

Risks and Legal Protection in Non-Cash Financial Transactions Through E-Wallets

Cahyo Oriento, Dharma Setiawan Negara, Arif Rachman Putra, Samsul Arifin, Rio Saputra

Sunan Giri University of Surabaya, Indonesia

ARTICLE INFO

Article history:

Received 2 September 2022

Revised 1 November 2022

Accepted 19 November 2022

Key words:

Legal protection,
Non-Cash transactions,
E-wallets,
Regulation,
Risk,
Data misuse,
Supervision.

ABSTRACT

The application of legal protection in non-cash financial transactions through e-wallets has become important as technology develops and the number of users of this service increases in Indonesia. Although facilitating transactions, e-wallets carry risks such as misuse of personal data and fraud. Proper legal protection is needed to ensure transaction security and protect consumers. Existing regulations, such as the Electronic Information and Transaction (ITE) Law, and Financial Services Authority (OJK) Regulations, provide a legal foundation, but there are still challenges in supervision and implementing regulations in line with technological developments. Strengthening supervision, improving digital literacy, and transparency from service providers are key to mitigating risks. Effective legal protection can increase public trust in financial technology and support financial inclusion. Adaptive policies and collaboration between relevant parties are needed to ensure a safe and fair digital ecosystem.

INTRODUCTION

Along with the rapid development of technology, non-cash payment system through e-wallets has become one of the most important innovations in the financial world. E-wallets allow individuals and companies to conduct financial transactions quickly and practically without the need to involve cash. This practicality has made e-wallets a top choice for many users, from daily transactions to payments for larger services. Indonesia, as one of the most populous countries in the world, has seen this trend grow very rapidly, with more and more e-wallets applications being used by the public (Usman, 2017).

Behind the convenience offered by this payment system, there are a number of risks that need to be considered. Non-cash transactions through e-wallets require users to rely on digital infrastructure that is vulnerable to cyber threats, such as personal data theft, account hacking, and unauthorized transactions (Tarantang et al., 2019). Users who do not understand how to secure their personal data may become easy targets for digital fraud. Other risks include dependence on technology that may fail or malfunction, potentially harming users. It is important to further examine the legal protections that can be provided to address these risks (Manurung et al., 2020).

E-wallets are also faced with challenges regarding legal aspects in addition to risks related to technology and security systems. In many cases, users find it difficult to obtain clear legal protection in the event of a dispute or misuse of transactions (Pakasi, 2021). For example, if a transaction made through an e-wallets is not what the user intended, or if there is an error in the transfer of funds, the legal procedures that can be followed by consumers are often unclear. Consumer protection laws and regulations governing digital transactions need to be studied more deeply in order to provide maximum protection guarantees (Anrova & Sembiring, 2022).

The Indonesian government has started to develop regulations governing these digital transactions. Although there are relevant regulations, such as Law Number 11 Year 2008 on Electronic Information and Transactions (ITE) and OJK Regulations, there are still gaps that need to be improved to make legal protection more comprehensive. One of the main challenges is the mismatch between existing regulations and the dynamics of rapid technological development. The issue of international law, especially in terms of cross-border transactions, is also an issue that needs further scrutiny to avoid greater losses for Indonesian consumers.

* Corresponding author, email address: dr.riosaputra@gmail.com

Within the framework of competition law, consumer protection should also be a major concern, as misuse by e-wallets service providers can directly harm consumers. The vagueness of clarity regarding consumer rights, ignorance of service provider obligations, and difficulties in the claims and dispute resolution process can exacerbate the injustice experienced by users. Strengthening legal protection in non-cash transactions through e-wallets is very important to prevent further potential losses for consumers and ensure the creation of a safe and reliable digital transaction ecosystem (Tarantang et al., 2019).

Although the existence of regulations governing electronic transactions, including e-wallets, there are still a number of fundamental problems related to legal protection for users. First, the gap between rapid technological development and existing regulations is a major obstacle in providing adequate legal protection. Existing regulations are not always able to keep up with the dynamic development of digital payment systems, making it difficult for the law to protect consumers appropriately and effectively. Although there are efforts to sanction offending service providers, the implementation of such sanctions is often not strict or swift enough, resulting in continued harm.

Second, although there are institutions that oversee digital transactions, such as OJK, they are not fully equipped to handle all the problems that arise in non-cash financial transactions. Cases of fraud or mishandling of e-wallets transactions are still common, and consumers do not always receive adequate protection or clear redress procedures. The public's lack of understanding and awareness of their rights in digital transactions is also a factor that exacerbates this situation and hinders the implementation of more effective legal protection.

This issue requires serious attention due to the increasing use of e-wallets along with the advancement of digital technology, especially in today's fast-paced and connected era. The security of digital transactions involving money or personal information is increasingly becoming a major concern for consumers. Without adequate legal protection, consumers may become victims of cybercrime that threatens their identity and assets (Usman, 2017). This study is important to ensure that existing regulations can provide sufficient protection and are in line with technological developments.

The presence of clear regulations and a robust protection system will also increase public trust in the non-cash payment system, which in turn will support greater growth of the digital economy (Lusiana, 2021). With efforts to improve the legal system,

Indonesia will be able to compete globally by providing safer and more transparent financial transactions. This study provides a foundation for policy evaluation that can strengthen legal protection in the future.

The purpose of this study is to analyze how the application of legal protection can be strengthened to address the risks associated with non-cash financial transactions through e-wallets. The study also aims to evaluate the effectiveness of existing regulations and provide recommendations on improvements needed to enhance consumer protection in the digital ecosystem. With the results of this study, it is expected to contribute to policy makers in formulating more appropriate regulations to support the security of digital transactions.

RESEARCH METHOD

The research method used in this study is a literature study and normative juridical approach. This approach focuses on the study of laws and regulations, legal doctrines, and various literatures relevant to the topic of legal protection in non-cash financial transactions through e-wallets. This literature study aims to analyze the legal principles governing digital transactions and to explore legal issues related to consumer protection and e-wallets providers. This normative juridical method will rely on primary legal materials, such as laws and regulations, as well as secondary materials in the form of academic literature, journals, articles, and books related to the topic of business competition law and electronic transactions (Soekanto, 2017).

This study will also examine various legal regulations applicable in Indonesia, such as Law Number 11 Year 2008 on Electronic Information and Transactions (ITE) and OJK Regulations, as well as other policies related to electronic transactions and consumer protection. This normative juridical study relies on the analysis of relevant legal doctrines and theories, with the aim of providing recommendations related to strengthening regulations and legal protection policies in non-cash transactions. In this case, the approach also involves comparing existing laws with technological developments and the practice of non-cash financial transactions (Marzuki, 2011).

RESULT AND DISCUSSION

The rapid development in digital payment technology has changed the way people interact in financial transactions. E-wallets are now the primary tool for many people to conduct various financial activities, from online shopping to bill payments,

providing convenience and efficiency. Its widespread use reflects a major transformation in people's consumption patterns. Behind the convenience it offers, there are potential risks that cannot be ignored, which demand serious attention from authorities.

As a technology that relies on electronic data exchange, e-wallets are vulnerable to various threats, both in terms of security and misuse of information. Hacking cases that result in loss of funds or personal data are concrete examples of the risks faced (Mills & Harclerode, 2017). Misuse of data by third parties or fraud involving digital transactions is increasingly prevalent, which makes consumer protection crucial. In this case, the law has an important role to play in creating a protection system that can provide security guarantees for users (Anrova & Sembiring, 2022).

For this reason, efforts to strengthen legal regulations and ensure effective legal protection for non-cash transactions must be made immediately. This serves to mitigate potential risks, and to foster public trust in the use of e-wallets (Aslinawati et al., 2016). Comprehensive legal protection will provide a sense of security for consumers and promote the development of a more stable and responsible digital financial market (Tarantang et al., 2019).

In general, legal protection in non-cash transactions through e-wallets should cover several aspects, including consumer rights, service provider obligations, and dispute resolution mechanisms. Existing regulations, such as Law Number 11 Year 2008 on ITE and OJK Regulation No. 77/POJK.01/2016 on the Implementation of Financial Technology, provide a legal basis to protect consumers in the event of misuse or transaction failure. Along with the rapid development of technology, the existing regulations still face various challenges in regulating various types of risks arising in digital transactions, especially those related to misuse of personal data and online fraud.

According to Article 1 point 2 of the ITE Law Number 11 Year 2008, electronic transactions are defined as legal actions carried out using computers, computer networks, and or other electronic media. From the formulation of the article, it can be concluded that any act of exchanging information carried out through an electronic network can be categorized as an electronic transaction. The concept of electronic money is closely related to e-wallets, which indicates that if the money owned is electronic, then the wallets that stores it must also be digital.

Conceptually, there are differences in terms of liability and legal consequences that need to be understood in relation to e-wallets, which depart from the principles in conventional transactions.

In this case, e-wallets that hold money and are in the hands of the owner place the responsibility entirely on the owner, similar to carrying cash. If an error is caused by the e-wallets organizer, where the money is stored by the organizer, then the responsibility for the loss or damage that occurs shifts to the e-wallets organizer (Usman, 2017). This is reinforced by Article 21 paragraph (4) of ITE Law Number 11 Year 2008, which states that if the loss in an electronic transaction is caused by the operational failure of the electronic agent due to the negligence of the service user, then all legal consequences are the responsibility of the user. The organizer is obliged to provide compensation in accordance with the losses suffered by service users, emphasizing the importance of understanding responsibility in electronic transactions.

Electronic transactions can be defined as an engagement or legal relationship conducted electronically, which integrates a network of computer-based information systems with communication systems that depend on telecommunications networks and services. This process is facilitated by the existence of a global computer network, the internet. In e-commerce, it is important to understand the theory of agreement underlying this transaction, as stipulated in Article 1313 of the Civil Code of Indonesia (KUHPerdata), which states that an agreement is an act in which one or more people bind themselves to one or more other people. The provisions regarding agreements are contained in Book III of the Civil Code of Indonesia, which is open, meaning that its provisions can be overridden and only function to regulate (Raditio, 2014).

In the legal aspect, electronic transactions are closely related to electronic contracts that occur remotely, across national borders, and are carried out faceless and paperless. Article 1338 of the Civil Code of Indonesia emphasizes that all agreements made legally apply like laws to the parties who make them. The principle of freedom of contract in an open system allows anyone to enter into an agreement and determine the contents of the agreement. The regulation of agreements in Indonesia only covers agreements in general, which are regulated in Article 1320 of the Civil Code of Indonesia regarding the validity of an agreement. In a sale and purchase agreement, Article 1458 of the Civil Code of Indonesia states that an agreement is deemed to have taken place between the seller and the buyer when they have agreed on the condition of the goods and the price, even though the goods have not been delivered and the price has not been paid.

Cybercrime, particularly in relation to electronic transactions, is increasingly prevalent and is known as cybercrime. These activities include criminal acts committed through or against computer systems, internet networks, or other digital devices. It is perceived as anti-social behavior by internet users, although the question of whether it can be prosecuted and punished under criminal law is a separate issue. Cybercrime can reach various aspects of activities related to electronic transactions, one of which is privacy. In this regard, crimes often include identity theft, illegal access, and dissemination of sensitive personal data and information. This threat to privacy shows how vulnerable personal data is in a digital environment (Tarantang et al., 2019).

Fraud is also a serious problem in electronic transactions. Internet-based fraud is a crime in which the perpetrator utilizes the elements of the internet to deceive and take the property or interests of others through false statements. Tactics used can include misleading information or concealing relevant facts. Perpetrators also often pose as official parties or use digital platforms such as websites, apps or social media to trick victims. It is important to understand and overcome various forms of cybercrime that can harm individuals and society, as well as to increase awareness of the need for personal data protection in electronic transactions (Manurung et al., 2020).

Law Number 8 Year 1999 on Consumer Protection regulates various provisions that aim to encourage producers and business actors to behave in accordance with principles that support national economic development. Any violations committed by producers will be subject to legal sanctions, both administrative and criminal, to create a healthy business climate. These sanctions serve as a rehabilitation tool to restore the situation after a violation, as well as a preventive measure to prevent the recurrence of the same act. In Article 60, this law stipulates the administrative liability that can be demanded from business actors, including the obligation to pay compensation of up to IDR 200,000,000.00 (two hundred million) for certain violations. There are also provisions regarding criminal liability that can be imposed on business actors, including imprisonment and fines, as well as additional sanctions that can take the form of confiscation of goods, announcement of a judge's decision, and revocation of business licenses.

On private liability, Article 19 stipulates that business actors are obliged to provide compensation for losses suffered by consumers due to the goods or services produced. This compensation must be implemented within seven days after the transaction,

and does not remove the possibility of criminal charges if there is an element of fault. If the business actor refuses to take responsibility, the consumer can file a lawsuit through the Consumer Dispute Resolution Agency (BPSK) or the court. E-wallets companies also have an obligation to compensate for losses incurred as a result of transactions through their applications, unless the fault is caused by the consumer (Pakasi, 2021). In this case, it is important to maintain a balance of protection between consumers and business actors, in order to create a healthy and sustainable business climate, in accordance with the provisions stipulated in the Consumer Protection Law and the ITE Law.

Effective legal protection requires strengthening supervision of e-wallets service providers. As a supervisory institution, the OJK has an important role in regulating and supervising the implementation of these digital transactions. OJK also needs to regularly update regulations to ensure that the existing rules remain relevant to rapid technological developments. One important thing that needs to be considered is the obligation of service providers to maintain the security of consumers' personal data and provide a transparent system for managing funds. In the absence of strict supervision, abuse by service providers can occur, which can directly harm consumers.

It is important to educate consumers about their rights in digital transactions, including in the event of misuse or faulty transactions. Many consumers still lack understanding of how to protect their personal data and do not realize the importance of clear privacy policies in any e-wallets application (Pakasi, 2021). It is important to introduce digital literacy to the public, so that they can be more aware and alert to potential risks that may occur. With a better understanding, consumers can be more proactive in protecting themselves from the risks that can occur in non-cash transactions (Lusiana, 2021).

Regarding dispute resolution mechanisms, clear regulations should ensure easy and fair access for consumers to file claims and obtain redress in the event of losses due to faulty or unauthorized transactions. This includes clarity of grievance procedures, responsive communication channels, and sufficient information on the rights and steps consumers can take. This is particularly important given that many consumers feel aggrieved but do not know where to complain. Service providers should also provide effective and transparent complaint channels. There needs to be legal enforcement for service providers that do not comply with consumer protection regulations, to prevent even greater violations.

One important aspect of legal protection is the application of strict sanctions for violations of existing regulations. These sanctions can be in the form of fines, revocation of business licenses, or other administrative sanctions that can provide a deterrent effect for irresponsible business actors. With strict sanctions, e-wallets service providers will be more encouraged to pay attention to the security and privacy of user data. This also provides assurance for consumers that their rights will be protected in every transaction made through e-wallets (Anrova & Sembiring, 2022).

The challenges faced in implementing this legal protection are also related to international legal aspects. Non-cash transactions through e-wallets often involve foreign parties, both in terms of service providers based abroad and consumers who transact across countries. Regulations are needed that can regulate cross-border digital transactions that provide legal protection for Indonesian consumers. International cooperation in the regulation of digital transactions is important to ensure that Indonesian laws remain relevant and protect consumers, even though transactions are conducted with foreign parties (Maskun & Meilarti, 2016).

It is also important to look at arrangements related to technology security. Institutions such as OJK and The Central Bank of Indonesia (BI) need to work with technology service providers to ensure that the systems used by e-wallets have adequate protection against cyber threats. The security of personal data and financial transactions is key in ensuring that consumers feel safe to use e-wallets in their daily activities. Without a secure system, the risks for consumers are even greater, which in turn can undermine public trust in the non-cash payment system (Lusiana, 2021).

In overcoming the existing risks, supervision of the development of financial technology must also be strengthened. Rapidly developing technology has a positive impact, but it also opens a gap for new crimes, such as online fraud or the use of illegal applications. The role of supervision is not only limited to service providers but also to the development of technology itself. Regulations that are more adaptive and dynamic to technological changes will help prevent potential risks that may arise (Sjahputra, 2010).

Strengthening digital literacy also plays an important role in supporting the legal protection of non-cash financial transactions. Consumers who are better informed and educated about technology and how to protect their personal data tend to be more cautious in conducting digital transactions.

Service providers should facilitate consumers with clear information on how to secure their accounts and transactions. Transparency in privacy and data protection policies should also be made clear by service providers, so that consumers feel more secure (Manurung et al., 2020).

Overall, implementing effective legal protection in non-cash financial transactions through e-wallets requires a synergy between strong regulations, strict supervision, and consumer education (Pakasi, 2021). This aims to create a safe, fair, and transparent digital ecosystem. With these measures, the risks involved in non-cash transactions can be minimized, and consumers can have more trust in using financial technology for their daily activities.

As the digital ecosystem continues to develop, strong legal protection will create a sense of security that consumers and businesses desperately need. Without clear security guarantees, public trust in financial technology may be compromised, potentially slowing down the adoption of digital payment systems (Anrova & Sembiring, 2022). By improving legal protection mechanisms, people will be more open to accessing digital services without worrying about potential risks. Maintained trust will strengthen the foundation of an increasingly complex and diverse digital economy.

The performance of Indonesia's digital economy sector relies heavily on proper regulation to maintain its sustainability and growth. Clear and firm regulations are needed to ensure that all actors in the digital ecosystem, both consumers and service providers, have legal certainty. Effective regulation will protect consumers, and provide a clear foundation for businesses to innovate without fear of harmful exploitation. This will create a conducive climate for the growth of the digital financial industry, where fairness and safety are enjoyed by all. In the long run, it will also contribute to improving Indonesia's competitiveness in the global arena (Tarantang et al., 2019).

By strengthening legal protection in non-cash transactions, Indonesia has the potential to become a pioneer in the implementation of a safe and transparent digital economic system. Strengthening this regulation enhances public security in electronic transactions and boosts confidence in financial technology. These steps must be balanced with public awareness of their rights and obligations in the digital world, as well as the government's commitment to continuously update policies and regulations as technology evolves. Collaboration between authorities, service providers, and users will be the key to creating a digital ecosystem that is fair, safe, and provides maximum benefits for the entire community.

CONCLUSION

The conclusion of this discussion is that the implementation of effective legal protection in non-cash financial transactions through e-wallets requires strong regulations and strict supervision. Although rapid growth, Indonesia's e-wallet sector remains vulnerable to data misuse, fraud, and transaction failures. Strengthening regulation through clear rules and supervision that is adaptive to technological developments are key to protecting consumers. A better understanding of consumer rights and service provider obligations also needs to be promoted so that the digital ecosystem can run safely and transparently.

The implication of better legal protection is increased public trust in digital transactions, which will accelerate the adoption and growth of the financial technology sector in Indonesia. With effective legal protections in place, both consumers and service providers will feel more secure in transacting using e-wallets, which in turn can promote financial inclusion in the community. The sector can also grow sustainably, by reducing potential risks that could harm businesses and consumers, and creating a fair and transparent market climate.

The advice that can be given is to continue to update existing regulations so that they are always in accordance with the dynamics of developing technology. The government and supervisory authorities such as OJK need to collaborate with e-wallets service providers to ensure that security and privacy aspects are always a top priority. Education to consumers should also be conducted intensively, so that they better understand their rights in digital transactions and how to protect their personal data.

REFERENCES

- Anrova, Y., & Sembiring, A. (2022). Peran Lembaga Penjamin Simpanan terhadap Saldo Uang Elektronik pada Dompot Elektronik Dana. *Jurnal Res Justitia: Jurnal Ilmu Hukum*, 2(1), 149-161.
- Aslinawati, E., Wulandari, D., & Soseco, T. (2016). Public Perception of the Effectiveness of Less Cash Society. *International Review of Social Sciences*, 4(1), 7-12.
- Lusiana, N. (2021). Transaksi Non Tunai Melalui Layanan Syariah LinkAja pada Ekosistem Keislaman di Kota Cirebon Ditinjau dari Perspektif Hukum Islam. *Theses*, IAIN Syekh Nurjati Cirebon.
- Manurung, E. D., Bakar, L. A., & Handayani, T. (2020). Kepastian Hukum dalam Penyelenggaraan Layanan Dompot Elektronik dalam Sistem Pembayaran Dikaitkan dengan Prinsip Lancar, Aman, Efisien, dan Andal Berdasarkan PBI Nomor 20/6/PBI/2018 tentang Uang Elektronik. *Jurnal Jurisprudence*, 10(1), 33-51.
- Marzuki, P. M. (2011). *Penelitian Hukum*. Kencana.
- Maskun, & Meilarti, W. (2016). *Aspek Hukum Penipuan Berbasis Internet*. Keni Media.
- Mills, J. L., & Harclerode, K. (2017). Privacy, Mass Intrusion and the Modern Data Breach. *Florida Law Review*, 69(3), 771-831.
- Negara, D.S. & D. Darmawan. (2023). Digital Empowerment: Ensuring Legal Protections for Online Arisan Engagements. *Bulletin of Science, Technology and Society*, 2(2), 13-19.
- OJK. (2016). *Peraturan Otoritas Jasa Keuangan (OJK) No. 77/POJK.01/2016 tentang Penyelenggaraan Teknologi Finansial*. Jakarta.
- Pakasi, S. S. (2021). Tinjauan Hukum terhadap Penggunaan Dompot Digital dalam Bertransaksi di Indonesia. *Lex Crimen*, 10(12), 69-76.
- Raditio, R. (2014). *Aspek Hukum Transaksi Elektronik Perikatan, Pembuktian dan Penyelesaian Sengketa*. Graha Ilmu.
- Republik Indonesia. (1999). *Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen*. Lembaran Negara Republik Indonesia Tahun 1999 Nomor 22. Sekretariat Negara, Jakarta.
- Republik Indonesia. (2008). *Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58. Sekretariat Negara, Jakarta.
- Sjahputra, I. (2010). *Perlindungan Konsumen dalam Transaksi Elektronik: Ditinjau dari Perspektif Hukum Perlindungan Konsumen dan Hukum Siber*. Alumni.
- Soekanto, S. (2017). *Pengantar Penelitian Hukum*. Raja Grafindo Persada.
- Tarantang, J., Awwaliyah, A., Astuti, M., & Munawaroh, M. (2019). Perkembangan Sistem Pembayaran Digital pada Era Revolusi Industri 4.0 di Indonesia. *Jurnal Al-Qardh*, 4(1), 60-75.
- Usman, R. (2017). Karakteristik Uang Elektronik dalam Sistem Pembayaran. *Yuridika*, 32(1), 134.