



Legal Problems with Qris Payment System Policy

Alfiansih Hasan^{1}, Dian Ekawaty Ismail^{2*}, Weny Almoravid Dungga^{3*}*

Universitas Negeri Gorontalo

alfiansih30@gmail.com, dian.ismail@ung.ac.id, wenyAD@ung.ac.id

ABSTRACT

This article aims to analyze the legal liability of perpetrators of misuse of QR-Code QRIS (Quick Response Code Indonesian Standard) in the context of digital payment systems in Indonesia. This study uses normative or doctrinal juridical methods by examining relevant legal provisions, such as the Information and Electronic Transactions Law (UU ITE) and the Banking Law. The results showed that perpetrators of QRIS abuse can be charged with criminal sanctions under Article 35 and Article 51 of the ITE Law, with a maximum criminal threat of 12 years in prison and/or a fine of up to Rp12 billion. In addition, the principle of customer confidentiality stipulated in the Banking Act is often an obstacle in the reporting and enforcement process. This calls for regulatory reforms that are more adaptive to the challenges of the digital age to improve surveillance, consumer protection, and public confidence in technology-based payment systems.

Keywords: QRIS, abuse, legal liability.

1. Background

Increasing human needs in the transaction process, presenting innovations to facilitate payment systems that are less practical with money in large transactions, then issued a transaction tool called checks and bilyet. The growth of technology developed by humans does not make humans stop developing payment systems that are used to facilitate the transaction process in everyday life. The presence of technology created cards (debit or credit cards) and electronic versions (e-money) whose use is carried out in electronic media connected to the internet and has been divided into several groups including E-wallets, E-Money, Fintech, Payment Gateway and the latest emerging is the Quick Response Code (QR Code).¹

The development of Industry 4.0 technology has created the emergence of a new industry called financial technology or commonly referred to as fintech. Fintech is part of the digital economy. Fintech puts technology as the basis of business in finance. The digital economy is a new activity related to virtual business and mutual transactions through exchange AIDS, namely internet technology.² Emerging fintechs provide ease of use related to various aspects of financial services, ranging from payment methods, fund transfers, and other methods. Fintech business is a financial innovation with a touch of modern technology, namely information technology to create new innovations in the financial services sector, which is faster and easier to use.³

One of them is an electronic payment system seen from the automatic monetary process, namely the exchange of value between parties in business transactions and the transmission of information value through information and Communication Technology Networks. Quick Response Code Indonesian Standard or commonly abbreviated as QRIS (read KRIS) is the unification of various QR from various payment system service providers (PJSP) using QR-code.⁴

Bank Indonesia issued a standard regulation on the use of Quick Response (QR Code) contained in the regulation of the Board of Governors number 21/18/PADG/ 2019 concerning the implementation of the use of Quick Response Code for payment systems.⁵ This QR Code includes a type of server-based electronic money payment, digital wallet, or internet banking which is often called the QR Code Indonesian Standard (QRIS) which has been enforced since January 1, 2020.⁶

¹ Izzani Ulf, "Tantangan dan Peluang Kebijakan Non-Tunai: Sebuah Studi Literatur", *Jurnal Ilmiah Ekonomi Bisnis*, Vol. 25 No. 1 (2020), h. 55–65, tersedia pada <https://doi.org/10.35760/eb.2020.v25i1.2379> (2020).

² Puluhalawa, J., Muhtar, M. H., Towadi, M., & Swarianata, V. *Apripari*. (2023). *The Concept of Cyber Insurance as a Loss Guarantee on Data Protection Hacking in Indonesia*. *Law, State and Telecommunications Review*, 15 (2), Article 2.

³ I Suastrawan dan Anak Kusuma, "Perlindungan hukum terhadap konsumen dalam transaksi elektronik dengan sistem pembayaran QR Code", *Jurnal Kertha Wicara*, Vol.10 No. 6 (2021), h. 419–429, tersedia pada <https://www.cnnindonesia.com/teknologi/20181128150502-185-349939/peranan-qr-code-> (2021).

⁴ Sri Adiningsih, *Transformasi Ekonomi Berbasis Digital...Op.Cit*, hlm 92.

⁵ Dungga, W. A., Muhtar, M. H., & Djaafar, L. (2023). The Assessment of Indonesia's Religious Courts in Resolving Shari'ah Banking Disputes According to the Principles of Justice. *Manchester Journal of Transnational Islamic Law & Practice*, 19(3), 179.

⁶ Onny Widjanarko, "QRIS Satu QR Code Untuk Semua Pembayaran", *Bank Indonesia*, https://www.bi.go.id/id/publikasi/ruang-media/news-release/Pages/SP_216219.aspx 17 Agustus 2019, diakses pada 2 September 2023

Quick Response Code (QR Code) is a code written in software that is realized in a pattern that is connected to the internet network system. A pattern consisting of several corners arranged in a mobile device that is activated to make payments. This pattern can store data in the form of alphanumeric, character, and symbol. The Data is used as a scan in the transaction as the transfer of a certain amount of money to make a payment.⁷

Type of payment using QRIS itself there are 3 kinds. Two of them will ask to scan the QR Code contained in one and the other is the truth, namely the QR Code that will be seen by The Merchant. The types of payments using QRIS consist of: static Merchant Presented Mode (MPM), dynamic Merchant Presented Mode (MPM), Customer Presented Mode (CPM).⁸

The use of QRIS certainly can not be separated from the advantages and disadvantages,⁹ the advantages of QRIS include being able to be used by anyone, facilitating transactions, payment system efficiency, and fast transactions. The weakness of QRIS is that the nominal transaction is limited, there is a threat of system error constraints, has a maximum transaction cost, and a serious threat of criminalization actions such as QRIS code forgery.

Some cases of QRIS code forgery committed by perpetrators of criminal acts, one of which is the attachment of QRIS codes carried out in several mosque charity boxes in the Jakarta area, namely Pondok Indah, Kalibata and kebayoran lama. There are approximately 12 mosques that have carried out charity box forgery.¹⁰

This case of QRIS forgery only began to appear to the public in 2023 and the more widespread this happens, causing concern for businesses and other QRIS service users. Researching the procedure for making QRIS is reported from the official website of Bank Indonesia and the researchers described above, there are several institutions that can provide access to QRIS Barcode registration, namely Banking and non-banking institutions. The ease of obtaining the QRIS code is an opportunity for criminals to launch their actions. According to Erwin Haryono, Executive Director of the bi Communication Department, the lack of verification and Know Your Merchant processes carried out by Payment Service Providers (PJP) and Payment System Service Providers (PJSP) authorized to issue QRIS barcodes, so this is an opportunity for criminals.¹¹

The main problem in using QRIS lies in the weakness of the verification and supervision system carried out by Payment Service Providers (PJP) and Payment System Service Providers (PJSP). The Know Your Merchant (KYM) process that is supposed to ensure the validity of the identity and intended use of QRIS is often not carried out optimally. As a result, criminals can easily create or falsify QRIS codes for criminal purposes, such as the case of sticking fake QRIS codes on mosque charity boxes in various areas of Jakarta.

The lack of supervision and lack of awareness of these potential risks exacerbate the situation, causing not only material losses for users, but also threatening public confidence in this digital-based payment system. In addition, the ease of gaining access to QRIS registration without a rigorous verification process provides a huge loophole for abuse. This shows that there is a gap between the development of payment technology and the implementation of regulations and effective security mechanisms.

On the other hand, threats to QRIS security not only affect individual users, but also businesses that rely on the system for their business operations. Fear of fraud or counterfeiting could potentially hinder the growth of adoption of QRIS as an efficient digital payment solution. As such, the issue calls for concrete steps from the authorities, including increased merchant verification standards, tighter supervision, and education to the public on how to recognize and avoid fake QRIS codes.

II. Rumusan Masalah

What is the legal liability for perpetrators of misuse of QR-Code QRIS?

III. Metode Penelitian

Normative research is understood as research to test a norm or applicable provision. It can also be said that research is carried out by researching library materials or secondary data. Because this research focuses on library materials, normative research is often also called doctoral research or library research. This type of research is the main characteristic in legal research, even though legal research is often identified with only normative research. Some jurists argue that normative legal research is the only type or category of research known in legal Science. Although in its development, legal research was strengthened and supplemented by empirical legal research or sociological research, which later emerged the term socio-legal research to accommodate all research originating from social science disciplines on legal phenomena as the object of study.¹²

Legal liability for perpetrators of misuse of QR-Code QRIS can be analyzed through a normative approach that focuses on applicable legal rules and criminal provisions related to digital crimes. In this case, the perpetrator of the misuse of the QRIS QR-Code may be subject to criminal liability

⁷ Wang, Y., Tian, X., Zhang, H., Yang, Z., & Yin, X. (2018). Anticounterfeiting Quick Response Code with Emission Color of Invisible Metal–Organic Frameworks as Encoding Information. *ACS Applied Materials & Interfaces*, 10(26), 22445–22452. <https://doi.org/10.1021/acsami.8b06901>

⁸ Bank Indonesia, "Jenis Pembayaran Menggunakan QRIS", QRIS.id, <https://www.bi.go.id/QRIS/default.aspx#QRIS> diakses 2 September 2023

⁹ Ana Srikaningsih, QRIS dan Era Baru Transaksi Pembayaran 4.0 (Yogyakarta: Penerbit ANDI, 2020), 3

¹⁰ Isna Rifka, Fakta-fakta Pemalsuan QRIS Kotak Amal Masjid, <https://money.kompas.com/read/2023/04/11/090600126/fakta-fakta-kasus-pemalsuan-qr-is-kotak-amal-masjid?page=all> diakses Pada Tanggal 4 September 2023

¹¹ Departemen Komunikasi, Bank Indonesia https://www.bi.go.id/id/publikasi/ruang-media/news-release/Pages/sp_2513123.aspx Diakses Pada 6 September 2023

¹² Irwansyah, "Penelitian Hukum: Pilihan Metode & Praktik penulisan Artikel" Yogyakarta: Mirra Buana Media, 2021. Hlm. 42.

under Article 30 paragraph (1) of Law Number 19 of 2016 concerning amendments to Law Number 11 of 2008 concerning electronic information and transactions (UU ITE), which states that any person who intentionally and without the right to access electronic systems belonging to others unlawfully can be punished. In addition, if this act of abuse is carried out with the aim of obtaining benefits or causing harm to another party, the perpetrator can be charged under Article 36 of the ITE Law, which provides for criminal threats for acts that cause material harm.

In the context of QR-Code QRIS, misuse such as code forgery can be considered as fraudulent acts that utilize digital technology. Perpetrators who are proven to have committed such acts may be subject to criminal sanctions under Article 378 of the Criminal Code (KUHP) on fraud, which provides that any person who with the intention of benefiting themselves or others unlawfully, using deception or a series of lies, may be punished. In addition, payment service providers (PJPS) or payment system service providers (PJSP) who are negligent in the verification and supervision process may be held administratively liable in accordance with Bank Indonesia regulations on payment systems. Thus, the legal liability for perpetrators of QRIS QR-Code abuse includes criminal aspects for perpetrators of crimes and administrative aspects for parties who fail to carry out their obligations in the management and supervision of QRIS. This law enforcement effort needs to be done decisively to protect users, prevent similar crimes in the future, and maintain public trust in digital payment systems.

IV. Discussion

The dynamics of the digital payment system have important implications for the financial system in Indonesia and this is in line with the increasing needs of an increasingly fast and diverse society. In addition, the convenience and cost-efficient factor is also a fundamental reason for people to prefer non-cash payments.¹³

Quick Response Code Indonesia Standard or known as QRIS has been implemented in Indonesia through Bank Indonesia since 2019. The massive use of technology in everyday life today is increasingly facilitated by the existence of QRIS. According To Bank Indonesia Regulation No.20/6/PBI / 2018 concerning electronic money Article 3 Paragraph (2) states that one of the electronic money storage media is in the form of a server, where one form of server-based electronic payment is payment through a Quick Response Code (QR) code.¹⁴

The payment method through QRIS embodies the principles of digitization, economic integration and National digital Finance. The existence of a payment method using QRIS carries the principle of security and consumer protection, as stipulated in Bank Indonesia Board of Governors Regulation No. 21/18 / PADG/2019 concerning the implementation of the Quick Response Code national standard for payments as amended in Board of Governors Regulation No. 23/8 / PADG/2021 concerning amendments to board of Governors Regulation No. 21/18 / PADG/2019 concerning, and the last amendment to the regulation of members of the Board of Governors number 24/1/ PADG /2022 concerning the Second Amendment to the regulation of members of the Board of Governors number 21/18/PADG/2019 concerning the implementation of the National Quick Response Code standard for payments.

QRIS is basically where various QR codes from various payment system service providers are put together, QR codes from any payment system service provider can be accessed through QRIS. Based on Article 11 of PADG QRIS, All Payment System Service Providers (PJSP) are required to obtain approval from Bank Indonesia by submitting an application and must meet the requirements in the form of:

1. Operational readiness
2. System safety and reliability
3. Application of risk management
4. Consumer protection

Currently, there are a number of payment system service providers who have obtained QRIS approval, ranging from Bank Buku 4, Non-Bank, to Switching, however, the ease of payment through QRIS is also accompanied by a rampant incidence of fraud in the form of counterfeit QRIS code stickers that have occurred lately. The actors in the financial system have certainly promised the security of transacting through QRIS.

In the increasingly sophisticated digital age, legal protection of personal data has become very important it is very important to ensure the privacy of individuals and stop the misuse of data.¹⁵ Security problems that can arise if hackers change the QRIS code to point to the hacker's account. The Bank explained that this problem has been minimized by a layered verification process. This layered verification requires the cooperation of QRIS users to continue to be vigilant in rechecking the funds sent transactions so that they are not sent to irresponsible hackers. During the verification process, the sender needs to make sure that the merchant name displayed on the QRIS application is the same as the merchant who is currently transacting with the sender. As a QRIS user, the public is obliged to maintain the confidentiality of the PIN by not spreading it to any party.¹⁶

QRIS (Quick Response Code Indonesian Standard) as a QR Code technology in electronic payments. QRIS is an integration system of various QR codes issued by various payment system service providers (PJSP). The existence of QRIS makes it easy to conduct every digital transaction quickly and

¹³ Ciplis Gema Qori'ah, dkk. "Dampak Perkembangan Uang Elektronik terhadap Efektivitas Kebijakan Moneter di Indonesia, Jurnal Ekonomi Indonesia", Vol. 9 No. 3, 2020, h. 266

¹⁴ Willa Wahyuni. 2023. "Marak Penipuan, Ini Cara Aman Menggunakan QRIS." <https://www.hukumonline.com/berita/a/marak-penipuan--ini-cara-aman-menggunakan-qr-is-1t6436871a70209/?page=all> Diakses 14 September 2024

¹⁵ HH. Samin, Dian Ekawaty Ismail, Erman I. Rahim, "The Urgency Of Legal Protection Of Personal Data", DE LEGA LATA: Jurnal Ilmu Hukum, Vol. 9 No. 2 (2024), h. 146

¹⁶ Willa Wahyuni. Op.Cit

efficiently and securely. The advancement of technology has given us everything. On the other hand, it is still necessary to be careful with the existing risks.

As an example of a case that occurred not long ago, namely the falsification of QRIS by parties who are not responsible and understand the weaknesses of parties who use QRIS as a means of payment. A man falsified QRIS barcodes for charity boxes at several mosques in South Jakarta. This QRIS forgery was caught on CCTV cameras when the perpetrator carried out his action at the Nurul Iman Mosque Blok M Square.

A similar case befell a mother named Rani, a street food vendor corndog in Bekasi, there was someone who put a fake QRIS on his business cart, until now Rani did not know who the perpetrator who put the fake QRIS. Rani was about to report the case to the authorities. Unfortunately Rani actually encountered obstacles regarding evidence. Rani did not have enough preliminary evidence to get the authorities to follow up.

Legally, usually a person needs to have sufficient preliminary evidence to open a police report as stipulated in Article 17 (KUHAP) which reads: "preliminary evidence to suspect a criminal offense in accordance with Article 1 Item 14 of the Criminal Procedure Code". While in Article 1 point 14 of the code of Criminal Procedure regulates that the suspect is a person who because of his actions or circumstances, based on preliminary evidence should be suspected as the perpetrator of a criminal offense.¹⁷

Lamintang argued that practically sufficient preliminary evidence is defined as "minimal evidence". The minimum evidence in question is evidence that has been regulated in Article 184 paragraph (1) of the Criminal Procedure Code. Sufficient preliminary evidence is preliminary evidence to suspect the existence of a criminal act committed by a person, so that when an arrest is made it is not done arbitrarily, but is directed to those who actually because of their actions committed a criminal offense.¹⁸

In terms of its function, sufficient preliminary evidence has two categories, namely as a prerequisite for:¹⁹

1. Conduct an investigation, namely to suspect the existence of a criminal offense, so that it can rise at the next stage, namely the investigation stage
2. Establish the status of a suspect against a person suspected of having committed a criminal offense

If reviewed from Law No. 10 of 1998 on amendments to Law No. 7 of 1992 on Banking (Banking Law), the provisions on bank secrets are regulated in Article 40 paragraph (1): "The Bank is obliged to keep the information about its Depository and depository customers confidential, except in the case referred to in Article 41, article 41A, Article 42, Article 43, Article 44, and Article 44A" Although there are exceptions from Article 40 of the banking law, such exceptions are only granted for judicial purposes as provided for in Article 42 jo. 42A of the Banking Act. Article 42 it reads:

- 1) for judicial purposes in criminal cases, the head of Bank Indonesia may grant permission to the police, prosecutors, or judges to obtain information from the bank regarding the suspect's or defendant's deposits with the bank.
- 2) the permission as meant in Paragraph (1) is granted in writing upon a written request from the Chief of Police of the Republic of Indonesia, the attorney general, or the chairman of the Supreme Court.
- 3) the request as meant in Paragraph (2) must mention the name and position of the police, prosecutor, or judge, the name of the suspect or defendant, the reason for the need for information and the relationship of the criminal case concerned with the necessary information."

Referring to the provisions above, obtaining written permission from the head of Bank Indonesia must at least be with a prior written request from the head of the Indonesian National Police. Reflecting on Rani's case, the process that must be taken is quite complicated and poses a dilemma. On the other hand, Rani had to face the stagnation of the police report due to the lack of sufficient preliminary evidence in making a report. Not to mention the increasingly complicated procedure for obtaining information from the bank as described above. Plus a rejection from the bank. Although initially experiencing rejection, Rani got a solution after consulting and explaining the conditions she experienced with one of the related banks. The Bank offered to help by suggesting Rani make a report explaining the chronology in detail via email which the bank responded to through the investigation team. Then, the bank promised to process Rani's request for 2-3 working days to help her problems. However, such assistance still does not guarantee that the bank will open information about the perpetrators.²⁰

The principle of QR-Code or Quick Response Code is the development of Bar-Code which was once a one-dimensional code into a two-dimensional code with the ability to store data that can be stored in the form of numeric, letter, binary, and kanji codes.²¹ QR-Code is a matrix code created by the

¹⁷ Harahap, T. K., Prayuti, Y., Latianingsih, N., Damanik, A., Maheni, T., Farida, I., & Muhtar, M. H. *Mustaqim*.(2023). *PENGANTAR ILMU HUKUM*. Penerbit Tahta Media. Hlm. 97

¹⁸ Benedictus S. Habonaran. 2023. "Kompleksitas Pembuktian Tindak Pidana Pemalsuan QRIS dan Peran Bank Indonesia." <https://www.hukumonline.com/berita/a/kompleksitas-pembuktian-tindak-pidana-pemalsuan-qr-is-dan-peran-bank-indonesia-1t64d9b5fda87be/?page=all> (Diakses pada 10 September 2024)

¹⁹ Ibid

²⁰ Ibid

²¹ Joseph Dedy Irawan dan Emmalia Adriantantri. *Pemanfaatan QR-Code Sebagai Media Promosi Toko*. Jurnal MNEMONIC, Vol. 1, No. 2, 2018, hal. 56.

Japanese company Denso-Wave in 1994. In essence, QR-Code is a form of evaluation of the Bar-Code that we usually see on a product that contains various information in it such as URL addresses, text, to phone numbers.²²

Code or QRIS is included in the electronic data. Therefore, based on the ITE Law, the perpetrators of QR-Code forgery may be subject to the following articles:

Article 35 of the Electronic Information and Transaction Law (UU ITE) provides that any person who intentionally and without rights or against the law manipulates, creates, changes, removes or destroys electronic information and/or electronic documents with the aim that such electronic information and/or electronic documents are considered as if they were authentic data, may be subject to criminal sanctions. This provision is reinforced by Article 51 paragraph (1) of the ITE Law which stipulates that perpetrators who meet the elements referred to in Article 35 shall be punished with a maximum imprisonment of 12 years and/or a maximum fine of Rp12, 000, 000, 000.00. In addition, if the dissemination of a false QR-Code or QRIS by the perpetrator causes harm to others, the perpetrator may be subject to additional penalties in the form of a maximum prison of 6 years and/or a maximum fine of Rp1, 000, 000, 000.00, in accordance with the criminal provisions of the ITE Law.²³

The conclusion of this discussion highlights the importance of strengthening regulation and law enforcement against the misuse of QR-Code or QRIS as a form of digital crime. In the legal context, there is a lack of norms that specifically regulate the misuse of QR-codes as part of modern financial transactions, although related regulations such as the ITE Law and the banking law have provided a legal basis for cracking down on perpetrators. However, the complexity of legal procedures, such as written permission to disclose customer data, suggests there are significant barriers to law enforcement.

In an effort to protect society from this crime, there is a need to develop policies that are more adaptive to technological developments, including simplifying the process of access to information for the authorities without compromising the principle of bank secrecy. In the future, strengthening the supervision mechanism for QRIS service providers, both in technical aspects and user verification, is also an important agenda to minimize the potential for abuse.

The Novelty of this discussion lies in the integrative perspective between criminal law and banking regulation, especially in the context of electronic data falsification that has an impact on financial transactions. This review contributes to the legal literature by emphasizing the need for legal reform that accommodates new challenges in the era of digitalization, while underlining the importance of collaboration between banks, payment system providers, and law enforcement officials to create a safer and more trusted financial ecosystem.

V. Conclusion

In legal liability against perpetrators of QR-Code QRIS abuse, victims usually need to have sufficient preliminary evidence to open a police report as stipulated in Article 17 (KUHP), on the other hand, the bank holds the principle of confidentiality of customer information based on Law Number 10 of 1998, so this will hamper the reporting process when it does not have evidence of data/information about, or judge to obtain information from the bank regarding customer information (suspect or defendant).

Reference

- Abdussamad, Z., Harun, A. A., Muhtar, M. H., Puluhulawa, F. U., Swarianata, V., & Elfikri, N. F. (2024). Constitutional balance: Synchronizing energy and environmental policies with socio-economic mandates. In *E3S Web of Conferences* (Vol. 506). EDP Sciences.
- Habonaran, B. S. (2023). Kompleksitas pembuktian tindak pidana pemalsuan QRIS dan peran Bank Indonesia. *Hukumonline.com*. <https://www.hukumonline.com/berita/a/kompleksitas-pembuktian-tindak-pidana-pemalsuan-qr-is-dan-peran-bank-indonesia-lt64d9b5fda87be/?page=all>
- Bank Indonesia. (n.d.). Jenis pembayaran menggunakan QRIS. *QRIS.id*. <https://www.bi.go.id/QRIS/default.aspx#QRIS>
- Bullah, N. (2020). Tindak pidana tidak melakukan pengelolaan limbah medis bahan berbahaya dan beracun (B3) terhadap lingkungan hidup (suatu penelitian di wilayah hukum kepolisian resor Aceh Barat). *JIM Bidang Hukum Pidana*, 4(1).
- Brendel, S., Fetter, É., Staupe, C., Vierke, L., & Biegel-Engler, A. (2018). Short-chain perfluoroalkyl acids: Environmental concerns and a regulatory strategy under REACH. *Environmental Sciences Europe*, 30(1). <https://doi.org/10.1186/s12302-018-0134-4>
- Irawan, J. D., & Adriantantri, E. (2018). Pemanfaatan QR-code sebagai media promosi toko. *Jurnal MNEMONIC*, 1(2).
- Irwansyah. (2021). *Penelitian hukum: Pilihan metode & praktik penulisan artikel*. Mirra Buana Media.
- Jayanti, D. D. (2023). Penyebar QRIS palsu, ini jerat hukumnya. *Hukumonline.com*. <https://www.hukumonline.com/klinik/a/penyebar-qr-is-palsu--ini-jerat-hukumnya-lt6436783926f9e/>

²² Dian Dwi Jayanti. 2023. "Penyebar QRIS Palsu, Ini Jerat Hukumnya." <https://www.hukumonline.com/klinik/a/penyebar-qr-is-palsu--ini-jerat-hukumnya-lt6436783926f9e/> Diakses pada 12 September 2024

²³ Pasal 28 ayat 1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ("UU ITE") jo. Pasal 1 angka 8 Undang-Undang Nomor 19 tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ("UU 19/2016") yang menambah baru Pasal 45A ayat (1) UU ITE.

- Maulana, A. (2020). Penegakan hukum lingkungan pidana terhadap perusahaan yang melakukan dumping limbah bahan berbahaya dan beracun (limbah B3). *Lex Administratum*, VIII(5).
- Mardikanto, T. (2014). *Corporate social responsibility (Tanggungjawab sosial korporasi)*. Alfabeta.
- Mamondol, S. A. T., Tampongongoy, G. H., & Korah, R. S. M. (2018). Aspek pengelolaan limbah medis cair sakit terhadap pencegahan pencemaran lingkungan. *Jurnal Hukum*, 12(1).
- Muhtar, M. H., Harun, A. A., Putri, V. S., Apripari, A., & Moha, M. R. (2024). Addressing the paradox: Why environmental constitutionalism is more than just rights? In *E3S Web of Conferences* (Vol. 506). EDP Sciences.
- Muhtar, M. H., Pedrason, R., & Harryarsana, I. G. K. B. (2023). Human rights constitution on health protection of Indonesian citizens. *Russian Law Journal*, 11(2).
- Onny Widjanarko. (2019, August 17). QRIS Satu QR Code Untuk Semua Pembayaran. *Bank Indonesia*. https://www.bi.go.id/id/publikasi/ruang-media/news-release/Pages/SP_216219.aspx
- Puluhulawa, J., Muhtar, M. H., Towadi, M., & Swarianata, V. A. (2023). The concept of cyber insurance as a loss guarantee on data protection hacking in Indonesia. *Law, State and Telecommunications Review*, 15(2), Article 2.
- Purwanto, N. R. (2020). Pengaturan pengelolaan limbah medis Covid-19. *Jurnal Yustika*, 23(02).
- Qori'ah, C. G., et al. (2020). Dampak perkembangan uang elektronik terhadap efektivitas kebijakan moneter di Indonesia. *Jurnal Ekonomi Indonesia*, 9(3).
- Rifka, I. (2023, April 11). Fakta-fakta pemalsuan QRIS kotak amal masjid. *Kompas.com*. <https://money.kompas.com/read/2023/04/11/090600126/fakta-fakta-kasus-pemalsuan-qr-is-kotak-amal-masjid?page=all>
- Rs, I. R., Muhtar, M. H., Harun, A. A., Bakung, D. A., & Junus, N. (2023). Protection of human rights against the environment in the Indonesian legal system. *Journal of Law and Sustainable Development*, 11(10).
- Setiawan, D., & Muhtar, M. H. (2023). Contemplating the morality of law enforcement in Indonesia. *Journal of Law and Sustainable Development*, 11(10).
- Srikaningsih, A. (2020). *QRIS dan era baru transaksi pembayaran 4.0*. Penerbit ANDI.
- Soekanto, S., & Mamudji, S. (2011). *Penelitian hukum normatif*. PT. Raja Grafindo Persada.
- Suastrawan, I., & Anak Kusuma. (2021). Perlindungan hukum terhadap konsumen dalam transaksi elektronik dengan sistem pembayaran QR Code. *Jurnal Kertha Wicara*, 10(6). <https://www.cnnindonesia.com/teknologi/20181128150502-185-349939/peranan-qr-code>
- Supriyadi. (2023, March 22). Limbah medis ditemukan di tumpukan sampah pekarangan warga di Jombang. *Kompas.com*. <https://pemilu.kompas.com/read/2023/03/22/095152178/limbah-medis-ditemukan-di-tumpukan-sampah-pekarangan-warga-di-jombang>
- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), jo. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU 19/2016) yang menambah baru Pasal 45A ayat (1) UU ITE.
- Wahyu, W. (2023). Marak penipuan, ini cara aman menggunakan QRIS. *Hukumonline.com*. <https://www.hukumonline.com/berita/a/marak-penipuan--ini-cara-aman-menggunakan-qr-is-lt6436871a70209/?page=all>
- Wang, Y., Tian, X., Zhang, H., Yang, Z., & Yin, X. (2018). Anticounterfeiting Quick Response Code with emission color of invisible metal-organic frameworks as encoding information. *ACS Applied Materials & Interfaces*, 10(26), 22445–22452. <https://doi.org/10.1021/acsami.8b06901>
- Wantu, F., Muhtar, M. H., Putri, V. S., Thalib, M. C., & Junus, N. (2023). Eksistensi mediasi sebagai salah satu bentuk penyelesaian sengketa lingkungan hidup pasca berlakunya Undang-Undang Cipta Kerja. *Bina Hukum Lingkungan*, 7(2), 267-289.