulation under both Indonesian positive law and Islamic criminal law, while simultaneously reconstructing an Islamic criminal policy framework for addressing contemporary digital payment fraud. As a conceptual contribution, this study proposes the adaptive *ta'zīr* framework, namely a reconstructed Islamic criminal policy framework that integrates the principles of *ta'zīr*, *maqāsid al-syarī'ah*, and Indonesian positive law to develop a legal response that is preventive, proportionate, restorative, and adaptive to the evolving nature of digital payment crimes.

Methods

This study employs a normative legal research approach (doctrinal legal research) to analyze the legal construction of QRIS-based payment manipulation as a form of digital payment fraud under Indonesian positive law and Islamic criminal law. The study applies statutory, conceptual, and comparative approaches, as proposed by Peter Mahmud Marzuki, while also adopting the characteristics of doctrinal legal research developed by Terry Hutchinson.[18] The analysis is based on primary legal materials consisting of statutory regulations, the Qur'an, hadith, and *fiqh jināyah* literature, supported by secondary legal materials, including books, scholarly

---

12 Fajri Zulia Ramdhani and A Hashfi Lutfi, "Sharia Norms and Digital Economy Practices: A Comparative Legal Analysis of Consumer Protection and E-Payment Regulation," *Asy-Syir'ah: Jurnal Ilmu Syari'ah Dan Hukum* 59, no. 2 (2026): 191–213, https://doi.org/10.14421/ajish.v59i2.1594.

13 Ariyanto, Faghlaifi Naim, and Adnan Qubbaja, "Penerapan Asas Konsensualisme Dalam E-Payment Berbasis QRIS," *Jurnal Hukum IUS QUIA IUSTUM* 32, no. 1 (2025): 149–75, https://doi.org/10.20885/iustum.vol32.iss1.art7.

14 Mas Rara Tri Retno Herryani, "Enhancing Legal Protection for Digital Transactions: Addressing Fraudulent QRIS System in Indonesia," *Rechtsidee* 11, no. 1 (2023): 1–12, https://doi.org/10.21070/jihr.v12i1.990.

15 Rouwa Yalda, Arshad Khan, and Narayan Nepal, "B-PhishQR—A Blockchain-Based Framework for Secure QR Code Verification against Phishing Attacks," *Telematics and Informatics Reports* 21 (2026): 100289, https://doi.org/10.1016/j.teler.2025.100289.

16 Nur Muhamad Hamka et al., "Analysis of QRIS Misuse Mode as a Means of Personal Data Theft and Account Takeover in Bandung City, Indonesia," *Advances in Community Services Research* 4, no. 2 (2026): 68–81, https://doi.org/10.60079/acsr.v4i2.878.

17 Sayyid Muttaqin, "A Fiqh Muamalah Analysis Of Merchant Discount Rate (MDR) In QRIS Transactions and Its Implications For Economic Justice," *International Journal of Management and Business Economics* 4, no. 3 (2026): 515–23, https://doi.org/10.58540/ijmebe.v4i3.1624.

18 Peter Mahmud Marzuki, *Penelitian Hukum Edisi Revisi*, Cet. 13 (Jakarta: Kencana, 2017); Terry Hutchinson, "The Doctrinal Method: Incorporating Interdisciplinary Methods in Reforming the Law," *Erasmus Law Review* 8, no. 3 (2015): 130–38, https://doi.org/10.5553/ELR.000055.

articles, research findings, and non-legal materials in the form of official reports and data concerning the development of digital payment systems.

The analysis of legal materials is conducted qualitatively through a prescriptive legal analysis method.[19] All legal materials are inventoried, classified, and interpreted using grammatical, systematic, and teleological methods of interpretation. These materials are subsequently analyzed through legal reasoning to assess criminal liability for QRIS-based payment manipulation and to examine the relevance of applying the concepts of *jarīmah ta'zīr*, *maqāsid al-syarī'ah*, and *hifz al-māl* in addressing digital payment crimes. This approach produces prescriptive legal arguments that serve as a foundation for formulating an Islamic criminal law response to the evolving landscape of contemporary digital payment crimes.

Results and Discussion

QRIS payment manipulation as contemporary digital payment fraud

Several cases reported in recent years demonstrate that QRIS has become a target for exploitation through various forms of digital manipulation, indicating that the increasing adoption of digital payment systems has been accompanied by greater opportunities for cybercrime. This phenomenon is consistent with Routine Activity Theory proposed by Cohen and Felson,[20] which explains that criminal acts occur when three elements converge simultaneously: a motivated offender, a suitable target, and the absence of a capable guardian. The rapid adoption of QRIS has created millions of users and merchants as potential targets, while limited digital security literacy has resulted in some members of society being unable to distinguish legitimate QR codes from manipulated ones.[21] Such conditions have indirectly generated an opportunity structure that expands the space for the development of various digital payment crime schemes.[22]

QRIS payment manipulation is not limited to the use of fraudulent QR codes, as is frequently reported in mass media.[23] The advancement of electronic payment technologies has facilitated

---

[19] Adriana Placani, "Prescriptive Rules in Legal Theory," *Public Governance, Administration and Finances Law Review* 8, no. 2 (2023): 5–16, https://doi.org/10.53116/pgaflr.6827.

[20] as cited by Renushka Madarie, Marleen Weulen Kranenbarg, and Christianne de Poot, "Cybersecurity Expert Perspectives on Data Thieves' Actions in Digital Environments: Potential Refinements for Routine Activity Theory," *Deviant Behavior* 47, no. 3 (2026): 544–62, https://doi.org/10.1080/01639625.2025.2453440.

[21] Herryani, "Enhancing Legal Protection for Digital Transactions: Addressing Fraudulent QRIS System in Indonesia"; Bulya Bulya and Suci Izzati, "Indonesia's Digital Literacy as a Challenge for Democracy in the Digital Age," *The Journal of Society and Media* 8, no. 2 (2024): 640–61, https://doi.org/10.26740/jsm.v8n2.p640-661; Laxman et al., "Emerging Threats in Digital Payment and Financial Crime: A Bibliometric Review."

[22] Marco Romagna and Rutger Erik Leukfeldt, "Social Opportunity Structures in Hacktivism: Exploring Online and Offline Social Ties and the Role of Offender Convergence Settings in Hacktivist Networks," *Victims & Offenders*, 2024, 1–23, https://doi.org/10.1080/15564886.2024.2372054.

[23] BBC News Indonesia, "QRIS 'palsu' Di 38 Masjid, Bagaimana Memastikan Transaksi Aman?," BBC News Indonesia, April 13, 2023, https://www.bbc.com/indonesia/articles/clw15qp47x50; Oprspitpoldariau, "Polres Kuansing Ungkap Penipuan Digital Bermodus QRIS," Humas Polri, February 18, 2026, https://humas.polri.go.id/news/detail/2288681-polres-kuansing-ungkap-penipuan-digital-bermodus-qris; Yuga Hassani, "Pedagang Di Sekitar Kampus Tel-U Jadi Korban Penipuan QRIS Palsu," detikJabar, October 13, 2025, https://www.detik.com/jabar/hukum-dan-kriminal/d-8158252/pedagang-di-sekitar-kampus-tel-u-jadi-korban-penipuan-qris-palsu; Yashirli Mulyadi, "Modus Bayar Pakai QRIS Palsu, Seorang Pria Di Solok Rugikan Toko Hingga Rp 43 Juta," infosumbar.net, May 2, 2026, https://infosumbar.net/berita/berita-sumbar/solok-raya/modus-bayar-pakai-qris-palsu-seorang-pria-di-solok-rugikan-toko-hingga-rp-43-juta; Reza Efendi, "Kasus Pemalsuan QRIS Rp2,5 Miliar Di Medan Bikin Heboh, Tersangka Ternyata Masih Bebas," Liputan6.com, May 10, 2026, https://berita.liputan6.com/regional/read/6407100/kasus-pemalsuan-qris-rp25-miliar-di-medan-bikin-heboh-tersangka-ternyata-masih-bebas. All online sources were accessed on 2 August 2026.

the emergence of increasingly complex and adaptive modus operandi. QRIS-based payment manipulation can be classified into four main typologies, as presented in Table 1.

Table 1. Typology of QRIS payment manipulation

No.	Typology	Operational method	Target	Impact
1.	QR Code Replacement	Replacing the official QRIS code belonging to a merchant with a QRIS code controlled by the perpetrator	Merchants and consumers	Payment funds are redirected to the perpetrator
2.	QR Phishing (Quishing)	Using QR codes that redirect victims to fraudulent websites designed to obtain banking credentials or authentication data	QRIS users	Digital identity theft and unauthorized access to bank accounts
3.	Merchant Impersonation	Illegally using a merchant's identity or account to receive payments	Consumers	Payments are received by unauthorized parties
4.	Social Engineering	Manipulating or deceiving victims into scanning specific QR codes or confirming fraudulent transactions	Digital payment users	Victims conduct transactions without realizing that manipulation has occurred

Source: compiled by the authors from relevant sources.

Table 1 demonstrates that all typologies of QRIS manipulation share a common objective: obtaining unlawful economic benefits through the abuse of electronic payment systems. The distinction among these typologies lies in the specific targets being exploited. QR Code Replacement manipulates the integrity of payment codes,[24] QR phishing (quishing) targets users' credentials and authentication data,[25] merchant impersonation exploits weaknesses in identity verification mechanisms, while social engineering leverages victims' psychological vulnerabilities to influence transaction decisions.[26] These variations indicate that QRIS manipulation has evolved from a simple form of fraud into a sophisticated digital crime that combines the exploitation of technological systems, security vulnerabilities, and user behavior.

The complexity of these threats has prompted Bank Indonesia and payment service providers to strengthen risk mitigation measures through the deactivation of misused QRIS codes, investigation of potential similar schemes, and enhanced public and merchant education regarding the verification of payment recipient identities.[27] These measures demonstrate that QRIS manipulation is no longer perceived merely as an issue between perpetrators and victims, but also as a threat to public trust and the integrity of the national payment system.

From a legal and criminological perspective, QRIS manipulation constitutes a form of digital payment fraud that exploits electronic payment infrastructure as the primary means of committing criminal acts.[28] Unlike conventional fraud, which primarily involves the unlawful acquisition of property through deception, QRIS manipulation also targets authentication data,

[24] Suliman A. Alsuhibany, "Innovative QR Code System for Tamper-Proof Generation and Fraud-Resistant Verification," *Sensors* 25, no. 13 (2025): 3855, https://doi.org/10.3390/s25133855.

[25] Yalda, Khan, and Nepal, "B-PhishQR—A Blockchain-Based Framework for Secure QR Code Verification against Phishing Attacks."

[26] Ariyanto, Naim, and Qubbaja, "Penerapan Asas Konsensualisme Dalam E-Payment Berbasis QRIS"; Herryani, "Enhancing Legal Protection for Digital Transactions: Addressing Fraudulent QRIS System in Indonesia."

[27] Haryono, "BI Terus Edukasi Masyarakat Dan Pedagang/Merchant Agar Terhindar Dari Upaya Penyalahgunaan QRIS."

[28] Ariyanto, Naim, and Qubbaja, "Penerapan Asas Konsensualisme Dalam E-Payment Berbasis QRIS"; Herryani, "Enhancing Legal Protection for Digital Transactions: Addressing Fraudulent QRIS System in Indonesia."

digital identities, payment mechanisms, and public trust in electronic payment systems.[29] These characteristics place QRIS manipulation within the domains of both cybercrime and financial crime, as its execution relies on electronic systems and has the potential to disrupt the stability and integrity of digital financial infrastructure.[30] Consequently, the evidentiary process in such cases cannot rely solely on conventional forms of evidence but must also incorporate electronic evidence, transaction logs, metadata, and digital forensic findings.[31]

Table 2. Characteristics of conventional fraud and QRIS payment manipulation

No.	Aspect	Conventional fraud	QRIS payment manipulation
1.	Crime medium	Face-to-face interaction or physical documents	Electronic payment systems
2.	Perpetrator–victim relationship	Generally involves direct contact	Does not always involve direct contact
3.	Target of attack	Property or physical assets	Funds, electronic data, and payment systems
4.	Transaction mechanism	Manual	Real-time transactions through digital platforms
5.	Dominant evidence	Physical evidence	Electronic evidence and digital traces
6.	Impact	Individual financial loss	Individual financial loss and declining trust in payment systems

Source: processed by the authors from various sources.

Table 2 illustrates that QRIS payment manipulation possesses fundamentally distinct characteristics from conventional fraud in terms of the crime medium, protected objects, transaction mechanisms, and evidentiary requirements. These differences indicate that QRIS manipulation is more appropriately classified as contemporary digital payment fraud, namely a form of digital payment crime in which electronic payment systems function both as the instrument and the target of criminal conduct. This conceptualization implies the need for criminal liability frameworks that extend beyond protecting individual victims to encompass the preservation of the integrity, security, and reliability of the national payment system.

Criminal liability for QRIS payment manipulation under Indonesian positive law

Indonesian criminal law doctrine places criminal liability on the fulfillment of the elements of a criminal offense and culpability. An individual may only be held criminally liable where the person has committed an act prohibited by law with a culpable mental state that is legally attributable to the offender.[32] QRIS payment manipulation is generally committed intentionally, as offenders deliberately design or exploit digital payment technologies to obtain unlawful financial benefits.[33] The replacement of a merchant's QR code, the creation of QR

---

29 David Njuguna and John Ndia, "Quick Response Code Security Attacks and Countermeasures: A Systematic Literature Review," *Journal of Cyber Security* 7, no. 1 (2025): 1–20, https://doi.org/10.32604/jcs.2025.059398.

30 Gargi Sarkar and Sandeep K. Shukla, "Behavioral Analysis of Cybercrime: Paving the Way for Effective Policing Strategies," *Journal of Economic Criminology* 2 (2023): 100034, https://doi.org/10.1016/j.jeconc.2023.100034; Herryani, "Enhancing Legal Protection for Digital Transactions: Addressing Fraudulent QRIS System in Indonesia."

31 Lena Klasén, Niclas Fock, and Robert Forchheimer, "The Invisible Evidence: Digital Forensics as Key to Solving Crimes in the Digital Age," *Forensic Science International* 362 (2024): 112133, https://doi.org/10.1016/j.forsciint.2024.112133.

32 Andi Hamzah, *Hukum Pidana Indonesia*, ed. Tarmizi (Jakarta: Sinar Grafika, 2017).

33 Ramdhani and Lutfi, "Sharia Norms and Digital Economy Practices: A Comparative Legal Analysis of Consumer Protection and E-Payment Regulation."

codes that redirect victims to phishing websites,[34] the unauthorized use of merchant identities,[35] and the use of social engineering techniques demonstrate the offender's knowledge of and intention to commit the act and bring about its consequences.[36]

Law No. 1 of 2023 on the Criminal Code (National Criminal Code) provides the general legal basis for imposing criminal liability for fraudulent conduct. Article 492 stipulates:

> *"Any Person who, with the intention of unlawfully benefiting himself/herself or another person, by using a false name or false position, employing fraudulent acts or a series of false statements, induces another person to surrender property, provide a loan, acknowledge a debt, or extinguish a receivable, shall be punished for fraud with imprisonment for a maximum of 4 (four) years or a fine of no more than Category V."* (Translated).[37]

This provision demonstrates that the principal elements of fraud consist of the intention to obtain an unlawful benefit, the use of a false name or position, fraudulent acts or a series of false statements, and an act by the victim involving the surrender of property, provision of a loan, acknowledgment of a debt, or extinguishment of a receivable. In the context of QRIS manipulation, these elements may be satisfied where an offender uses a counterfeit QRIS code or alters a QRIS code through deceptive means, thereby inducing the victim to make a payment to the offender.[38] Accordingly, Article 492 serves as a *lex generalis* provision for prosecuting QRIS manipulation insofar as the conduct fulfills the constituent elements of fraud.

The use of electronic means in QRIS manipulation may also fall within the scope of Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions (the Electronic Information and Transactions Law or ITE Law). Article 28 paragraph (1) provides:

> *Every Person who intentionally and without authorization disseminates false and misleading information that causes consumer losses in Electronic Transactions."* (Translated).[39]

This provision focuses on conduct carried out intentionally and without authorization, namely the dissemination of false or misleading information that causes losses to consumers in electronic transactions.[40] The provision is relevant to QRIS manipulation where an offender disseminates misleading electronic information to induce a victim to make a payment through a manipulated QRIS code.

Article 45A paragraph (1) further provides:

> *"Every Person who intentionally distributes and/or transmits Electronic Information and/or Electronic Documents containing false notifications or misleading information*

---

[34] Yalda, Khan, and Nepal, "B-PhishQR—A Blockchain-Based Framework for Secure QR Code Verification against Phishing Attacks."

[35] Muttaqin, "A Fiqh Muamalah Analysis Of Merchant Discount Rate (MDR) In QRIS Transactions and Its Implications For Economic Justice."

[36] Ariyanto, Naim, and Qubbaja, "Penerapan Asas Konsensualisme Dalam E-Payment Berbasis QRIS"; Herryani, "Enhancing Legal Protection for Digital Transactions: Addressing Fraudulent QRIS System in Indonesia."

[37] Republik Indonesia, "Undang-Undang Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana," 2023.

[38] Herryani, "Enhancing Legal Protection for Digital Transactions: Addressing Fraudulent QRIS System in Indonesia."

[39] Republik Indonesia, "Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," 2024.

[40] Bambang Sugeng Ariadi Subagyono et al., "Can Indonesia's Laws Keep Up? Protecting Consumer Rights in Digital Transactions," *Journal of Law and Legal Reform* 5, no. 3 (2024): 869–90, https://doi.org/10.15294/jllr.v5i3.4202.

that causes material losses to consumers in Electronic Transactions as referred to in Article 28 paragraph (1) shall be punished by imprisonment for a maximum of 6 (six) years and/or a fine of up to IDR 1,000,000,000 (one billion rupiahs)." (Translated).[41]

Article 45A paragraph (1) establishes criminal sanctions for the conduct referred to in Article 28 paragraph (1), carrying a maximum imprisonment term of 6 years and/or a fine of up to IDR 1 billion. Accordingly, the EIT Law may complement Article 492 where QRIS manipulation is carried out through the distribution or transmission of misleading electronic information that causes material losses to consumers.

QRIS manipulation may also involve the misuse of personal data. Law No. 27 of 2022 on Personal Data Protection (the Personal Data Protection Law or PDP Law), particularly Articles 67 to 69, establishes criminal provisions concerning the unlawful acquisition, collection, disclosure, use, or misuse of personal data. These provisions prescribe a maximum imprisonment term of 6 years and/or a fine of up to IDR 6 billion, as well as additional penalties in the form of the confiscation of proceeds and/or assets obtained from the criminal offense and the payment of compensation.[42] These provisions are relevant where QRIS manipulation is accompanied by the unauthorized acquisition or use of victims' personal data, ensuring that legal protection extends beyond financial losses to encompass the victims' identities and personal data.[43]

The security of payment systems is regulated by Regulation of the Members of the Board of Governors of Bank Indonesia No. 3 of 2025 on the Third Amendment to Regulation of the Members of the Board of Governors of Bank Indonesia No. 21/18/PADG/2019 on the Implementation of the National Standard for Quick Response Code Payments. This regulation contains provisions concerning risk management, payment system security, and user protection.[44] It functions as a preventive instrument for maintaining the security and governance of the QRIS payment ecosystem. Unlike the National Criminal Code, the ITE Law, and the PDP Law, this Bank Indonesia regulation does not constitute a basis for criminal prosecution but rather supports the prevention and mitigation of risks associated with manipulation within the payment system.

Based on this legal framework, criminal liability for QRIS manipulation is constructed through several legal regimes with distinct functions. The *National Criminal Code* provides the general legal basis for fraud, the ITE Law addresses manipulation involving electronic information and transactions, the PDP Law protects victims' personal data, while Bank Indonesia regulations govern the security and governance of the payment system.[45] Nevertheless, no specific criminal provision currently regulates QRIS manipulation as an independent criminal offense. Consequently, law enforcement remains dependent on the application of different legal provisions according to the particular form of conduct committed by the offender.[46] This condition demonstrates that Indonesian positive law provides a legal

---

41 Republik Indonesia, "Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik."

42 Republik Indonesia, "Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi," 2022.

43 Hamka et al., "Analysis of QRIS Misuse Mode as a Means of Personal Data Theft and Account Takeover in Bandung City, Indonesia."

44 Bank Indonesia, "Peraturan Anggota Dewan Gubernur Nomor 3 Tahun 2025 Tanggal 19 Februari 2025 Tentang Perubahan Ketiga Atas Peraturan Anggota Dewan Gubernur Nomor 21/18/PADG/2019 Tentang Implementasi Standar Nasional Quick Response Code Untuk PembayarAn," 2025.

45 Ramdhani and Lutfi, "Sharia Norms and Digital Economy Practices: A Comparative Legal Analysis of Consumer Protection and E-Payment Regulation."

46 Hamka et al., "Analysis of QRIS Misuse Mode as a Means of Personal Data Theft and Account Takeover in Bandung City, Indonesia"; Herryani, "Enhancing Legal Protection for Digital Transactions: Addressing Fraudulent QRIS System in Indonesia."

basis for imposing criminal liability, but has yet to specifically accommodate the characteristics of contemporary digital payment fraud, which may not only cause losses to individual victims but also potentially undermine the security and integrity of the digital payment system.

QRIS payment manipulation as *jarīmah* in Islamic criminal

The prohibition against unlawfully acquiring and possessing wealth constitutes one of the fundamental principles of Islamic law. As stated in the Qur'an, Allah SWT says:

> *"O you who believe! Do not consume one another's wealth unjustly, except through lawful trade conducted by mutual consent among you. And do not kill yourselves. Surely, Allah is Most Merciful to you."* (Q.S. al-Nisā' [4]: 29).

This verse emphasizes the prohibition against acquiring another person's property through means that are not sanctioned by Islamic law. The prohibition encompasses various forms of conduct that undermine genuine consent or valid agreement in transactions, including fraud, deception, manipulation, and abuse of trust. This principle is universal and is not confined to the forms of transactions known at the time of the Qur'an's revelation.[47] Advances in payment technology do not alter the substance of the Islamic prohibition against unlawfully acquiring wealth. Rather, they merely transform the means and methods employed, while the underlying nature of the conduct, namely, the unauthorized taking or transfer of another person's property, remains within the scope of the prohibition.[48]

The prohibition against fraudulent conduct is further emphasized in a hadith of the Prophet Muhammad PBUH:

> *"Qutaybah ibn Sa'īd narrated to us; Ya'qūb—namely, Ibn 'Abd al-Rahmān al-Qārī—narrated to us. (In another narration:) Abū al-Ahwas Muhammad ibn Hayyān narrated to us; Ibn Abī Hāzim narrated to us. Both narrated from Suhayl ibn Abī Sāliḥ, from his father, from Abū Hurayrah RA, that the Messenger of Allah SWT said: 'Whoever takes up arms against us is not one of us, and whoever deceives us is not one of us.'"* (H.R. Muslim No. 146).[49]

This hadith demonstrates that fraud (*ghish*) is inconsistent with the values of honesty, trustworthiness, and mutual trust that underpin *mu'āmalāt*. Fraud not only causes harm to the victim but also undermines the trust necessary for economic relationships to operate fairly.[50] QRIS payment manipulation exhibits characteristics consistent with this prohibition where an offender intentionally manipulates payment instruments, conceals or misrepresents a merchant's identity, employs quishing, or uses social engineering to induce a victim to make a payment to an unauthorized party. Although the methods and instruments employed are digital, the substance of the conduct remains an act of deception or manipulation that causes the victim's property to be transferred without a lawful basis.[51]

From the perspective of *fiqh jināyah*, QRIS payment manipulation does not constitute a *jarīmah hudūd*, because the *hudūd* category requires a clear textual basis in Islamic law

---

[47] Hendra Cipta, "Jual Beli Yang Diridhoi Dalam Perspektif Surat An-Nisa' (4) Ayat 29," *Asy Syar'iyyah: Jurnal Ilmu Syari'ah Dan Perbankan Islam* 3, no. 2 (2018): 47–62, https://doi.org/10.32923/asy.v3i2.1155.

[48] Auliya Ghazna Nizami, Andini Rahma Hidayah, and Hidayatulloh, "Inappropriate Behavior in Buying and Selling Usernames on Twitter: An Islamic Law Perspective," *Jurnal Hukum Islam* 21, no. 2 (2023): 309–34, https://doi.org/10.28918/jhi_v21i2_04.

[49] Hadits Tazkia, "Bab Perkataan Nabi Shallallahu 'alaihi Wa Sallam 'Barangsiapa Menipu Kami Maka Bukan Dari Golongan Kami,'" Hadits Tazkia, 2020, https://hadits.tazkia.ac.id/hadits/bab/2:47. Accessed 3 August 2026. Accessed 3 August 2026.

[50] Ahyani et al., "Fraud in the Digital Space: A Comparative Study of Jinayah Fiqh and Indonesian Criminal Law."

[51] Ramdhani and Lutfi, "Sharia Norms and Digital Economy Practices: A Comparative Legal Analysis of Consumer Protection and E-Payment Regulation."

establishing both the prohibited conduct and its prescribed punishment. QRIS manipulation, as a form of crime that has emerged alongside digital payment technologies, has no specific *hadd* provision prescribing either the conduct or its punishment in the Qur'an or hadith.[52] Nor does the conduct constitute a *jarīmah qisās* or *diyāt*, because its primary object of infringement concerns property and transactional rights rather than life or bodily integrity.[53] Accordingly, QRIS payment manipulation is more appropriately classified as a *jarīmah ta'zīr*, namely, conduct prohibited by Islamic law for which neither the type nor the degree of punishment is specifically prescribed by *nass* and whose determination is entrusted to the *ulil amri* in accordance with the degree of culpability, harm, and public interest to be achieved.

The classification of QRIS manipulation as a *jarīmah ta'zīr* is further supported when examined through the elements of criminal liability in *fiqh jināyah*. Regarding the *rukn sharʿī*, there is a normative basis prohibiting the unlawful appropriation of property and fraudulent conduct, as reflected in Q.S. al-Nisā' [4]: 29 and the Prophetic hadith prohibiting deception. Regarding the *rukn maddī*, the conduct involves concrete acts of manipulating digital payment instruments or information that cause the victim's property to be transferred to the offender or another unauthorized party. Regarding the *rukn adabī*, criminal liability is attributable to an offender who possesses legal capacity (*mukallaf*) and commits the conduct knowingly and intentionally.[54] Once these three elements are satisfied, QRIS payment manipulation may be regarded as conduct that establishes the basis for criminal liability within the category of *jarīmah ta'zīr*.

The perspective of *maqāṣid al-sharīʿah* further strengthens the need for legal protection against QRIS payment manipulation. Such conduct directly implicates the protection of property (*hifz al-māl*), as the manipulation is intended to unlawfully acquire or divert the victim's property. The transfer of funds resulting from manipulation of a payment system is not merely an individual economic loss but also constitutes an infringement of property rights protected under Islamic law. In the context of digital transactions, the protection of *hifz al-māl* should not be understood merely as protection of property after its transfer. It also encompasses the protection of the mechanisms and instruments that facilitate the lawful transfer of ownership rights.[55]

This *maqāsid* dimension is also connected to the protection of intellect (*hifz al-'aql*), particularly where manipulation is carried out through quishing and social engineering. These methods employ information-based manipulation to influence victims' ability to understand circumstances and make decisions freely and consciously. Such manipulation of information is inconsistent with the principles of *sidq*, trustworthiness, and transparency that constitute the foundations of *mu'āmalāt*. Although *hifz al-'aql* is not the primary interest infringed by QRIS manipulation, this dimension demonstrates that the consequences of digital crime may extend beyond financial loss. Manipulation may also undermine trust in economic relationships and

---

52 Reni Surya, "Klasifikasi Tindak Pidana Hudud Dan Sanksinya Dalam Perspektif Hukum Islam," *Samarah: Jurnal Hukum Keluarga Dan Hukum Islam* 2, no. 2 (2019): 530–47, https://doi.org/10.22373/sjhk.v2i2.4751.

53 Muhammad Tahmid Nur, "Justice in Islamic Criminal Law: Study of the Concept and Meaning of Justice in The Law of Qiṣāṣ," *Asy-Syir'ah: Jurnal Ilmu Syari'ah Dan Hukum* 55, no. 2 (2021): 335–65, https://doi.org/10.14421/ajish.v55i2.1011.

54 Misran Misran, "Criteria of Offenses as Part of Ta'zir Penalty [Kriteria Tindak Pidana Yang Diancam Hukuman Ta'Zir]," *Legitimasi: Jurnal Hukum Pidana Dan Politik Hukum* 10, no. 1 (2021): 25–40, https://doi.org/10.22373/legitimasi.v10i1.10515.

55 Ahyani et al., "Fraud in the Digital Space: A Comparative Study of Jinayah Fiqh and Indonesian Criminal Law."

affect the security of digital interactions, which have increasingly become an integral part of social life.[56]

The harm caused by QRIS manipulation is therefore multidimensional. Victims may suffer financial losses and misuse of personal data, while merchants, payment service providers, and society at large may experience declining trust in digital payment systems. The broader the impact caused by an offense, the greater the interests that must be protected through *ta'zīr* policy. Accordingly, the application of *ta'zīr* is not solely directed toward punishing the offender but also toward preventing recidivism, protecting victims' rights, maintaining the integrity of transactions, and preserving public welfare.[57]

The nature of *ta'zīr* provides *ulil amri* with discretion to determine the type and severity of sanctions according to the characteristics of the offense and its surrounding circumstances. The determination of sanctions may take into account the offender's degree of culpability, the amount of loss, the number of victims, the sophistication of the modus operandi, the frequency of the conduct, its impact on the payment system, and the likelihood of recurrence. Sanctions may include imprisonment, fines, compensation (*ta'wīd*), restrictions on certain rights, or other forms of punishment permitted under Islamic law and imposed through lawful authority.[58] Thus, the flexibility inherent in *ta'zīr* does not confer unlimited discretion; rather, it provides the state with room to formulate proportionate sanctions based on the degree of harm and the public interest (*maslahah*) to be achieved.

This framework demonstrates the strong relevance of *ta'zīr* in responding to contemporary digital payment fraud. Digital payment crimes possess characteristics that distinguish them from forms of property crime discussed in classical Islamic legal literature, particularly because they involve technology, electronic systems, data, and continuously evolving patterns of manipulation.[59] Nevertheless, the development of new methods does not negate the fundamental Islamic prohibition against unlawfully acquiring property. Rather, *ta'zīr* provides a normative framework through which Islamic criminal law can respond to emerging forms of crime while remaining oriented toward justice, public welfare, the protection of rights, and the prevention of *mafsadah*.

Based on this construction, the reconstruction of Islamic criminal liability for QRIS payment manipulation may be formulated through four principal principles:

1) QRIS manipulation constitutes conduct contrary to Islamic principles, as it involves the unlawful acquisition of property, fraud, deception, and abuse of trust in transactions.
2) QRIS manipulation exhibits the characteristics of a *jarīmah ta'zīr* because it does not fall within the categories of *jarīmah hudūd*, *qisas*, or *diyāt*, but constitutes prohibited conduct that causes harm to victims and society.
3) criminal liability is not oriented solely toward the culpability of the offender, but also toward the protection of *maqāsid al-sharī'ah*, particularly *hifz al-māl*, as well as the protection of security and trust within the digital payment system.
4) the determination of the type and severity of sanctions falls within the authority of the *ulil amri* and must be exercised proportionately by considering the degree of culpability,

---

[56] Herryani, "Enhancing Legal Protection for Digital Transactions: Addressing Fraudulent QRIS System in Indonesia"; Ramdhani and Lutfi, "Sharia Norms and Digital Economy Practices: A Comparative Legal Analysis of Consumer Protection and E-Payment Regulation."

[57] Misran, "Criteria of Offenses as Part of Ta'zir Penalty [Kriteria Tindak Pidana Yang Diancam Hukuman Ta'Zir]."

[58] Misran.

[59] Hamka et al., "Analysis of QRIS Misuse Mode as a Means of Personal Data Theft and Account Takeover in Bandung City, Indonesia"; Ahyani et al., "Fraud in the Digital Space: A Comparative Study of Jinayah Fiqh and Indonesian Criminal Law."

the magnitude of the loss, the sophistication of the modus operandi, the social impact, victims' interests, and the public interest.

This reconstruction demonstrates that the concept of *jarīmah ta'zīr* possesses an adaptive capacity to respond to the development of digital payment crimes without departing from the fundamental principles of Islamic law. Such adaptability enables Islamic criminal law to address continuously evolving criminal methods, while its orientation toward *maqāsid al-sharī'ah* ensures that criminal sanctions remain directed toward the protection of property, restoration of victims' rights, crime prevention, the realization of public welfare, and the prevention of *mafsadah*.

Reconstructing Islamic criminal policy for digital payment fraud

The analysis presented in the preceding subsection demonstrates that QRIS payment manipulation exhibits the characteristics of contemporary digital payment fraud, causing harm not only to individual victims but also potentially undermining payment system security and public trust. Indonesian positive law provides a basis for criminal liability through several statutory instruments, while the perspective of *fiqh jināyah* classifies such conduct as a *jarīmah ta'zīr*. Nevertheless, this classification alone does not provide an adequate framework for formulating Islamic criminal policy in response to the evolving nature of digital payment crimes.

Previous studies have generally examined cybercrime from the perspective of *jarīmah ta'zīr*, analyzed the constituent elements of *fiqh jināyah*, or employed *maqāsid al-sharī'ah* as a normative basis for the protection of property. Research concerning QRIS, meanwhile, has primarily focused on regulatory frameworks, payment system security, and consumer protection.[60] The relationship between Indonesian positive law and Islamic criminal law in formulating criminal policy for digital payment fraud, particularly QRIS manipulation, has yet to be comprehensively developed. This gap indicates that the contribution of the present study lies not merely in determining the legal status of QRIS manipulation as a *jarīmah ta'zīr*, but rather in developing a criminal policy framework capable of integrating Islamic criminal law principles with the protection requirements of the digital payment ecosystem.

On this basis, this study develops an adaptive *ta'zīr* framework as a normative framework for responding to *contemporary digital payment fraud*. The framework integrates the concepts of *ta'zīr* and *maqāsid al-sharī'ah* with principles of modern criminal policy into an approach that conceptualizes *ta'zīr* not merely as a category of criminal offense, but also as a foundation for developing criminal policies that can adapt to advances in financial technology. Accordingly, the novelty of this study lies in repositioning the function of *ta'zīr* from merely serving as a basis for legal classification and punishment toward a broader policy framework encompassing prevention, punishment, restoration, and governance.

Table 3. Synthesis of research developments and the contribution of the present study

Research	Focus	Contribution	Limitations	Position of the Present Study
Cybercrime from the perspective of Islamic	Classificatio n of cybercrime as *jarīmah*	Demonstrates the relevance of *fiqh jināyah* to digital crimes	Does not specifically examine digital payment fraud	Focuses on QRIS manipulation as a form of contemporary digital payment fraud.

[60] Ahyani et al., "Fraud in the Digital Space: A Comparative Study of Jinayah Fiqh and Indonesian Criminal Law"; Ramdhani and Lutfi, "Sharia Norms and Digital Economy Practices: A Comparative Legal Analysis of Consumer Protection and E-Payment Regulation."

criminal law.[61]	*ta'zīr*			
Studies on *maqāsid al-sharī'ah* and cybercrime.[62]	Protection of *hifz al-māl* and public welfare (*maslahah*)	Strengthens the normative foundation for the protection of property	Does not develop an operational criminal policy framework	Integrates *maqāsid*, *fiqh jināyah*, and criminal policy into a unified analytical framework.
Studies of QRIS under Indonesian positive law.[63]	Regulation and criminal liability	Explains the relevant national legal instruments	Does not connect QRIS regulation and criminal liability with Islamic criminal law	Establishes a comprehensive link between Indonesian positive law and *fiqh jināyah*.
Studies on the reformulation of *ta'zīr* in the digital era.[64]	The flexibility of *ta'zīr*	Demonstrates the capacity of Islamic law to adapt to technological developments	Does not propose a criminal policy reconstruction for digital payment systems	Mengembangkan rekonstruksi kebijakan pidana Islam yang adaptif terhadap kejahatan pembayaran digital.

Source: Compiled by the author based on a synthesis of previous studies.

The synthesis demonstrates that Islamic criminal policy addressing digital payment crimes cannot be adequately developed merely by classifying QRIS manipulation as a *jarīmah ta'zīr*. Advances in financial technology have expanded the scope of legal interests requiring protection, from individual property to the security and integrity of digital payment systems, which now function as essential infrastructure for economic activities.[65] This development necessitates a criminal policy that is oriented not only toward punishing offenders but also toward preventing crime, restoring victims' losses, protecting public interests, and maintaining public trust in payment systems.

In response to these needs, this study develops an adaptive *ta'zīr* framework as a normative framework that integrates the principles of *fiqh jināyah*, *maqāsid al-sharī'ah*, and modern criminal policy in addressing *contemporary digital payment fraud*. The framework is not intended to replace Indonesian positive law but rather to provide a philosophical and normative foundation for developing criminal policies that are more responsive to advances in digital payment technologies. The relationship between positive law and Islamic criminal law is therefore conceptualized as complementary: positive law provides legal certainty through the formulation of criminal offenses, enforcement mechanisms, and the determination of sanctions, whereas Islamic criminal law provides normative guidance concerning the protection

[61] Putra Aulia, Maulana Muklis, and Rosdewi Pulungan, "Perbandingan Perspektif Hukum Pencegahan Kejahatan Dunia Maya Dalam Hukum Positif Dan Hukum Pidana Islam," *Jurnal El-Thawalib* 6, no. 2 (2025): 172–86, https://doi.org/10.24952/el-thawalib.v6i2.14928.

[62] Bunyamin Bunyamin et al., "Reforming Indonesia's Correctional System: The Role of Maqāṣid Al-Syarīʿah in Ensuring Justice and Rehabilitation," *De Jure: Jurnal Hukum Dan Syar'iah* 17, no. 1 (2025): 52–71, https://doi.org/10.18860/j-fsh.v17i1.29258.

[63] Herryani, "Enhancing Legal Protection for Digital Transactions: Addressing Fraudulent QRIS System in Indonesia."

[64] Imroatul Azizah et al., "Digitalization and Cyberfeminism: Reinterpreting Islamic Criminal Law for Gender Equality and Women's Rights," *Volksgeist: Jurnal Ilmu Hukum Dan Konstitusi* 9, no. 1 (2026): 127–43, https://doi.org/10.24090/volksgeist.v9i1.15378.

[65] Ahyani et al., "Fraud in the Digital Space: A Comparative Study of Jinayah Fiqh and Indonesian Criminal Law."

of public welfare, proportionality in punishment, restoration of rights, and the prevention of *mafsadah*.

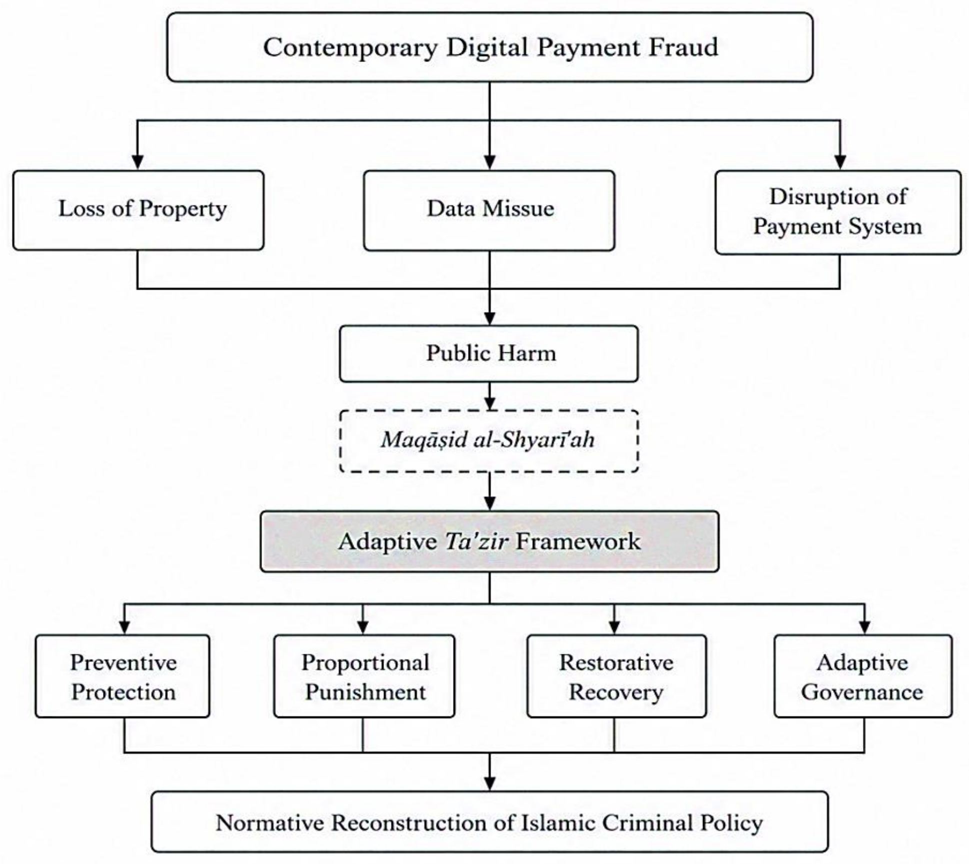

Figure 1. Adaptive *ta'zīr* framework

The adaptive *ta'zīr* framework is constructed around four interrelated components: preventive protection, proportional punishment, restorative recovery, and adaptive governance. Together, these components form a unified criminal policy framework that integrates prevention, punishment, restoration, and policy adaptation in response to developments in digital payment technologies.

Preventive protection places prevention at the forefront of criminal policy. This principle is closely associated with the concept of *sadd al-dharā'i'*, which seeks to block the means that may lead to harm.[66] Prevention is pursued not only through the threat of criminal sanctions after an offense has occurred, but also through improving public digital literacy, strengthening QRIS security standards, developing early-warning systems for suspicious transactions, and enhancing oversight of payment system operators. This approach shifts legal protection to the stage before harm occurs, thereby minimizing opportunities for QRIS manipulation.

Proportional punishment establishes proportionality as the principal basis for determining sanctions. The nature of *ta'zīr* grants *ulil amri* discretion to determine the type and severity of punishment according to the offender's degree of culpability and the harm caused.[67] In cases of QRIS manipulation, proportionality should not be assessed solely by reference to the amount of material loss. It should also take into account the number of victims, the sophistication of the modus operandi, the degree of intent, the frequency of the conduct, the use of technology,

---

[66] Muhammad Nazir Alias et al., "The Position of Maqasid Al-Shariah within Islamic Legal Sources: A Comprehensive Analysis," *Samarah: Jurnal Hukum Keluarga Dan Hukum Islam* 9, no. 2 (2025): 937–64, https://doi.org/10.22373/sjhk.v9i2.26659.

[67] Misran, "Criteria of Offenses as Part of Ta'zir Penalty [Kriteria Tindak Pidana Yang Diancam Hukuman Ta'Zir]."

and its impact on the security of and public confidence in the payment system. Sanctions may therefore be calibrated to the offender's culpability and the legal interests requiring protection.

Restorative recovery places restoration at the core of criminal policy. Criminal justice should not end with the imposition of sanctions on the offender but should also address the recovery of losses suffered by victims and other affected parties.[68] The return of misappropriated funds, payment of compensation (*ta'wīd*), protection of affected merchants, and restoration of public confidence in digital payment systems form part of this orientation. This approach is consistent with *maqāsid al-sharī'ah*, particularly *hifz al-māl*, because the protection of property seeks not only to prevent unlawful appropriation but also to ensure the restoration of the rights of injured parties and the preservation of public welfare.[69]

Adaptive governance emphasizes the capacity of criminal policy to evolve in response to developments in financial technology. Digital payment crimes are inherently dynamic because technological innovation can generate new methods of offending that were not contemplated when existing regulations were adopted. Developments such as artificial intelligence, blockchain technology, cross-border payment systems, and central bank digital currencies may create new forms of attacks against payment infrastructures.[70] The flexibility of *ta'zīr* enables *ulil amri* to exercise policy-oriented *ijtihād* through regulatory reform, legal harmonization, stronger inter-agency coordination, and enhanced capacity among law enforcement authorities.[71] Such adaptability must nevertheless operate through lawful authority and remain guided by the principles of legality, justice, proportionality, and public welfare.

These four components operate as complementary elements within a single framework. Preventive protection reduces opportunities for crime; proportional punishment ensures accountability commensurate with culpability and harm; restorative recovery secures the restoration of victims' rights and losses; and adaptive governance ensures that criminal policy remains responsive to technological developments. Their integration positions the adaptive *ta'zīr* framework as an Islamic criminal policy model that extends beyond punishment to encompass prevention, victim protection, payment system security, and public welfare.

This construction broadens the understanding of *hifz al-māl* in the digital era. Protection of property extends beyond ownership itself to include the security of the mechanisms through which property is lawfully transferred. QRIS manipulation not only causes financial loss but may also undermine the integrity of payment systems and diminish public confidence in digital transactions.[72] Accordingly, *hifz al-māl* should encompass the security and sustainability of payment ecosystems as part of the protection of public welfare.

From a theoretical perspective, this reconstruction expands the function of *ta'zīr* in responding to contemporary crime. *Ta'zīr* grants *ulil amri* discretion to determine sanctions according to the degree of culpability and harm involved.[73] This flexibility may serve as a normative foundation for criminal policies capable of adapting to technological developments

---

68 Ahmad Ropei, "The Resolution of Criminal Cases Through a Restorative Justice Approach in Islamic Law Perspective," *Jurnal Hukum Islam* 18, no. 2 (2020): 293–312, https://doi.org/10.28918/jhi.v18i2.2936.

69 Alias et al., "The Position of Maqasid Al-Shariah within Islamic Legal Sources: A Comprehensive Analysis."

70 Ahyani et al., "Fraud in the Digital Space: A Comparative Study of Jinayah Fiqh and Indonesian Criminal Law"; Nizami, Hidayah, and Hidayatulloh, "Inappropriate Behavior in Buying and Selling Usernames on Twitter: An Islamic Law Perspective."

71 Misran, "Criteria of Offenses as Part of Ta'zir Penalty [Kriteria Tindak Pidana Yang Diancam Hukuman Ta'Zir]."

72 Herryani, "Enhancing Legal Protection for Digital Transactions: Addressing Fraudulent QRIS System in Indonesia"; Ramdhani and Lutfi, "Sharia Norms and Digital Economy Practices: A Comparative Legal Analysis of Consumer Protection and E-Payment Regulation."

73 Misran, "Criteria of Offenses as Part of Ta'zir Penalty [Kriteria Tindak Pidana Yang Diancam Hukuman Ta'Zir]."

without departing from the fundamental principles of Islamic law.[74] In this sense, *ta'zīr* functions not only as an instrument of punishment but also as a foundation for welfare-oriented criminal policy.

From a regulatory perspective, this reconstruction highlights the importance of harmonizing criminal law, payment system regulation, personal data protection, and cybersecurity. Such harmonization is necessary to ensure that responses to *digital payment fraud* extend beyond offender punishment to include prevention, victim protection, recovery of losses, and strengthening payment system security. Continuous policy adaptation should remain anchored in the principles of legality, justice, proportionality, and public welfare.

The principal contribution of this study lies in developing the adaptive *ta'zīr* framework, which integrates preventive protection, proportional punishment, restorative recovery, and adaptive governance as a comprehensive Islamic criminal policy framework for contemporary digital payment fraud. The framework demonstrates that the Islamic criminal law response to digital crime should not stop at classifying conduct as a *jarīmah ta'zīr*. Rather, it should extend to prevention, proportionate punishment, restoration of victims' rights, and adaptive governance. In doing so, the adaptive *ta'zīr* framework places *maqāsid al-sharī'ah* at the substantive core of an Islamic criminal policy that remains responsive to technological change while grounded in justice and public welfare.

Conclussion

This study concludes that QRIS payment manipulation constitutes a form of contemporary digital payment fraud that not only causes individual victims to suffer financial losses but also threatens the integrity of digital payment systems and public trust. The analysis demonstrates that Indonesian positive law provides a basis for criminal liability through various statutory instruments, while Islamic criminal law classifies such conduct as a *jarīmah ta'zīr*, with the determination of sanctions entrusted to *ulil amri* in accordance with the principle of public welfare (*maslahah*). The synthesis of these two perspectives gives rise to the adaptive *ta'zīr* framework as a reconstruction of Islamic criminal policy integrating preventive protection, proportional punishment, restorative recovery, and adaptive governance. This framework repositions *ta'zīr* not merely as a classification of criminal offenses but also as a normative foundation for developing criminal policies capable of adapting to advances in financial technology while remaining oriented toward the protection of *maqāsid al-sharī'ah*.

This study is subject to limitations, particularly its reliance on a normative legal approach and its focus on QRIS payment manipulation. Future research should empirically examine the implementation of the adaptive *ta'zīr* framework, extend the analysis to other forms of digital payment fraud, and investigate its relevance across different legal systems. Such research may strengthen the practical applicability of the proposed framework while contributing to the development of contemporary *fiqh jināyah* as a normative basis for criminal policies responsive to technological transformation and the digital economy.

Acknowledgements

The authors have no acknowledgements to report.

Disclosure Statement

The authors reported no potential conflict of interest.

---

74 Aulia, Muklis, and Pulungan, "Perbandingan Perspektif Hukum Pencegahan Kejahatan Dunia Maya Dalam Hukum Positif Dan Hukum Pidana Islam."

AI Usage Statement

The authors used OpenAI's ChatGPT and DeepL AI solely for language support, including grammar, clarity, readability, and translation. These tools were not involved in the study design, analysis, interpretation, or conclusions. The authors independently reviewed and verified the manuscript and remain fully responsible for its accuracy and integrity.

Author Contributions

M.G.: Conceptualization, methodology, investigation, formal analysis, data curation, visualization, and writing—original draft preparation. B.M.: Validation, supervision, and writing—review and editing. D.A.B.A.: Investigation, validation, and writing—review and editing. All authors reviewed and approved the final version of the manuscript.

References

Ahyani, Hisam, Parhan Parhan, Muhtolib Muhtolib, Ahmad Berizi, Nurhasana Nurhasana, and Nurul Ilyana Muhd Adnan. "Fraud in the Digital Space: A Comparative Study of Jinayah Fiqh and Indonesian Criminal Law." *Jurnal Hukum Islam* 23, no. 1 (2025): 37–72. https://doi.org/10.28918/jhi.v23i1.02.

Alias, Muhammad Nazir, Muhammad Najib Abdullah, Mohd Farihal Osman, Nor Faizah Ismail, and Mohd Sham Kamis. "The Position of Maqasid Al-Shariah within Islamic Legal Sources: A Comprehensive Analysis." *Samarah: Jurnal Hukum Keluarga Dan Hukum Islam* 9, no. 2 (2025): 937–64. https://doi.org/10.22373/sjhk.v9i2.26659.

Alpaullivarez, Angelique Aurielle, and Ahmad Nurul Fajar. "Exploring Factors Influencing User Avoidance Behavior Toward QR-Based Payment Scams." *Journal of Information Systems Engineering and Business Intelligence* 12, no. 2 (2026): 458–73. https://doi.org/10.20473/jisebi.12.2.458-473.

Alsuhibany, Suliman A. "Innovative QR Code System for Tamper-Proof Generation and Fraud-Resistant Verification." *Sensors* 25, no. 13 (2025): 3855. https://doi.org/10.3390/s25133855.

Ariyanto, Faghlaifi Naim, and Adnan Qubbaja. "Penerapan Asas Konsensualisme Dalam E-Payment Berbasis QRIS." *Jurnal Hukum IUS QUIA IUSTUM* 32, no. 1 (2025): 149–75. https://doi.org/10.20885/iustum.vol32.iss1.art7.

Aulia, Putra, Maulana Muklis, and Rosdewi Pulungan. "Perbandingan Perspektif Hukum Pencegahan Kejahatan Dunia Maya Dalam Hukum Positif Dan Hukum Pidana Islam." *Jurnal El-Thawalib* 6, no. 2 (2025): 172–86. https://doi.org/10.24952/el-thawalib.v6i2.14928.

Azizah, Imroatul, Mabarroh Azizah, Saiful Bakhri, Suqiyah Musafa'ah, Amang Fathurrohman, and Shofa Robbani. "Reconstructing Islamic Criminal Liability for Economic Crimes: A Maqasid-Based Framework for Indonesia's Sharia Finance." *El-Mashlahah* 16, no. 1 (2026): 41–64. https://doi.org/10.23971/el-mashlahah.v16i1.11254.

Azizah, Imroatul, Lisa Aminatul Mukaromah, Khurul Anam, Sanuri, and Nafi' Mubarok. "Digitalization and Cyberfeminism: Reinterpreting Islamic Criminal Law for Gender Equality and Women's Rights." *Volksgeist: Jurnal Ilmu Hukum Dan Konstitusi* 9, no. 1 (2026): 127–43. https://doi.org/10.24090/volksgeist.v9i1.15378.

Bank Indonesia. "Peraturan Anggota Dewan Gubernur Nomor 3 Tahun 2025 Tanggal 19 Februari 2025 Tentang Perubahan Ketiga Atas Peraturan Anggota Dewan Gubernur Nomor 21/18/PADG/2019 Tentang Implementasi Standar Nasional Quick Response Code Untuk PembayarAn," 2025.

BBC News Indonesia. "QRIS 'palsu' Di 38 Masjid, Bagaimana Memastikan Transaksi Aman?" BBC

News Indonesia, April 13, 2023. https://www.bbc.com/indonesia/articles/clw15qp47x5o.

Bulya, Bulya, and Suci Izzati. "Indonesia's Digital Literacy as a Challenge for Democracy in the Digital Age." *The Journal of Society and Media* 8, no. 2 (2024): 640–61. https://doi.org/10.26740/jsm.v8n2.p640-661.

Bunyamin, Bunyamin, Firdaus Arifin, Ihsanul Maarif, Robi Assadul Bahri, and Mohd Kamarulnizam Abdullah. "Reforming Indonesia's Correctional System: The Role of Maqāṣid Al-Syarīʿah in Ensuring Justice and Rehabilitation." *De Jure: Jurnal Hukum Dan Syar'iah* 17, no. 1 (2025): 52–71. https://doi.org/10.18860/j-fsh.v17i1.29258.

Cipta, Hendra. "Jual Beli Yang Diridhoi Dalam Perspektif Surat An-Nisa' (4) Ayat 29." *Asy Syar'iyyah: Jurnal Ilmu Syari'ah Dan Perbankan Islam* 3, no. 2 (2018): 47–62. https://doi.org/10.32923/asy.v3i2.1155.

Djalaluddin, Muhammad Mawardi, Bulqia Mas'ud, Dedy Sumardi, Isnawardatul Bararah, and Kamus Kamus. "The Implementation of Ta'zīr Punishment as an Educational Reinforcement in Islamic Law." *Samarah: Jurnal Hukum Keluarga Dan Hukum Islam* 7, no. 1 (2023): 399–417. https://doi.org/10.22373/sjhk.v7i1.15101.

Efendi, Reza. "Kasus Pemalsuan QRIS Rp2,5 Miliar Di Medan Bikin Heboh, Tersangka Ternyata Masih Bebas." Liputan6.com, May 10, 2026. https://berita.liputan6.com/regional/read/6407100/kasus-pemalsuan-qris-rp25-miliar-di-medan-bikin-heboh-tersangka-ternyata-masih-bebas.

Gunawan, Ali, Alifia Farrah Fatikasari, and Selva Aisah Putri. "The Effect of Using Cashless (QRIS) on Daily Payment Transactions Using the Technology Acceptance Model." *Procedia Computer Science* 227 (2023): 548–56. https://doi.org/10.1016/j.procs.2023.10.557.

Hadits Tazkia. "Bab Perkataan Nabi Shallallahu 'alaihi Wa Sallam 'Barangsiapa Menipu Kami Maka Bukan Dari Golongan Kami.'" Hadits Tazkia, 2020. https://hadits.tazkia.ac.id/hadits/bab/2:47.

Hamka, Nur Muhamad, Sylpi Nopiya, Tantri Pebyani, Suci Fitriani, Viny Limbong, and Yulianah Yulianah. "Analysis of QRIS Misuse Mode as a Means of Personal Data Theft and Account Takeover in Bandung City, Indonesia." *Advances in Community Services Research* 4, no. 2 (2026): 68–81. https://doi.org/10.60079/acsr.v4i2.878.

Hamzah, Andi. *Hukum Pidana Indonesia*. Edited by Tarmizi. Jakarta: Sinar Grafika, 2017.

Haryono, Erwin. "BI Terus Edukasi Masyarakat Dan Pedagang/Merchant Agar Terhindar Dari Upaya Penyalahgunaan QRIS." Bank Indonesia, April 11, 2023. https://www.bi.go.id/id/publikasi/ruang-media/news-release/Pages/sp_259323.aspx.

Hassani, Yuga. "Pedagang Di Sekitar Kampus Tel-U Jadi Korban Penipuan QRIS Palsu." detikJabar, October 13, 2025. https://www.detik.com/jabar/hukum-dan-kriminal/d-8158252/pedagang-di-sekitar-kampus-tel-u-jadi-korban-penipuan-qris-palsu.

Herryani, Mas Rara Tri Retno. "Enhancing Legal Protection for Digital Transactions: Addressing Fraudulent QRIS System in Indonesia." *Rechtsidee* 11, no. 1 (2023): 1–12. https://doi.org/10.21070/jihr.v12i1.990.

Hutchinson, Terry. "The Doctrinal Method: Incorporating Interdisciplinary Methods in Reforming the Law." *Erasmus Law Review* 8, no. 3 (2015): 130–38. https://doi.org/10.5553/ELR.000055.

Kilay, Alfonz Lawrenz, Bachtiar H. Simamora, and Danang Pinardi Putra. "The Influence of E-Payment and E-Commerce Services on Supply Chain Performance: Implications of Open Innovation and Solutions for the Digitalization of Micro, Small, and Medium Enterprises (MSMEs) in Indonesia." *Journal of Open Innovation: Technology, Market, and Complexity* 8, no. 3 (2022): 119. https://doi.org/10.3390/joitmc8030119.

Klasén, Lena, Niclas Fock, and Robert Forchheimer. "The Invisible Evidence: Digital Forensics as Key to Solving Crimes in the Digital Age." *Forensic Science International* 362 (2024): 112133. https://doi.org/10.1016/j.forsciint.2024.112133.

Komdigi RI. "Waspada Modus Kejahatan Lewat QRIS." Direktorat Jenderal Ekosistem Digital, December 30, 2025. https://djed.komdigi.go.id/news/waspada-modus-kejahatan-lewat-qris.

Laxman, Vishnu, Nithyashree Ramesh, Senthil Kumar Jaya Prakash, and Ravi Aluvala. "Emerging Threats in Digital Payment and Financial Crime: A Bibliometric Review." *Journal of Digital Economy* 3 (2024): 205–22. https://doi.org/10.1016/j.jdec.2025.04.002.

Madarie, Renushka, Marleen Weulen Kranenbarg, and Christianne de Poot. "Cybersecurity Expert Perspectives on Data Thieves' Actions in Digital Environments: Potential Refinements for Routine Activity Theory." *Deviant Behavior* 47, no. 3 (2026): 544–62. https://doi.org/10.1080/01639625.2025.2453440.

Marzuki, Peter Mahmud. *Penelitian Hukum Edisi Revisi*. Cet. 13. Jakarta: Kencana, 2017.

Misran, Misran. "Criteria of Offenses as Part of Ta'zir Penalty [Kriteria Tindak Pidana Yang Diancam Hukuman Ta'Zir]." *Legitimasi: Jurnal Hukum Pidana Dan Politik Hukum* 10, no. 1 (2021): 25–40. https://doi.org/10.22373/legitimasi.v10i1.10515.

Muchtar, Evan Hamzah, Budi Trianto, Irwan Maulana, Muhammad Nurul Alim, Ruslan Husen Marasabessy, Wahyu Hidayat, Edy Junaedi, and Masrizal. "Quick Response Code Indonesia Standard (QRIS) E-Payment Adoption: Customers Perspective." *Cogent Business & Management* 11, no. 1 (2024): 2316044. https://doi.org/10.1080/23311975.2024.2316044.

Mulyadi, Yashirli. "Modus Bayar Pakai QRIS Palsu, Seorang Pria Di Solok Rugikan Toko Hingga Rp 43 Juta." infosumbar.net, May 2, 2026. https://infosumbar.net/berita/berita-sumbar/solok-raya/modus-bayar-pakai-qris-palsu-seorang-pria-di-solok-rugikan-toko-hingga-rp-43-juta.

Muttaqin, Sayyid. "A Fiqh Muamalah Analysis Of Merchant Discount Rate (MDR) In QRIS Transactions and Its Implications For Economic Justice." *International Journal of Management and Business Economics* 4, no. 3 (2026): 515–23. https://doi.org/10.58540/ijmebe.v4i3.1624.

Nizami, Auliya Ghazna, Andini Rahma Hidayah, and Hidayatulloh. "Inappropriate Behavior in Buying and Selling Usernames on Twitter: An Islamic Law Perspective." *Jurnal Hukum Islam* 21, no. 2 (2023): 309–34. https://doi.org/10.28918/jhi_v21i2_04.

Njuguna, David, and John Ndia. "Quick Response Code Security Attacks and Countermeasures: A Systematic Literature Review." *Journal of Cyber Security* 7, no. 1 (2025): 1–20. https://doi.org/10.32604/jcs.2025.059398.

Nur, Muhammad Tahmid. "Justice in Islamic Criminal Law: Study of the Concept and Meaning of Justice in The Law of Qiṣāṣ." *Asy-Syir'ah: Jurnal Ilmu Syari'ah Dan Hukum* 55, no. 2 (2021): 335–65. https://doi.org/10.14421/ajish.v55i2.1011.

OJK Indonesia. "Modus Layanan Keuangan Ilegal Masih Mengintai." X (Twitter), June 25, 2026. https://x.com/ojkindonesia/status/2070046016242606347.

Oprspitpoldariau. "Polres Kuansing Ungkap Penipuan Digital Bermodus QRIS." Humas Polri, February 18, 2026. https://humas.polri.go.id/news/detail/2288681-polres-kuansing-ungkap-penipuan-digital-bermodus-qris.

Placani, Adriana. "Prescriptive Rules in Legal Theory." *Public Governance, Administration and Finances Law Review* 8, no. 2 (2023): 5–16. https://doi.org/10.53116/pgaflr.6827.

Ramdhani, Fajri Zulia, and A Hashfi Lutfi. "Sharia Norms and Digital Economy Practices: A Comparative Legal Analysis of Consumer Protection and E-Payment Regulation." *Asy-Syir'ah: Jurnal Ilmu Syari'ah Dan Hukum* 59, no. 2 (2026): 191–213. https://doi.org/10.14421/ajish.v59i2.1594.

Republik Indonesia. "Undang-Undang Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana," 2023.

———. "Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," 2024.

———. "Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi," 2022.

Romagna, Marco, and Rutger Erik Leukfeldt. "Social Opportunity Structures in Hacktivism: Exploring Online and Offline Social Ties and the Role of Offender Convergence Settings in Hacktivist Networks." *Victims & Offenders*, 2024, 1–23. https://doi.org/10.1080/15564886.2024.2372054.

Ropei, Ahmad. "The Resolution of Criminal Cases Through a Restorative Justice Approach in Islamic Law Perspective." *Jurnal Hukum Islam* 18, no. 2 (2020): 293–312. https://doi.org/10.28918/jhi.v18i2.2936.

Sarkar, Gargi, and Sandeep K. Shukla. "Behavioral Analysis of Cybercrime: Paving the Way for Effective Policing Strategies." *Journal of Economic Criminology* 2 (2023): 100034. https://doi.org/10.1016/j.jeconc.2023.100034.

Subagyono, Bambang Sugeng Ariadi, Mochamad Kevin Romadhona, Zahry Vandawati Chumaida, Bambang Suheryadi, and Noureldin Samy Elkhashab. "Can Indonesia's Laws Keep Up? Protecting Consumer Rights in Digital Transactions." *Journal of Law and Legal Reform* 5, no. 3 (2024): 869–90. https://doi.org/10.15294/jllr.v5i3.4202.

Surya, Reni. "Klasifikasi Tindak Pidana Hudud Dan Sanksinya Dalam Perspektif Hukum Islam." *Samarah: Jurnal Hukum Keluarga Dan Hukum Islam* 2, no. 2 (2019): 530–47. https://doi.org/10.22373/sjhk.v2i2.4751.

Telukdarie, Arnesh, and Aviksha Mungar. "The Impact of Digital Financial Technology on Accelerating Financial Inclusion in Developing Economies." *Procedia Computer Science* 217 (2023): 670–78. https://doi.org/10.1016/j.procs.2022.12.263.

Yalda, Rouwa, Arshad Khan, and Narayan Nepal. "B-PhishQR—A Blockchain-Based Framework for Secure QR Code Verification against Phishing Attacks." *Telematics and Informatics Reports* 21 (2026): 100289. https://doi.org/10.1016/j.teler.2025.100289.

Yonathan, Agnes Z. "Nilai Transaksi QRIS Tembus Rp128 Triliun Q3 2025." GoodStats Data, December 12, 2025. https://goodstats.id/article/nilai-transaksi-qris-tembus-rp128-triliun-q3-2025-vPpbG.