LEGAL PROTECTION QUICK RESPONSE CODE AS A PAYMENT SYSTEM

Normalita Destyarini[1], Falah Al Ghozali[2], Muhamad Rois[3]
Universitas Duta Bangsa[1], Universitas Duta Bangsa[2]
Email: normalita_destyarini@udb.ac.id[1], falahalghozali@windowslive.com[2]

ARTICLE INFO

Received:
Revised:
Approved:

ABSTRACT

Technology in the payment system brings convenience to its users and as an effort to improve the economy, the use of QR Code technology. Indonesia has a standardized standard in terms of using the QR Code, namely by using QRIS (Quick Response Code Indonesian Standard) issued by payment service providers as stipulated in the Regulation of the Members of the Board of Governors of Bank Indonesia Number 23/6/PBI/2021 concerning Payment Service Providers. There are risks that may arise, namely the occurrence of QRIS transaction fraud. Sanctions for Payment Service Providers as in the Regulation of Members of the Board of Governors of Bank Indonesia Number 23/6 / PBI / 2021 concerning Payment Service Providers in the form of administrative sanctions to termination of business activities further Law Number 13 of 2011 concerning Fund Transfers Article 79 to Article 86 by providing criminal provisions for perpetrators of fund transfers that do not have a license.

KEYWORDS QRIS, Fraud, Payment Service Providers

INTRODUCTION

People's lives in fulfilling their needs and carrying out their interests require activities in the form of economic activities, in economic activities the community fulfills obligations in the form of making payments in order to obtain rights in the form of delivery of an item or need. The development of a payment system that starts with barter by exchanging the goods it needs with the goods it has to other people who need it. Using a means of payment with currency as a measure of a desired item, to the existence of a payment system that uses cards, application-based and digital wallets. The convenience provided by technology to the community is increasing rapidly, people no longer need to carry cash when making payments, this provides convenience in practice. Everything that is *instant* does not necessarily provide true security for users. Using this digital system makes it easier for people who make transactions in relatively small amounts, not many people are reluctant to use a digital payment system if the transaction is large. Information technology contained in the *QR Code* workings is included as information technology because it is a technique for collecting, preparing, storing, processing, analyzing and disseminating information by loading electronic information using electronic systems that carry out the functions of collecting, preparing, storing, processing, announcing, analyzing and disseminating electronic information.

Technology in the payment system brings convenience to its users and as an effort to improve the economy, the use of *QR Code* technology in the system is a digital code that contains data or information as a link to service providers, that *QR Code* technology can only be translated with a tool to read the code such as using a camera on a mobile device. The influence given to the existence of this technology has an impact on regulations in cyber space and crimes that arise due to the existence of QR Code technology. The existence of the *QR Code* in the payment system brings financial inclusion and the spirit of *cashless* implementation (Deloitte Consulting, 2018). Support for national digital economy and financial integration by digitizing payment system services needs to be developed by maintaining a balance between innovation with stability and sound business practices and ensuring national interests.

The development of payments using digital finance with the payment system using the QR Code. In Indonesia, the use of the QR Code payment system is in accordance with predetermined standards. The QR Code standard used is in accordance with the PADG (Regulation of Members of the Board of Governors) of Bank Indonesia Number. 21 /18 PADG/2019 concerning Implementation of the National *Quick Response Code* Standard for Payment. The parties involved in processing QRIS transactions are Payment System Service Providers including front end payment system service providers that can come from banks and non-bank institutions, *Switching* Institutions, *Merchant Aggregators* and NMR Managers. This research is used to determine the scope of regulations related to the issuance of QR Codes as a payment system issued by Payment Service Providers in overcoming the problem of QRIS transaction fraud.

RESEARCH METHOD

The type of legal research method chosen by legal research in the typology of normative legal research research focuses on positive legal norms in the form of laws. (Zainuddin Ali, 2018). The statutory approach is carried out by examining the laws and regulations related to the legal issues under study (Peter Mahmud, 2010). Descriptive analytical is the nature of the research specifications used by the author, because the specifications of this research describe and describe the object problem under study. The data that has been obtained is then collected and then compiled to be analyzed and explained in order to obtain conclusions from the research conducted.

RESULT AND DISCUSSION

A. *Quick Response Code* Working System

Digitalization is expected to improve the national economy in order to improve the welfare of the community so that public services can be carried out effectively and efficiently. The implementation must be able to provide a sense of security, justice and legal certainty. The influence of technology affects and changes the way business works practically and gets better results in the form of innovations developed in the payment system with a payment system. (M & Ralph, 2018) in the form of innovations developed in the payment system by making payments using *Quick Response Code* or quick code response which can be an image containing a two-dimensional matrix that has the ability to store data in it, this technology was developed by Denso Corporation, a Japanese company engaged in the Automotive sector. There is a *QR Code* Reader that can read the data stored by the *QR Code*, it can be an application or just by using a cellphone camera so that the data reads the information data in it and then converted to text that can be read by humans. (Pande, 2017). Has a two-dimensional code with a square-shaped marker dimension pattern to store alphanumeric, characters and symbols used for payments without making direct contact. As a marker of a product both goods and services issued by a company as a differentiator because when the *QR Code is* moved it will display the content as programmed by the company that made the *QR Code*.

The payment system using the *QR Code* is done by taking an image contained in the *merchant.* Protection of the digital payment system by using a security authentication system using a PIN (*personal identification number)* code, biometric *fingerprint*, and One Time Password (OTP) (P & Akpojaro, 2014) and One Time Password (OTP). This is because support for transactions made with cash as one of the basic *attributes of customer satisfaction with electronic payment.* (Kombo, Belas, Koraus, & Korau, 2016). Someone who uses a *QR Code* by scanning the code using a cellphone camera so that the camera captures the code which will then be connected to a website or application page. The activity of scanning the code contained in the *QR Code* using the *QR Code* reader application to take users to the intended address in the form of a website page or application. (Dwi, 2017) or application. With the use of this system, service providers who use, who create *QR Codes* must be able to guarantee that there are limits to permissions in their performance capabilities, maintain and control data on applications and consumer privacy. *QR Code* creation using a web page that then processes a password in the form of a unique text that represents the *QR Code*. *QR Code* types with dimensions that can be read with a *qr-code* reader or camera on a smartphone (Várallyai, 2013) the data load is larger than the barcode (Cornelia & Repanovici, 2015) in the payment system can contain data in the form of prices, merchant locations, device IP addresses and time, in connection (Kurniawan, 2018) with the built-in application where the *QR reader* can allow access to data in the form of photos due to permission to use the camera.

B. QRIS Transaction Risks

The parties in the implementation of QRIS service transactions by payment system service providers in this case are banks or institutions other than banks that organize payment system service activities. There is a *Merchant Aggregator* as a payment system service provider by acquiring *merchants* by forwarding funds from QRIS transactions to merchants in collaboration with Payment System Service Providers and QRIS users as parties who make payments in QRIS Transactions. Payment System Service Provider in carrying out QRIS transaction processing activities must first obtain approval from Bank Indonesia.

The determination of the *QR Code* national standard in the implementation of payment transaction processing involves various parties, so that the implementation of QRIS requires further arrangements so that the implementation of payment system services facilitated by the *QR Code* in Indonesia can run effectively and efficiently and ensure clarity of roles and responsibilities of the parties in payment transaction processing using the *QR Code* Payment. Payment System Service Providers as QRIS issuers must provide a sense of security and reliability.

Risks that may arise in the event of fraudulent QRIS transactions to fake merchants. Fraud in a transaction as a form of failure to prevent or deter unauthorized transactions, interception of confidential information or other fraud. Efforts to prevent fraud risk by increasing security and supervising QRIS services. Regulations governing the QRIS payment system Payment System Service Providers as the party that issues QRIS are contained in the Regulation of the Members of the Board of Governors Number 21/18 / PADG / 2019 concerning Implementation of the *Quick Response Code* National

Standard for Payment, Regulation of the Members of the Board of Governors Number 23/6 / PBI / 2021 concerning Payment Service Providers.

C. Legal Framework

Payment system operators must comply with the general principles in the implementation of the payment system based on Bank Indonesia Regulation Number 23/6/PBI/2021 concerning Payment Service Providers which consists of:

a. Organizing obligations that include aspects:
   1. Governance;
   2. Risk management including prudence
   3. Information system security standards
   4. Interconnection and interoperability and
   5. Fulfillment of statutory provisions
b. Bank Indonesia's policy on pricing schemes in the operation of payment systems and
c. Human resources and organizational capabilities, as well as a healthy code of ethics and business conduct.

Fulfillment of the obligations of risk management aspects including the prudential principle by conducting active supervision by the board of directors and the board of commissioners for payment service providers incorporated as limited liability companies and functions or organs that carry out management and supervisory functions for payment service providers incorporated as other legal entities. Providing a safe and reliable payment system to provide security and protection of data confidentiality, fraud management with the stages of prevention, detection, handling and monitoring, fulfilling certification and/or standards for system security and reliability, maintaining and improving technological security and information system availability, implementing cybersecurity standards, securing data and/or information and conducting periodic information system audits.

Sanctions against payment service providers who violate the provisions may be subject to administrative sanctions in the form of :

a. Reprimand
b. Temporary suspension, part or all of the activities including the implementation of cooperation and/or
c. Revocation of license as payment service provider

Fraud management with prevention stages by having policies related to cyber risk management that are separate from information technology management with organs independent of business functions and information system management and the fulfillment of human resources who have cyber resilience and security competencies to support cyber risk culture, detection, handling and monitoring.

Payment service providers collect and obtain user data that is identified and can be combined with other information electronically or non-electronically as Article number 29 of Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP PTSE), electronic system providers are required to protect the personal data they manage to prevent data leakage and data loss. The use of hardware and software by service providers must meet the aspects of security, interconnectivity and comability with the system used with after-sales maintenance by the seller and guarantee of service continuity. The principles that must be implemented in protecting personal data are when specific collection is carried out legally fair and with the knowledge and consent of the data owner, processed in accordance with the purpose. Supervision carried out by the Minister in the form of monitoring, controlling, examining, tracing, and securing. The parties organizing electronic transactions pay attention to good faith, the principles of prudence, transparency, accountability and fairness.

The use of *QR codes* in the payment system is a form of technological development in the financial sector. The existence of this payment system is in line with Law No. 3 of 2019 concerning Fund Transfers because there is a utilization of technology using information facilities as a transfer of information contained in a barcode to be translated so that it can be read by humans. The data content in QR Codes must be ensured to be safe, therefore the Fund Transfer Law has criminal provisions for parties who utilize the *QR Code* technology of the parties in question. The electronic system used by service providers that utilize the *QR Code* as a payment system uses electronic agents in the form of electronic data, visuals and other forms. Obligations that must be owned by the electronic agent organizer in the form of supervision, canceling orders to then provide confirmation or reconfirmation, the option to continue the next activity, being able to know the status of a successful or failed transaction and the content of agreement information before making a transaction.

Law No. 13 of 2011 on Fund Transfers in Article 79 to Article 86 provides criminal provisions for perpetrators of unlicensed fund transfer operations to obtain imprisonment of up to 3 years and a fine of up to 3 billion rupiah so that they must stop organizing fund transfer activities. If unlawfully storing the means of fund transfer orders personally or for other people, the penalty is imprisonment for two years with a fine of two billion rupiah, if then using and delivering the means is punished with a maximum imprisonment of 4 years with a fine of 4 billion. The act of fraud committed by the perpetrator who deletes, removes and changes part or all of the information contained in the fund transfer news for himself or others is punishable by imprisonment with a maximum of two years imprisonment or a maximum fine of one billion rupiah. If the act of deleting, removing or changing part or all of the data contained in the fund transfer order so as to cause losses to the sender or recipient or other parties, the perpetrator will be sentenced to a maximum of four years imprisonment with a maximum fine of two billion rupiah.

CONCLUSION

The development of payments using digital finance with the payment system using the QR Code. In Indonesia, the use of the QR Code payment system is in accordance with predetermined standards. The QR Code standard used is in accordance with the PADG (Regulation of Members of the Board of Governors) of Bank Indonesia Number. 21 /18 PADG/2019 concerning Implementation of the National *Quick Response Code* Standard for Payment. This development brings problems that can be caused by the use of QRIS in the form of transaction fraud in the form of unauthorized transactions, interception of confidential information or other fraud. Payment service providers as parties that issue QRIS have an obligation to fulfill the general principles of implementing payment systems in the form of governance, risk management including the precautionary principle, information system security standards and fulfillment of laws and regulations. Safe and reliable payment system providers to provide security and protection of data confidentiality, fraud management with stages of prevention, detection, handling and monitoring, fulfillment of certification and / or system security and reliability standards, maintaining and improving technological security and information system availability, implementing cybersecurity standards, securing data and / or information and conducting periodic information system audits. Further regulations regarding the implementation of fund transfers carried out by payment service providers are contained in Law No. 3 of 2019 concerning Fund Transfers which provides an explanation that in the event of fraud in transactions, fund transfer operators who do not have a license receive a prison sentence of up to 3 years and a fine of up to 3 billion rupiah so that they must stop organizing fund transfer activities. Meanwhile, Bank Indonesia Regulation Number 23/6/PBI/2021 concerning Payment Service Providers provides sanctions in the form of warnings, temporary suspension, part or all of the activities and license revocation.

REFERENCES

Books

Peter Mahmud Marzuki, 2010, Legal Research, Jakarta, Kencana, p. 93

Zainuddin Ali. (2018). *Metode Penelitian Hukum*. Jakarta: Sinar Grafika.

Scientific Journals

Cornelia, A.-M., & Repanovici, A. (2015). Legal Information Management Using QR Codes. *Qualitative and Quantitative Methods in Libraries (QQML)*, *4*, 381–397. Retrieved from http://www.qrcode.com/en/codes/

Deloitte Consulting. (2018). *Bolstering Financial Inclusion in Indonesia: How QR Codes Can Drive Digital Payments and Enable Financial Inclusion*. p. 44. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/id/Documents/financial-services/id-fsi-financial-inclusion.pdf

Dwi, A. S. (2017). Studi Tingkat Kecelakaan Lalu Lintas Jalan di Indonesia Berdasarkan Data KNKT (Komite Nasional Keselamatan Transportasi) Dari Tahun 2007-2016 Nasional Keselamatan Transportasi) Database from 2007-2016. *Warta Penelitian Perhubungan*, *29*(2), 179–190.

Kombo, F., Belas, J., Koraus, A., & Korau, M. (2016). A Electronic Banking Security and Cutomer Satatisfication in Commercial Banks. *Journal of Security and Sustainbilitu Issues*, *5*(3), 411–422. https://doi.org/10.9770/jssi.2016.5.3(9)

Kurniawan, D., Zusrony, E. dan Kusumajaya, R.A. (2018), Analisa Persepsi Pengguna Layanan Payment Gateway Pada Financial Technology Dengan Metode Eucs, Jurnal INFORMA Politeknik Indonusa Surakarta, 4(3), 1–5

M, K. W., & Ralph, W. H. (2018). The Impact of Technology on Business and Society. *Global Journal of Business Research*, *12*(1), 23–39. https://doi.org/10.1097/sla.0000000000002936

P, A., & Akpojaro, J. (2014). Analysis of Security Issues in Electronic Payment Systems. *International Journal of Computer Applications Volume 108 – No. 10, December 2014.*, *108*(10), 10–14. https://doi.org/http://dx.doi.org/10.5120/18946-9993

Várallyai, L. (2013). From Barcode to QR Code Applications. *Journal of Agricultural Informatics*, *3*(2), 9–17. https://doi.org/10.17700/jai.2012.3.2.92