Legal Protection of Personal Data in Electronic Transactions through the QRIS Payment System in Indonesia

Sri Windani, Pretty Fakhirah, Farabian Saleh, M. Alamsyah

Abstract

The development of digital technology has encouraged people to switch to electronic payment systems, one of which is through QRIS (*Quick Response Code Indonesian Standard*) developed by Bank Indonesia. However, behind this convenience there is a potential breach of consumer personal data that can occur due to weak supervision and understanding of users. This article examines how the legal protection of personal data in electronic transactions using QRIS is regulated in Indonesia, including challenges and solutions to ensure users' rights. The research method used is normative juridical with a legislative approach and a conceptual approach. This study found that although there are legal tools such as the Personal Data Protection Law, ITE Law, and regulations from Bank Indonesia, their implementation is still not optimal due to weak supervision and lack of digital literacy. Therefore, it is necessary to strengthen derivative regulations, public socialization, and stricter technical supervision of payment system service providers.

***Keywords**:* Legal Protection, Personal Data, QRIS (Quick Response Code Indonesian Standard)

Sri Windani[1]
[1]Lecturer of Bachelor of Law,Universitas Putra Abadi Langkat, Indonesia
e-mail: sriwindani@gmail.com[1]

Pretty Fakhirah[2], Farabian Saleh[3], M. Alamsyah[4]
[2,3,4]Student of the Law, Universitas Putra Abadi Langkat, Indonesia
e-mail: pretty.fakhirah.pf@gmail.com[2], farabiansaleh6@gmail.com[3],
muhammadalamsyah029@gmail.com[4]

2nd International Conference on Islamic Community Studies (ICICS)
Theme: History of Malay Civilisation and Islamic Human Capacity and Halal Hub in the Globalization Era

Introduction

The advancement of information and communication technology has brought significant changes to various aspects of human life, including the economic and financial sectors. Digital transformation has encouraged the emergence of innovations in payment systems aimed at improving efficiency, speed, and convenience in transactions[1]. One of Indonesia's key innovations is the implementation of the *Quick Response Code Indonesian Standard* (QRIS), developed by Bank Indonesia as a standardized QR-based payment system. Since its launch on August 17, 2019, and nationwide implementation on January 1, 2020, QRIS has become a major instrument in supporting the *National Non-Cash Movement* (*Gerakan Nasional Non-Tunai* or GNNT) and expanding financial inclusion. QRIS is designed to integrate various *Payment System Service Providers* (PJSPs), allowing transactions across different platforms through a single QR code. This innovation provides convenience and efficiency for users, particularly for *Micro, Small, and Medium Enterprises* (MSMEs) that increasingly participate in the digital economy ecosystem[2].

However, behind these conveniences lies a significant challenge concerning personal data protection. Each transaction through QRIS involves personal information such as names, phone numbers, locations, and account numbers, which can be misused if not properly managed. This issue has become increasingly relevant as Indonesia ranks among the top five countries with the highest number of personal data breaches globally, according to research by Surfshark[3]. The main contributing factors include weak supervision and low digital literacy among the public. In the context of digital payment systems, the misuse of personal data may occur when user data is collected, stored, or processed by PJSPs or third parties without the explicit consent of the data owner. Such practices clearly violate citizens' constitutional rights as guaranteed by Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which ensures protection of personal privacy and data security[4].

In response to the growing threat to privacy, the Indonesian government enacted Law No. 27 of 2022 on Personal Data Protection (PDP Law). This regulation serves as the first comprehensive legal framework governing data subject rights, data controller obligations, and administrative as well as criminal sanctions for personal data violations[5]. Alongside the PDP Law, Law No. 11 of 2008 on Electronic Information and Transactions (EIT Law) and several Bank Indonesia regulations also provide legal provisions for digital payment security. Nevertheless, the implementation of legal protection for personal data in QRIS transactions still faces several obstacles, including weak supervision, regulatory overlaps, and low legal awareness among both service providers and users.

Based on these issues, this study aims to analyze the legal protection mechanisms for personal data in electronic transactions using QRIS and to examine the responsibility of payment system service providers in safeguarding user data. Furthermore, this research seeks to formulate legal solutions that can ensure optimal protection for QRIS users. The study is expected to contribute to strengthening regulatory frameworks, enhancing oversight effectiveness, and promoting public legal literacy in the use of digital payment systems. Ultimately, this will help maintain public trust in Indonesia's digital financial ecosystem and support the realization of a secure, transparent, and equitable financial transformation.

Literature Review

The development of digital technology has transformed the paradigm of global economic transactions, including in Indonesia. In the legal context, this transformation demands regulatory updates that ensure the protection of personal data as part of fundamental human rights. Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia

guarantees every individual the right to personal protection, including the security of personal data in digital environments. Therefore, legal protection of personal data is not merely a technical necessity but a constitutional imperative[6].

The legal framework underlying this study consists of several key instruments. First, Law No. 27 of 2022 on Personal Data Protection (PDP Law) serves as the primary legal basis governing data subject rights, data controller and processor obligations, as well as administrative and criminal sanctions for violations. Second, Law No. 11 of 2008 on Electronic Information and Transactions (EIT Law) and its derivatives provide legal recognition for electronic transactions and establish the responsibility of electronic system providers in safeguarding user data. Third, Bank Indonesia Regulation No. 23/6/PBI/2021 on Payment System Operations regulates the security, interoperability, and integrity of digital payment systems, including QRIS[7].

In addition to the legal framework, this study employs a conceptual approach, drawing upon the theories of legal protection and legal liability. According to Philipus M. Hadjon, legal protection aims to safeguard the rights of legal subjects from arbitrary actions, whether by the state or other powerful entities[8]. In this context, the protection of personal data must guarantee the individual's right to privacy, security, and control over the use of their data. Meanwhile, legal liability theory emphasizes that any party committing a violation or negligence in fulfilling its obligations must bear legal consequences, including compensation, administrative sanctions, or criminal penalties[9].

Thus, this literature review serves as a theoretical foundation to analyze how existing legal mechanisms provide protection for users' personal data in electronic transactions using QRIS, and how payment system service providers are held accountable for ensuring the security and integrity of user information.

Research Methodology

This study employs a normative juridical research method with both a statutory approach and a conceptual approach[10]. This method was chosen because the research problem is closely related to the analysis of existing legal norms in Indonesia and the underlying legal principles governing personal data protection in electronic transactions[11].

The statutory approach is applied to examine various laws and regulations related to personal data protection and electronic payment systems, including Law No. 27 of 2022 on Personal Data Protection (PDP Law), Law No. 11 of 2008 on Electronic Information and Transactions (EIT Law) and its amendments, as well as Bank Indonesia Regulations governing QRIS-based payment systems. These instruments are analyzed to assess how far the existing legal framework provides adequate protection for users' personal data in digital transactions.

The conceptual approach is used to explore the fundamental concepts of legal protection and legal liability within the digital transaction context. This approach enables the research to go beyond written norms and examine the underlying values, principles, and legal theories that inform the development of relevant legislation.

The data used in this research are secondary data, obtained through library research comprising primary, secondary, and tertiary legal materials. Primary legal materials include laws and regulations; secondary materials consist of books, scholarly journals, and previous studies; and tertiary materials include legal dictionaries, encyclopedias, and credible online sources.

The data analysis employs a descriptive-analytical method, which involves describing and interpreting the applicable laws while assessing their practical implementation in QRIS

usage. Through this analysis, the study aims to provide a comprehensive understanding of the legal protection mechanisms for personal data in electronic transactions using QRIS and to propose relevant and applicable legal solutions to strengthen data protection systems in Indonesia.

Results

4.1 Legal Protection and the Responsibility of Payment System Service Providers (PJSPs) in Electronic Transactions Using QRIS

Legal protection of personal data in electronic transactions using QRIS is rooted in the constitutional right to privacy, as guaranteed by Article 28G paragraph (1) of the 1945 Constitution of Indonesia. In practice, this protection is implemented through legal instruments such as Law No. 27 of 2022 on Personal Data Protection (PDP Law), Law No. 11 of 2008 on Electronic Information and Transactions (EIT Law), and Bank Indonesia Regulation No. 23/6/PBI/2021 on Payment System Operations[12].

The PDP Law emphasizes that all data processing must comply with principles of lawfulness, transparency, purpose limitation, and accountability. In the QRIS context, Payment System Service Providers (PJSPs) act as data controllers responsible for collecting, storing, and processing user information[13]. They must obtain explicit consent from data subjects and maintain the integrity and security of user data to prevent misuse or unauthorized access[14]. However, findings indicate that implementation remains suboptimal. Challenges include:

- Weak regulatory supervision of PJSP compliance with data protection standards;
- Lack of integrated technical guidelines on data protection in digital payment services; and
- Low user awareness of their data rights, leading to passive acceptance of data processing without explicit consent.

These gaps increase the risk of personal data misuse for commercial purposes or data breaches caused by inadequate system security[15]. Therefore, PJSPs bear legal responsibility not only for maintaining technical safeguards but also for implementing *due diligence* and transparency in data management[.

From a legal perspective, PJSP responsibilities can be categorized as:

1. Preventive responsibility, ensuring system security from the design stage (*security by design*);
2. Repressive responsibility, providing notification and compensation to users in case of data breaches; and
3. Administrative and criminal liability, when negligence or misuse occurs as stipulated in Articles 58–62 of the PDP Law.

Thus, effective legal protection of personal data in QRIS transactions depends on both robust regulatory mechanisms and strict compliance by PJSPs under continuous supervision by authorities.

4.2 Legal Solutions to Address Personal Data Breaches in QRIS Transactions

Personal data breaches in QRIS transactions pose significant threats, including loss of public trust and potential financial harm to users. Therefore, legal solutions must encompass preventive, corrective, and educational strategies to ensure comprehensive protection. From a preventive standpoint, the government must develop implementing regulations under the PDP Law that specifically address data protection within financial technology services, including QRIS. These should define minimum security standards, mandatory audit mechanisms, and clear *incident reporting* procedures for PJSPs[17].

From a corrective standpoint, regulatory oversight by Bank Indonesia and the Financial Services Authority (OJK) should be strengthened through more rigorous enforcement and sanctions for non-compliance. Legal enforcement must involve coordinated actions between supervisory bodies, law enforcement agencies, and data protection authorities to ensure administrative and criminal accountability.

From an educational perspective, improving public digital literacy is essential. Users must be aware of their data rights and how to safeguard their personal information when using digital payment systems. Public awareness campaigns, cybersecurity training, and legal education initiatives are vital to empowering consumers[18].

By implementing these strategies, Indonesia can build a safer and more trustworthy digital payment environment where QRIS operates not only as an efficient financial tool but also as a system that upholds the highest standards of personal data protection.

Conclusion

Based on the analysis, it can be concluded that legal protection of personal data in electronic transactions using QRIS is a fundamental aspect of the state's obligation to uphold citizens' constitutional rights to privacy and data security. Although Indonesia has established legal instruments such as Law No. 27 of 2022 on Personal Data Protection (PDP Law), Law No. 11 of 2008 on Electronic Information and Transactions (EIT Law), and Bank Indonesia Regulation No. 23/6/PBI/2021 on Payment System Operations, their implementation remains suboptimal in practice.

Payment System Service Providers (PJSPs), as data controllers, bear legal responsibility for ensuring the confidentiality, integrity, and security of users' personal data. However, weak oversight, the absence of specific technical guidelines, and low levels of legal and digital literacy among users have hindered effective protection. The PJSPs' legal responsibilities include preventive duties (preventing data breaches), repressive duties (managing incidents and providing compensation), and administrative or criminal liabilities for negligence or data misuse.

Thus, the effectiveness of legal protection for personal data in QRIS transactions depends not only on the existence of regulations but also on consistent law enforcement, active supervision by authorities, and increased public awareness regarding data privacy in digital payment systems.

References

[1] F. M. Pattynama, H. A. Santoso, F. R. D. Miarsa, dan T. Pribadi, "Legal Problems for Quick Response Code Indonesian Standard (Qris) Users in Online Payment

Transactions," *Anayasa J. Leg. Stud.*, vol. 2, no. 1, hal. 44–55, 2024, doi: 10.61397/ays.v2i1.183.

[2] Matthew Jakaria Sitanggang dan Imam Haryanto, "QRIS as a Single Payment Gateway as a Solution for Payment Efficiency and Legal Protection for e-commerce Consumers Through a Comparison With China," *J. Law, Polit. Humanit.*, vol. 5, no. 3, hal. 1840–1852, 2025, doi: 10.38035/jlph.v5i3.1339.

[3] W. D. Mulia, "Legal Protection Against Bri ' S Quick Response Code Indonesian Standard (Qris) Transactions In Micro , Small , And Medium Enterprises In Kartasura District," *Int. Conf. Restruct. Transform. Law*, vol. 4, no. 1, hal. 501–513, 2025.

[4] Nimrod, Tri Susanti, dan I. P. A. S. Sinaga, "Legal Aspects of Contracts in Digital Transactions Through E-Commerce Shopee With QRIS Payment Method," *J. Pract. Learn. Educ. Dev.*, vol. 5, no. 2, hal. 429–434, 2025, doi: 10.58737/jpled.v5i2.452.

[5] H. E. S. Samosir, I. Natsir, H. Setiawan, J. Hendra, Suyanto, dan B. Sipayung, "Perspective of Sharia Economic Law and Positive Law for Non-Cash Payment Qris Users in Indonesia According to The SDG," *J. Lifestyle SDGs Rev.*, vol. 4, no. 2, hal. e01741, 2024, doi: 10.47172/2965-730x.sdgsreview.v4.n02.pe01741.

[6] Ariyanto, "The Implementation of Consent Principle in QRIS-Based E-Payment," *J. Huk. Ius Quia Iustum*, vol. 32, no. 1, hal. 149–175, 2025.

[7] F. Alfiani, N. Hasanah, dan D. K. Respati, "Adaptation Of Qris To Increase Msme Income (Phenomenological Study On The Perception Of Msme Transaction Security) International Journal of Current Economics & Business Ventures," *Int. J. Curr. Econ. Bus. Ventur.*, vol. 5, no. 1, hal. 221–246, 2025.

[8] S. Wibisono dan H. Subiyantoro, "Transformation Towards a Clean Digital Economy by Optimizing Non-Cash Transactions as an Instrument to Prevent Corruption," *Indones. J. Multidiscip. Sci.*, vol. 4, no. 10, hal. 714–727, 2025.

[9] A. Ayuningtyas, H. H. Adinugraha, dan M. Sulthoni, "Quick Response Code Indonesian Standard as a Digital Payment Solution to Increase the Turnover and Reduce the Circulation of Counterfeit Money," *J. Educ. Comput. Appl.*, vol. 1, no. 1, hal. 25–31, 2024, doi: 10.69693/jeca.v1i1.7.

[10] Nanda Dwi Rizkia dan H. Fardiansyah, *Metode Penelitian Hukum (Normatif Dan Empiris)*. Bandung: Widina Media Utama, 2023.

[11] S. Soekanto, "Penelitian Hukum Normatif," *Kertha Widya J. Huk.*, vol. 1, no. 1, hal. 4, 2013.

[12] W. P. Widia, M. S. Sakmaf, Jumiran, dan Husain, "Consumer Protection Law in Electronic Transactions : Between Rights and Obligations in the Digital Era," *MAWADDAH J. Huk. Kel. Islam*, vol. 2, no. 2, hal. 177–189, 2024.

[13] A. Y. Silalahi dan A. N. Zhafarina, "Arrangement of Blockchain Technology as an Effort to Prevent Payment Fraud via the Indonesian Standard Quick Response Code (Qris) Performed by Consumers in Electronic Transactions," *Leg. Br.*, vol. 13, no. 2, hal. 267–276, 2024, [Daring]. Tersedia pada: https://legal.isha.or.id/index.php/legal/index

[14] A. Melinda dan N. Wardhani, "QRIS implementation benefits and risks: A phenomenological study of Sleman's culinary MSMEs," *Revenue Rev. Manag. Accounting, Bisness Stud.*, vol. 5, no. 2, hal. 128–140, 2024, [Daring]. Tersedia pada: www.antaranews.com,

[15] E. Hamzah Muchtar *et al.*, "Quick response code Indonesia standard (QRIS) E-payment adoption: customers perspective," *Cogent Bus. Manag.*, vol. 11, no. 1, hal. 1–19, 2024, doi: 10.1080/23311975.2024.2316044.

[16] M. R. Nur, A. Hendrawan, S. A. Marits, dan S. Herman, "Development of Digital Payment Systems in Indonesia," *J. Ilm. Manaj. Kesatuan*, vol. 11, no. 3, hal. 1335–1344, 2023.

[17] L. Septiningrum *et al.*, "Theoretical Framework of Cashless Payment Systems in

Indonesia: Analyzing Condition in Different Era's," *J. NATAPRAJA Kaji. Ilmu Adm. Negara 2406-9515*, vol. 12, no. 01, hal. 25–42, 2025.

[18] K. Sanjaya, P. R. Masdiantini, dan I. P. Julianto, "MSMEs ' Perceptions of QRIS Use in Financial Transactions and Recording in Singaraja City," *J. Penelit. dan Pengemb. Sains dan Hum.*, vol. 9, no. 2, hal. 366–374, 2025.