E-ISSN: 3031-8629
P-ISSN: 3032-3258
Halaman 1-37
Volume 2 Nomor 4 Tahun 2025

Cybersecurity Legal Policy Model For Enhancing Trust Among Indonesian E-Wallet Transaction Users

Tri Ginanjar Laksana[1]
[1]Program Studi Teknik Informatika, Universitas Bhayangkara Jakarta Raya
e-mail: tri.ginanjar.laksana@dsn.ubharajaya.ac.id

Abstrak

Transaksi dompet elektronik telah menjadi bagian integral dari kehidupan kita saat ini. Berkat kemajuan teknologi informasi, semakin banyak orang menggunakan dompet elektronik untuk melakukan pembayaran, mentransfer uang tunai, dan melakukan aktivitas keuangan lainnya. Namun, efektivitas transaksi dompet elektronik sangat bergantung pada kepercayaan pengguna terhadap keamanan dan kerahasiaan data mereka. Oleh karena itu, kita harus membangun kepercayaan dalam transaksi dompet elektronik. Esai ini akan mengeksplorasi pentingnya kepercayaan dalam transaksi dompet elektronik. Penelitian ini menggunakan teknik penelitian doktrinal. Metodologi yang digunakan meliputi metode legislatif dan konseptual. Sumber hukum yang digunakan dalam penelitian ini meliputi sumber primer, sekunder, dan tersier. Dokumen hukum teknis diperoleh dengan melakukan penelusuran web dan melakukan evaluasi literatur (studi dokumentasi). Dalam melakukan penelitian, analisis dokumen hukum bersifat deskriptif. Berdasarkan penelitian ini, terbukti bahwa membangun kepercayaan dalam transaksi dompet elektronik sangatlah penting. Hal ini dapat dicapai dengan menerapkan langkah-langkah yang memprioritaskan keamanan siber dan perlindungan data. Melalui prioritas kepercayaan dan keamanan, pemerintah dapat membangun ekosistem transaksi dompet elektronik yang aman dan dapat diandalkan, sehingga mendorong ekspansi masa depan dan kelangsungan jangka panjang.

Kata kunci: *e-Wallet, Transaksi, Keamanan Siber, Teknologi Informasi, Kepercayaan, Ancaman, Kebijakan Hukum, Model.*

E-ISSN: 3031-8629
P-ISSN: 3032-3258
Halaman 1-37
Volume 2 Nomor 4 Tahun 2025

Abstract

E-Wallet transactions have become an integral component of our contemporary existence. Due to advancements in information technology, an increasing number of individuals are using e-wallets for the purpose of conducting payments, transferring cash, and engaging in other financial activities. However, the efficacy of e-wallet transactions relies significantly on users' confidence in the security and confidentiality of their data. Hence, we must establish confidence in electronic wallet transactions. This essay will explore the significance of trust in e-wallet transactions. This study used a doctrinal research technique. The methodologies used include both legislative and conceptual methods. The legal sources used in this study include of primary, secondary, and tertiary sources. Technical legal documents were obtained by doing web searches and conducting literature evaluations (documentation studies). When doing research, the analysis of legal documents is characterized as descriptive. Based on this study, it is evident that establishing confidence in e-wallet transactions is crucial. This may be achieved by implementing measures that prioritize cyber security and data protection. Through the prioritization of trust and security, the government may establish a secure and dependable e-wallet transaction ecosystem, thus fostering future expansion and long-term viability.

Keywords : *e-Wallet, Transaction, Cybersecurity, Information Technology, Trust, Threats, Legal Policy, Model.*

PENDAHULUAN

Trust is the foundation of all transactions, including those made via e-wallets. Users are more likely to engage in transactions and provide information if they consider the e-wallet platform reliable . Nevertheless, in the event of a breach of this trust, consumers may discontinue their use of e-Wallets and seek out other options . Hence, e-wallet service providers must enhance user confidence using robust

encryption technology, stringent data-safeguarding measures, and transparent and unequivocal privacy policies . Prioritising customer trust is crucial to guarantee the future development and sustainability of e-Wallet transactions .

Cybersecurity plays a crucial role in ensuring the security of e-wallet transactions . Cybersecurity in the realm of e-Wallet transactions include safeguarding user data from cyber attacks and defending against other security vulnerabilities . In an ever more interconnected digital society, the risks associated with e-Wallet transactions are becoming more intricate and varied . Hence, it is essential for e-Wallet service providers to possess a comprehensive understanding of cyber security and implement suitable steps to address cyber risks . Implementing encryption technologies, robust authorization procedures, and vigilant monitoring of suspicious activities are effective measures that may be used. By comprehending and surmounting cyber security dangers, we may develop an e-Wallet transaction system that is secure and dependable .

Cybersecurity plays a crucial role in ensuring the security of e-Wallet transactions. Cybersecurity in e-Wallet transactions involves safeguarding user data from cyber attacks and other security risks . In an ever more interconnected digital society, the risks associated with e-Wallet transactions are becoming more intricate and varied . Hence, it is essential for e-Wallet service providers to possess a comprehensive understanding of cyber security and implement suitable steps to address cyber risks . Possible measures to be implemented include the use of encryption technology, robust authorization mechanisms, and vigilant surveillance of dubious behaviour. Through comprehensive comprehension and mitigation of cyber security risks, we can construct an e-Wallet transaction system that ensures the safety and dependability for consumers. One must be aware of the risks associated with doing e-Wallet transactions. Phishing attacks, which include the use of counterfeit websites or messages, are a prevalent sort of threat aimed at acquiring users' personal information. An further menace is posed by malware assaults, when wrongdoers attempt to contaminate consumers' machines with malevolent software. Furthermore, there are other risks such as identity theft, Distributed Denial of Service

(DDoS) attacks, and unauthorised access to user data . E-wallet service providers are required to use suitable technology and practices to safeguard clients from these potential risks. The system encompasses user guidance on effective security protocols, vigilant monitoring of suspicious activities, and periodic system upgrades to rectify recently identified security vulnerabilities. To provide a secure and dependable transaction environment, we use measures to safeguard e-Wallets against prevalent attacks .

A robust cybersecurity law policy model should have many crucial components. Initially, the model must set unambiguous security prerequisites for e-Wallet service providers. The requirements may include the use of robust encryption technology, the enforcement of stringent access restrictions, and the safeguarding of user data against unauthorised access . In addition, the legal policy model should include steps to safeguard consumers from dangers such as phishing attempts and malware assaults . This may include instructing users in effective security protocols and performing monitoring and identification of potentially illicit behaviour . Ultimately, a comprehensive legal policy framework must include the mechanisms used to disclose, handle, and uphold security breaches. Model legal regulations may give e-Wallet service providers with a robust framework to uphold user security and privacy .

Collaboration between the government, e-Wallet service providers, and consumers is essential for the enforcement of cybersecurity regulations in e-Wallet transactions. The government should establish explicit norms and regulations to control e-Wallet transactions and provide assistance and legal measures to combat security breaches . Furthermore, e-Wallet service providers should actively engage consumers in the implementation of legal laws. Users are required to actively engage in upholding the security of their e-Wallets by adhering to sound security protocols and promptly reporting any suspicious behaviour . By collaborating, the cyber security legal policy model for e-Wallet transactions may be swiftly and effectively implemented .

Several case studies have shown that cybersecurity legal policy approaches have achieved success in e-Wallet transactions. Singapore's stringent legal rules have effectively curtailed cybercrime in e-Wallet transactions . Nations mandate that e-wallet service providers enforce stringent authorization methods and use robust encryption technologies . Furthermore, Singapore enforces stringent penalties for security breaches in order to enhance user and service provider knowledge and adherence. The implementation of robust legal laws has created a secure and dependable e-wallet transaction ecosystem, fostering user trust and stimulating economic development .

The prospects for enhancing cybersecurity in e-wallet transactions are quite promising. With the ongoing advancement of information technology, we may expect emerging trends in cyber security that will enhance the protection of users from progressively intricate cyber assaults . Future developments include the use of artificial intelligence for the identification of cyber threats, the advancement of biometric technology for user verification, and the implementation of blockchain to enhance transaction security. Furthermore, it is essential for us to consistently enhance user awareness and comprehension of sound security protocols when using e-Wallets . Through the formulation and enhancement of legislative frameworks, we may provide a more secure and trustworthy prospect for e-Wallet transactions.

METODE

Undoubtedly, studying necessitates using research techniques as the fundamental basis for logical and analytical thought. The research technique is a systematic approach that seeks answers by following certain stages. This study employs a doctrinal legal research methodology with a legal and conceptual approach. This technique utilizes fundamental ideas and relevant legal theories to investigate the significant issue of the research as a component of this methodology. This study employs doctrinal legal research methodologies and examines primary and secondary legal documents. The research information is gathered and organized

interdisciplinary to explore the legal problems under study and provide suitable answers.

HASIL DAN PEMBAHASAN

The Significance of Trust in Electronic Transactions

In this day of advancing technology, electronic transactions have become the preferred option for many individuals. An increasingly common approach for conducting electronic transactions is the use of e-wallets. These digital platforms enable users to securely store and utilise funds electronically using devices such as smartphones[1]. Although e-wallets have many advantages, trust is still very important for successful transactions. Trust is the foundation of every relationship, including e-wallet transactions. In the context of digital transactions, trust is the user's confidence that the e-wallet platform can provide safe, reliable and quality services. If there is no trust, users are likely to avoid using e-wallets and opt for more familiar conventional payment methods[2]. Because it involves electronic transfer of money, trust is essential in e-wallet transactions. Customers must be assured that their funds will be processed safely and will not fall into the wrong hands[3]. They must also be assured that their personal information will be properly protected and that irresponsible parties will not take advantage of it. Customers are encouraged to believe in the security and confidentiality of e-wallet transactions due to these factors.

Commented [t1]: The results and discussion are well-developed but could benefit from stronger connections to the *real-world implications* of the proposed model. Present more specific findings from the analysis and show how they contribute to advancing the cybersecurity landscape for e-wallet transactions.
Suggested revision:
"The analysis reveals several key factors that contribute to the security of e-wallet transactions, including strong encryption protocols, multifactor authentication, and continuous regulatory oversight. The proposed model integrates these elements with a focus on government-industry collaboration to create a trusted ecosystem for digital payments. The findings demonstrate that implementing such a model could significantly reduce the frequency of cybersecurity breaches and build consumer confidence in digital financial platforms."

[1] Setiyawan, "Indonesian Online Shopping Practices in the COVID-19 Pandemic Era: A Study of Culture and Cyber Security Law," *Jurnal Hukum Novelty* 12, no. 1 (2021): 29–44, https://doi.org/10.26555/novelty.v12i01.a16944.

[2] E Watt, *State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law*, *State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law*, 2021, https://doi.org/10.4337/9781789900101.

[3] D Suhendi, "Cyber Laws Related to Prevention of Theft of Information Related to Acquisition of Land and Infrastructure Resources in Indonesia," *International Journal of Cyber Criminology* 15, no. 2 (2021): 135–43, https://doi.org/10.5281/zenodo.4766552.

Trust is also one of the key factors in building long-term relationships between customers and e-wallet service providers[4]. In the competitive world of business, customers have many choices and they will tend to choose platforms they trust. They want to feel comfortable and confident that the e-wallet service provider they choose is trustworthy and can provide quality service. Therefore, for e-wallet service providers, building customer trust is an important step to win the competition[5]. To build trust, e-wallet service providers must provide clear and transparent information about their security and privacy policies. Customers need to know how their data will be processed and protected. In addition, e-wallet service providers also need to adopt advanced security technology that can effectively protect customer transactions and data. Having a recognized security certification can also be proof of credibility for an e-wallet service provider.

Effective customer service is crucial for establishing confidence. Customers should have convenient access to the e-wallet service provider for prompt resolution of any issues or inquiries. Prompt and efficient problem-solving will enhance client trust and provide a feeling of security. Trust is a crucial element in electronic wallet transactions. Amidst the constant advancements in the digital realm, users need a sense of security and assurance when using electronic wallets. They want assurance that their cash will be securely handled and their personal information will be kept confidential. Establishing consumer trust is crucial for e-wallet service providers to outperform competitors and secure their sustained prosperity. Through the implementation of explicit security protocols, reliable security technology, and exemplary customer care, e-wallet transactions may provide a secure and easy alternative for all users.

Trust plays a key role in e-wallet transactions or electronic payments. Here are some reasons why trust is very important in this context: (1) Transaction Security:

[4] M E Amin, "Harmonization of Cyber Crime Laws with the Constitutional Law in Indonesia," *International Journal of Cyber Criminology* 15, no. 1 (2021): 79–94, https://doi.org/10.5281/zenodo.4766534.

[5] M Raymond, "Social Practices of Rule-Making for International Law in the Cyber Domain," *Journal of Global Security Studies* 6, no. 2 (2021): 1–24, https://doi.org/10.1093/jogss/ogz065.

Security is a major factor in e-wallet transactions. Users must be confident that their personal and financial information is safe during the transaction process. Trust in electronic payment systems can increase users' confidence that their data will be processed and stored safely. (2). Consumer Protection: Trust plays an important role in protecting consumers from potential fraud or unauthorized use of their information. If users have trust in an e-wallet platform, they will be more likely to use the service without excessive concerns regarding security. (3). Service Reputation: Trust is also closely related to the reputation of the e-wallet service provider. Companies that have a good reputation for providing reliable and safe services will find it easier to gain customer trust. A good reputation can build long-term customer loyalty. (4). Convenience and Efficiency: Users will feel comfortable using e-wallets if they trust that the process is efficient and seamless. Trust in ease of use and fast transaction processing can increase the adoption of electronic payments. Regulatory Compliance: (5) Trust is also related to compliance with regulations and security standards. An e-wallet platform that complies with regulations and security policies will be more appreciated by users, and this can create a sense of confidence in the use of the service. (6) Customer Support: Trust is also related to the quality of customer support. Users need to feel that they can get help if they encounter problems or questions regarding their e-wallets. Responsive and effective support can build customer trust. (7) Innovation and Sustainability: Trust is also strengthened by the ability of e-wallet service providers to continuously innovate and update their systems. Users want to know that the electronic payment systems they use will remain relevant and support technological developments.

By building and maintaining customer trust, e-wallet service providers can create a healthy and sustainable ecosystem for electronic payments[6]. This trust is an important basis for the growth and adoption of e-wallets in society.

e-Dompet Analyse the concept of cybersecurity in electronic wallet transactions.

[6] M Jha, "Cyber Security: Terms, Laws, Threats and Protection," *Proceedings - 2021 International Conference on Computing Sciences, ICCS 2021*, 2021, https://doi.org/10.1109/ICCS54944.2021.00037.

The popularity of e-wallets is growing rapidly due to the rising digitization. This digital payment technique provides both efficiency and ease in transactions. Nevertheless, within this ongoing digital transformation, the significance of cyber security is undeniable[7]. Understanding the cybersecurity aspects of e-wallet transactions is very important to ensure the security and confidentiality of our personal and financial information[8]. E-wallet is a type of digital wallet that allows users to store and transfer funds electronically. They are usually connected to a bank account or credit card, allowing users to make payments or transfer money with just a few clicks on their mobile devices. This convenience makes e-wallets the preferred choice for many people, but it also carries certain risks. One of the main concerns with e-wallet transactions is the potential for cyber attacks. Hackers are constantly looking for ways to exploit vulnerabilities in digital systems, and e-wallets are no exception. If hackers gain access to your e-wallet, they can potentially steal your personal and financial information, resulting in unauthorized transactions or even identity theft[9]. To protect against such threats, e-wallet providers implement various security measures to protect their users' information.

One such measure is encryption, which ensures that any data sent between the user's device and the e-wallet server is encrypted and cannot be intercepted by unauthorized parties. Additionally, e-wallets often require users to create unique and complex passwords, further enhancing security. Another important aspect of e-wallet security is user education. Users should be aware of potential risks and take necessary precautions to protect their e-wallets. This includes regularly updating their e-wallet applications and mobile devices with the latest security patches, as well as avoiding suspicious websites or links that could lead to phishing attempts. It

[7] R Walters, *Cyber Security, Artificial Intelligence, Data Protection & the Law*, *Cyber Security, Artificial Intelligence, Data Protection & the Law*, 2021, https://doi.org/10.1007/978-981-16-1665-5.

[8] Novi Asih Muharam and Azis Budianto, "Carding Crime Analysis as A Form of Cyber Crime in Indonesia ' s Criminal Law," *ICLSSEE* 1, no. 1 (2022): 1–6, https://doi.org/10.4108/eai.16-4-2022.2320085.

[9] E Syarief, "Security Concerns in Digital Transformation of Electronic Land Registration: Legal Protection in Cybersecurity Laws in Indonesia," *International Journal of Cyber Criminology* 16, no. 2 (2022): 32–46, https://doi.org/10.5281/zenodo.4766565.

is also recommended to only download e-wallet applications from trusted sources, such as official application stores. Cybercriminals often create fake e-wallet applications with the aim of stealing user information. By being alert and careful, users can significantly reduce the risk of becoming a victim of such fraud. In addition to these precautions, e-wallet users must also monitor their transactions regularly.

By regularly checking e-wallet reports and transaction history, users can quickly identify unauthorized activity and report it to their e-wallet provider. Timely reporting of suspicious transactions can help minimize potential losses and enable providers to take appropriate action to correct the situation. Additionally, e-wallet users should be careful when using public Wi-Fi networks. Public Wi-Fi networks are often insecure, making it easy for hackers to intercept data sent over them. Therefore, it is recommended to avoid e-wallet transactions when connected to public Wi-Fi. Instead, users should choose a more secure network, such as private mobile data or a trusted Wi-Fi network. In conclusion, although e-wallets offer convenience and simplicity in conducting digital transactions, it is important to understand and prioritize cybersecurity. By implementing proper security measures, such as encryption and strong passwords, as well as educating themselves about potential risks and taking necessary precautions, users can enjoy the benefits of e-wallets while ensuring the security and confidentiality of their personal and financial information. Remember, cybersecurity is not something to be taken lightly, and being proactive in protecting yourself is key to a secure e-wallet experience.

Cybersecurity is very important in e-wallet transactions because it involves the process of exchanging financial and personal information online. Here are several aspects that need to be understood regarding cyber security in e-wallet transactions:

1. Data Encryption: Information transmitted between the user's device and the e-wallet server must be encrypted using strong security protocols. The use of encryption protocols such as SSL/TLS can help protect data from attacks by third parties who try to access or manipulate information during the transaction process.

2. User Authentication: Security of e-wallet transactions requires strong user authentication. Dual authentication methods, such as using a password in conjunction with an SMS verification code or authentication app, can increase the level of security and prevent unauthorized access.
3. Protection Against Malware and Phishing: E-wallet users must be protected from the threat of malware and phishing attacks aimed at stealing login information or financial data. User education about digital security practices, as well as the implementation of effective security software, can help reduce these risks.
4. Risk Management and Anomaly Detection: The e-wallet system must be equipped with a risk management mechanism capable of detecting suspicious or unusual activity. Analysis of user behavior and transaction patterns can help detect inappropriate events and trigger countermeasures.
5. Continuous Security Monitoring: Continuous security monitoring is necessary to detect new security threats that may emerge. By monitoring transaction activity and attack patterns, e-wallet service providers can identify and respond quickly to potential risks.
6. Strong Security Policies: Adoption of strong security policies and ensuring that all stakeholders, including users, understand and follow recommended security practices, can help prevent attacks and protect the integrity of e-wallet transactions.
7. Regular Software Updates: Performing regular software updates is an important step in maintaining the security of your e-wallet system. The update includes necessary security fixes to address security gaps that may be discovered by malicious parties.
8. Cooperation with Security Authorities and Regulators: E-wallet service providers must cooperate with security authorities and regulators to ensure compliance with applicable security standards and to gain insight into the latest security threat trends.

Understanding and implementing these security measures is critical to building and maintaining user trust in e-wallet transactions. Strong cybersecurity is the foundation for the growth and acceptance of e-wallets in society.

Typical Risks Associated with e-Wallet Transactions

The popularity of e-wallets is growing rapidly due to the rising digitization. This digital payment technique provides both ease and efficiency in transactions[10]. However, in the midst of this digital revolution, the importance of cyber security cannot be denied. Understanding the cybersecurity aspects of e-wallet transactions is very important to ensure the security and confidentiality of our personal and financial information. E-wallet is a type of digital wallet that allows users to store and transfer funds electronically[11]. They are usually connected to a bank account or credit card, allowing users to make payments or transfer money with just a few clicks on their mobile devices. This convenience makes e-wallets the preferred choice for many people, but it also carries certain risks[12]. One of the main concerns in e-wallet transactions is the potential for cyber attacks. Hackers are constantly looking for ways to exploit vulnerabilities in digital systems, and e-wallets are no exception[13]. If hackers gain access to your e-wallet, they can potentially steal your personal and financial information, resulting in unauthorized transactions or even identity theft. To protect against such threats, e-wallet providers implement various security measures to protect their users' information. One such measure is encryption, which ensures

[10] R Buchan, "Cyber Espionage and International Law," *Research Handbook on International Law and Cyberspace*, 2021, https://api.elsevier.com/content/abstract/scopus_id/85127834341.

[11] B J Barrie J Gordon, "Toepaslike Regsraamwerk Vir Geoutomatiseerde Gesigherkenningstegnologie in Suid-Afrika," *Litnet Akademies:'n Joernaal Vir Die …* 2, no. 1 (2021): 1–17, https://doi.org/10.10520/ejc-litnet-v18-n1-a20.

[12] T M Makunya, "The Nexus between Constitutionalism, Peace and Security in the Law and Practice of the African Union," *RiA Recht in Afrika| Law in Africa| Droit En Afrique* 6, no. 2 (2022): 1–16, https://doi.org/10.5771/2363-6270-2022-1-53/the-nexus-between-constitutionalism-peace-and-security-in-the-law-and-practice-of-the-african-union-jahrgang-25-2022-heft-1.

[13] L A QUADRI and M O RASAQ, "Cyber Theatre: A Fifth Domain of International Politics," *Akdeniz Havzası ve Afrika Medeniyetleri …*, 2020, https://dergipark.org.tr/en/pub/akaf/issue/58349/799564.

that any data sent between the user's device and the e-wallet server is encrypted and cannot be intercepted by unauthorized parties. Additionally, e-wallets often require users to create unique and complex passwords, further enhancing security. Another important aspect of e-wallet security is user education.

Users should be aware of potential risks and take necessary precautions to protect their e-wallets. This includes regularly updating their e-wallet applications and mobile devices with the latest security patches, as well as avoiding suspicious websites or links that could lead to phishing attempts. It is also recommended to only download e-wallet applications from trusted sources, such as official application stores[14]. Cybercriminals often create fake e-wallet applications with the aim of stealing user information. By being alert and careful, users can significantly reduce the risk of becoming a victim of such fraud [15]. In addition to these precautions, e-wallet users must also monitor their transactions regularly[16].

By regularly checking e-wallet reports and transaction history, users can quickly identify unauthorized activity and report it to their e-wallet provider. Timely reporting of suspicious transactions can help minimize potential losses and enable providers to take appropriate action to correct the situation[17]. Additionally, e-wallet users should be careful when using public Wi-Fi networks. Public Wi-Fi networks are often insecure, making it easy for hackers to intercept data sent over them. Therefore, it is recommended to avoid e-wallet transactions when connected to public Wi-Fi. Instead, users should choose a more secure network, such as private mobile data or a trusted Wi-Fi network. In conclusion, although e-wallets offer

[14] Y Daeng et al., "Analisis Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber Di Indonesia," *Innovative: Journal Of ...*, 2023, http://j-innovative.org/index.php/Innovative/article/view/6376.

[15] Tri Ginanjar Laksana, "Perlindungan Hukum Konsumen E-Commerce Pada Produk Kesehatan: Pembelajaran Pada Kejahatan Siber," *Indo Green Journal* 2, no. 1 (2024): 31–44, https://doi.org/https://doi.org/10.31004/green.v2i1.45.

[16] S Ganapati, L Ortega Franco, and A N Le, "American State Government Cybersecurity Policies," *Proceedings of the 24th Annual ...*, 2023, https://doi.org/10.1145/3598469.3598540.

[17] Tri Ginanjar Laksana and Sri Mulyani, "Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusahaan," *Jurnal Ilmiah Multidisplin* 3, no. 1 (2024): 109–22, https://doi.org/https://doi.org/10.56127/jukim.v3i01.1143.

convenience and simplicity in conducting digital transactions, it is important to understand and prioritize cybersecurity. By implementing proper security measures, such as encryption and strong passwords, as well as educating themselves about potential risks and taking necessary precautions, users can enjoy the benefits of e-wallets while ensuring the security and confidentiality of their personal and financial information. Remember, cybersecurity is not something to be taken lightly, and being proactive in protecting yourself is key to a secure e-wallet experience.

Various threats can lurk e-wallet transactions, and understanding these risks is important to mitigate potential losses. Some common threats to e-wallet transactions involve: Phishing: Phishing attacks attempt to obtain personal or financial information from users by impersonating a trusted entity. E-wallet users can be targeted by phishing attacks targeting passwords, credit card numbers, or personal identification information. Malware: The use of malware, such as malicious software or viruses, can compromise the security of e-wallets. Malware can steal login information, financial data, or even control access to e-wallet accounts. Man-in-the-Middle Attacks: In this attack, the attacker tries to enter the communication between the user and the e-wallet server. This could allow attackers to steal or manipulate transaction data, including payment information. Device Security: If the user's device used to access the e-wallet is not secure, for example due to loss or theft, important information may be at risk. Device security includes screen locking, data encryption, and protection against unauthorized physical access. Credit Card and Chargeback Fraud:

The use of credit cards in e-wallet transactions can be a target for fraud, either through direct credit card theft or through unauthorized chargebacks. Fake Identities or Identity Theft: Criminals can use fake identities or steal user identities to carry out illegal or fraudulent e-wallet transactions. This can harm victims financially and damage their reputation. DDoS (Distributed Denial of Service) Attack: A DDoS attack aims to make e-wallet services inaccessible by flooding servers with fake internet traffic. This may disrupt service availability and cause disruptions in the transaction process.

Application Vulnerabilities: If there are vulnerabilities in the e-wallet software or application, attackers can exploit them to gain unauthorized access or carry out attacks such as code injection or web security vulnerabilities. Poor Network Security: Poor network security can facilitate unauthorized access to transaction data. Attacks such as network sniffing can be used to steal sensitive information sent over a network. Human Error: User errors, such as using weak passwords, not protecting devices properly, or sharing account information with others, can open the door to security threats. Implementing comprehensive security measures, such as data encryption, dual authentication, transaction monitoring, and user education, can help protect e-wallet transactions from these threats. Apart from that, regular system updates and collaboration with cybersecurity providers are also crucial in maintaining the security of e-wallet transactions.

The Significance of Legal Policy in Safeguarding Cybersecurity

Cybersecurity is a significant worry for both the government and society in this ever sophisticated digital age. The task of maintaining cyber security is becoming more complex due to the ever-expanding range of cyber threats and their persistent growth[18]. Therefore, solid and effective legal policies are needed to ensure optimal cyber security. Currently, cyber activities have become an inseparable part of everyday life. Along with the development of information and communication technology, many activities are carried out online, both by individuals and organizations. However, with the increasing number of these activities, cyber security risks also increase. In this case, the role of legal policy is very important to minimize cyber security risks. First, legal policies can regulate procedures for the safe use of information and communication technology. In this case, there needs to be clear laws regarding the protection of personal data and confidentiality of information. With legal policies that regulate this, individuals and organizations will be more vigilant in using technology and maintaining the security of their data[19].

[18] Mabizar, "Cyber Security Diplomacy and International Law.Pdf," 2021.
[19] Ulya Amaliya, "E-Commerce Di Singapura Dan Indonesia : Sebuah Perbandingan Kebijakan."

Apart from regulating procedures for the safe use of information and communication technology, legal policies can also provide strict sanctions for cyber security violations. In this case, it is important for the government to have adequate legal instruments to deal with criminal acts in cyberspace. With strict sanctions, it is hoped that it can prevent and reduce the number of cyber attacks carried out by irresponsible parties. Regulating and providing sanctions, legal policies can also facilitate cooperation between the government, private sector and society in maintaining cyber security. Through various cooperation programs, such as increasing technological capabilities, exchanging information, and increasing awareness of the importance of cyber security, it is hoped that we can build a strong cyber security ecosystem.

However, putting in place effective legal policies in maintaining cyber security is not an easy thing. Legal policies must be flexible and responsive to technological developments and ever-evolving cyber threats. Apart from that, there needs to be strict supervision in the implementation of these legal policies. This is to ensure that the activities carried out comply with applicable regulations. In conclusion, the role of legal policy is very important in ensuring cyber security. Legal policies can regulate procedures for the safe use of information and communication technology, provide strict sanctions, facilitate cooperation, and maintain flexibility and responsiveness in facing cyber threats. With the existence of solid and effective legal policies, it is hoped that optimal cyber security can be created.

Various threats can lurk e-wallet transactions, and understanding these risks is important to mitigate potential losses. Some common threats to e-wallet transactions involve: Phishing: Phishing attacks attempt to obtain personal or financial information from users by impersonating a trusted entity[20]. E-wallet users can be targeted by phishing attacks targeting passwords, credit card numbers, or personal identification information. Malware: The use of malware, such as malicious

[20] Setiyawan, "Indonesian Online Shopping Practices in the COVID- 19 Pandemic Era : A Study of Culture and Cyber."

software or viruses, can compromise the security of e-wallets. Malware can steal login information, financial data, or even control access to e-wallet accounts.

Man-in-the-Middle Attacks: In this attack, the attacker tries to enter the communication between the user and the e-wallet server. This could allow attackers to steal or manipulate transaction data, including payment information. Device Security: If the user's device used to access the e-wallet is not secure, for example due to loss or theft, important information may be at risk. Device security includes screen locking, data encryption, and protection against unauthorized physical access. Credit Cards and Chargeback Fraud: The use of credit cards in e-wallet transactions can be a target for fraud, either through direct credit card theft or through unauthorized chargeback actions. Fake Identities or Identity Theft: Criminals can use fake identities or steal user identities to carry out illegal or fraudulent e-wallet transactions. This can harm victims financially and damage their reputation. DDoS (Distributed Denial of Service) Attack: A DDoS attack aims to make e-wallet services inaccessible by flooding servers with fake internet traffic. This may disrupt service availability and cause disruptions in the transaction process.

Application Vulnerabilities: If there are vulnerabilities in the e-wallet software or application, attackers can exploit them to gain unauthorized access or carry out attacks such as code injection or web security vulnerabilities. Poor Network Security:

Poor network security can facilitate unauthorized access to transaction data. Attacks such as network sniffing can be used to steal sensitive information sent over a network. Human Error: User error, such as using a weak password, not protecting the device properly, or sharing account information with others, can open the door to security threats. Implementing comprehensive security measures, such as data encryption, dual authentication, transaction monitoring, and user education, can help protect e-wallet transactions from these threats. Apart from that, regular system updates and collaboration with cybersecurity providers are also crucial in maintaining the security of e-wallet transactions.

Elements of an all-encompassing legal framework for cybersecurity

Cybersecurity is a growing worry in the current digital age. Technology and digital infrastructure play a crucial role in our everyday lives, since they are essential for communication, transactions, and corporate operations. Nevertheless, the escalating quantity of cyber security risks necessitates an all-encompassing legislative framework to safeguard our data and information[21]. An all-encompassing legislative framework for cybersecurity must take into account many crucial elements. Initially, the topic at hand is personal data protection. Amidst a time when our personal data is becoming more susceptible to unauthorised access and improper use, it is imperative to establish legislation that safeguards our privacy. The policy should include a comprehensive explanation of the rights and responsibilities of data owners, as well as the penalties that will be imposed on individuals or entities found guilty of unauthorised data use. An all-encompassing legislative policy on cybersecurity must also include provisions for safeguarding vital infrastructure[22]. Infrastructure such as communications systems, transportation, energy, and banking networks are highly vulnerable to cyberattacks. Laws governing the protection of critical infrastructure must ensure that there are effective measures to prevent and respond to attacks, as well as cooperation between the public and private sectors to protect infrastructure that is vital to our daily lives.

A comprehensive cyber security legal policy must include strategies for handling and investigating cyber crimes. Cyber attacks not only threaten data and information, but can also have serious economic and social impacts. Therefore, this policy must consider effective law enforcement efforts to overcome attacks and arrest cybercriminals. In addition, a comprehensive cybersecurity legal policy must also involve diverse stakeholders, such as the private sector, government and civil society. Collaboration and cooperation between these sectors is essential to ensure strong and effective cybersecurity protection. In this case, policies must also regulate

[21] Botagoz Khamzina et al., "Determination of Cyber Security Issues and Awareness Training for University Students," *Ijet* 17, no. 18 (2022): 177–91.

[22] C Singh, "European Cyber Security Law in 2023: A Review of the Advances in the Network and Information Security 2 Directive 2022/2555," *Cyber Security: A Peer-Reviewed Journal* 9, no. 3 (2023): 1–22, https://www.ingentaconnect.com/content/hsp/jcs/2023/00000007/00000001/art00010.

the forms of cooperation that occur, such as exchanging information and training to increase awareness and expertise in dealing with cyber security threats[23].

A comprehensive cybersecurity legal policy must also consider regulatory and supervisory aspects. In a rapidly changing digital era, policies must be updated regularly to adapt to technological developments and new threats. In addition, this policy must include an effective monitoring mechanism to ensure that the established rules are implemented properly and are not misused[24]. In conclusion, a comprehensive cybersecurity legal policy must take into account several important components. Personal data protection, protection of critical infrastructure, handling cybercrime, stakeholder collaboration, and effective regulation and supervision are important elements that must be present in this policy model. With a strong legal policy in place, we will be able to address cyber security threats more effectively and protect our data and information better. A comprehensive cyber security legal policy model must cover various aspects to ensure effective protection of e-wallet transactions and data which is related. The following are several important components of a comprehensive cybersecurity legal policy model: Privacy and Data Protection: Establish clear and firm rules regarding privacy protection and management of personal data in e-wallet transactions. This includes encryption requirements, fair processing of data, and notification obligations in the event of a security breach.

Minimum Security Standards: Sets minimum security standards that e-wallet service providers must adhere to. This includes measures such as the use of encryption, strict access management, suspicious activity monitoring, and protection against common cyberattacks. Security Incident Reporting Obligations: Includes obligations to report significant security incidents to regulators, competent

[23] K Mania, "American and European Perspectives on Arbitration Agreements in Online Consumer Contracts," *Journal of International Arbitration* 36, no. 5 (2019): 659–70, https://api.elsevier.com/content/abstract/scopus_id/85081980532.

[24] G E Larrea and J C Quinzaños, "Report: Privacy in Latin America During COVID-19 Times and Reasonable Digital Security," *Global Privacy Law Review* 11, no. 1 (2021): 1–21, https://kluwerlawonline.com/journalarticle/Global+Privacy+Law+Review/2.2/GPLR2021021.

authorities and users. These reporting obligations must include sufficient information to understand the impact of the incident and the steps taken to address the issue. Consumer Protection Regulations: Establish rules and regulations that ensure adequate consumer protection, including dispute resolution mechanisms and the responsibility of e-wallet service providers for loss of user funds due to illegal actions or security accidents. Cybercrime Law: Introduces legislation that defines criminal offenses in the cyber domain, providing a legal basis for the prosecution of cybercriminals. This includes attacks on e-wallets, identity theft, and other acts of cybercrime. Oversight and Enforcement: Gives regulators the authority to monitor and enforce regulatory compliance. Clear and consistently enforced sanctions can be an incentive for compliance. Security Education and Training: Establishes requirements for cybersecurity education and training for e-wallet service providers and their employees. This education can involve understanding cyber threats, preventive measures, and responding to security incidents.

Collaboration with the Private Sector: Encourage collaboration and information sharing between governments, regulators and the private sector, including cybersecurity companies. This can create a strong ecosystem to address cyber threats. Security Testing and Auditing: Establish requirements for regular security testing and auditing by independent third parties. The results of these audits can help ensure compliance with security standards and identify potential vulnerabilities. Rapid Detection and Response Systems: Includes requirements for advanced threat detection systems and rapid response to security incidents. This involves proactive monitoring of suspicious activity and steps to quickly resolve attacks. Risk Management and Impact Assessment: Establish a risk management framework that enables e-wallet service providers to identify, assess, and manage security risks in a proactive manner. User Awareness and Education: Involves steps to increase user awareness of cyber threats, including education campaigns, security guides, and user training. Continuous Revision: Establish mechanisms to periodically review and revise policies to match technological developments, new cyber threats, and learning experiences. By integrating these components, a cybersecurity legal

policy model can be comprehensive and effective in protecting e-wallet transactions and overall user security.

Applying the Cybersecurity Legal Policy Model to e-Wallet Transactions

The rapid progression of technology has significantly transformed several facets of our life, including the manner in which we conduct transactions. The advent of digital wallets, often known as e-Wallets, in Indonesia has significantly enhanced the convenience of making payments and accessing financial services for the general population[25]. However, as the digital landscape evolves, the importance of cyber security also increases in ensuring the security and integrity of these transactions. Implementing a legal cyber security policy model is very important to protect consumers and service providers involved in e-Wallet transactions. The policy should include a comprehensive framework that addresses the evolving nature of cyber threats and provides clear guidance on how to prevent and respond to these threats. One of the key elements of an effective cybersecurity policy model for e-Wallet transactions is the establishment of a regulatory body to oversee and enforce cybersecurity measures[26]. This body should have the authority to set standards and guidelines for service providers, as well as the authority to conduct audits and investigations to ensure compliance. Another important aspect of this policy model is the integration of risk assessment and management. As cyber threats continue to evolve, it is important for service providers to conduct regular risk assessments to identify potential vulnerabilities in their systems.

This will allow them to implement adequate security measures and protocols to mitigate risks. Encryption and authentication protocols are also important

[25] D M Lloyd-Jones, "Status of Cardiovascular Health in US Adults and Children Using the American Heart Association's New 'Life's Essential 8' Metrics: Prevalence Estimates From the National Health and Nutrition Examination Survey (NHANES), 2013 Through 2018," *Circulation* 146, no. 11 (2022): 822–35, https://doi.org/10.1161/CIRCULATIONAHA.122.060911.

[26] K Cusi, "American Association of Clinical Endocrinology Clinical Practice Guideline for the Diagnosis and Management of Nonalcoholic Fatty Liver Disease in Primary Care and Endocrinology Clinical Settings: Co-Sponsored by the American Association for the Study of Liver Diseases (AASLD)," *Endocrine Practice* 28, no. 5 (2022): 528–62, https://doi.org/10.1016/j.eprac.2022.03.010.

components of a cybersecurity policy model. Service providers should be required to implement strong encryption algorithms to protect sensitive customer data during transmission. Additionally, strong authentication methods, such as two-factor authentication or biometric authentication, should be used to verify user identity and prevent unauthorized access. To further enhance the security of e-Wallet transactions, service providers should be mandated to implement strict access controls and monitoring systems. This includes implementing a strong password policy, limiting access to sensitive data where necessary, and implementing real-time monitoring and alerting systems to detect suspicious activity. In the event of a cybersecurity breach, service providers must have an incident response and recovery plan. This includes having processes and procedures in place to quickly identify and address breaches, notify affected users, and provide support and assistance to mitigate the impact of breaches. In conclusion, implementing a strong legal cybersecurity policy model is essential to guarantee the security and integrity of e-Wallet transactions. This includes the establishment of regulatory bodies, risk assessment and management, encryption and authentication protocols, access control and monitoring systems, and incident response and recovery plans. By prioritizing cyber security, we can exploit the full potential of e-Wallet transactions while safeguarding the interests of consumers and service providers.

Implementing a cyber security legal policy model in e-wallet transactions requires concrete steps and collaboration between the government, regulators, e-wallet service providers and other stakeholders. The following are several steps that can be taken to implement a cyber security legal policy model in e-wallet transactions: Determination of Security Standards: The government or regulator can set minimum security standards that must be adhered to by e-wallet service providers. These standards may include data encryption, protection against physical and cyber access, and strict risk management procedures. Data Protection Regulations: Adopting and strengthening data protection regulations is an important step. This may include rules regarding the processing and storage of personal data, as well as obligations to notify users of security breaches or data leaks. Security

Incident Reporting Obligations: E-wallet service providers should be required to report significant security incidents to regulators and users promptly. This obligation can enable rapid action to reduce the impact of attacks and mitigate further risks.

Cybercrime Act: Introduces cybercrime legislation that covers attacks on e-wallets, data theft, or other cyber activities. This can provide a legal basis for the prosecution of cybercriminals. Empowerment of Regulatory Authorities: Provide adequate authority to regulators to supervise and enforce cybersecurity policies. Such authorities must have the power to impose sanctions on violators and ensure compliance with regulations. Private Involvement in Policy Formulation: Involving the private sector, including technology and cybersecurity companies, in policy formulation. This ensures that the policies implemented are an effective response to the ever-changing dynamics of cyber threats. International Cooperation: Collaborating with other countries to overcome cross-border cyber threats. International agreements can help identify and follow up on cybercriminals who flee to foreign territories. Extension and Training: Involves outreach and training programs for e-wallet service providers and end users. Education and training increases awareness of cyber threats and helps mitigate risks caused by negligence or lack of understanding. Regular Security Tests and Audits: Requires e-wallet service providers to regularly conduct security tests and security audits. This may include independent inspections and regular evaluations to ensure compliance with security standards.

Rapid Detection and Response System: Implement a sophisticated threat detection system and respond quickly to security incidents. This could involve collaboration with specialist cybersecurity agencies and the use of artificial intelligence technology. Regulations Related to New Technologies: Adapting legal policies to developments in new technologies, such as blockchain or digital currencies, to ensure adequate protection. Through a holistic and collaborative approach, implementing a cyber security legal policy model in e-wallet transactions can help create a safe, reliable and trustworthy ecosystem for users and service providers.

An analysis of an effective legal framework for cybersecurity in e-wallet transactions.

Recent years have seen a surge in e-commerce due to fast technology advancements. The increasing dependence of individuals on digital platforms for daily transactions has made it crucial to have a robust cybersecurity strategy[27]. In Indonesia, one model that has achieved significant success in ensuring the security of e-wallet transactions is the Cybersecurity Legal Policy[28]. The Cybersecurity Law Policy is designed to address the increasing concerns and risks associated with online transactions[29]. Its main focus is to protect the interests of consumers and businesses operating in the e-commerce sector. By establishing a comprehensive set of guidelines and regulations, the policy aims to create a safe and trusted digital transaction environment. One of the successful case studies that highlights the effectiveness of the Cybersecurity Legal Policy is the implementation of security measures in e-wallet transactions[30]. E-wallets are becoming increasingly popular in Indonesia, allowing users to carry out various financial transactions, such as bill payments, online purchases, and fund transfers, all via their mobile devices. To ensure the security of e-wallet transactions, the Cybersecurity Legal Policy imposes strict regulations on e-wallet service providers.

These regulations include strong authentication processes, secure encryption technology, regular security audits, and strong firewall implementation. By complying with these regulations, e-wallet service providers can minimize the risk of data

[27] S Jadey, "Introduction to Cyber Security," *Methods, Implementation, and Application of Cyber Security Intelligence and Analytics*, 2022, https://doi.org/10.4018/978-1-6684-3991-3.ch001.

[28] G Grunberger, "American Association of Clinical Endocrinology Clinical Practice Guideline: The Use of Advanced Technology in the Management of Persons With Diabetes Mellitus," *Endocrine Practice* 27, no. 6 (2021): 505–37, https://doi.org/10.1016/j.eprac.2021.04.008.

[29] M Kamran, "Cyber Security Control Selection Based Decision Support Algorithm under Single Valued Neutrosophic Hesitant Fuzzy Einstein Aggregation Information," *AIMS Mathematics* 8, no. 3 (2023): 5551–73, https://doi.org/10.3934/math.2023280.

[30] A K Hiett, "Performance of IOTA Simple Rules, Simple Rules Risk Assessment, ADNEX Model and O-RADS in Differentiating between Benign and Malignant Adnexal Lesions in North American Women," *Ultrasound in Obstetrics and Gynecology* 59, no. 5 (2022): 668–76, https://doi.org/10.1002/uog.24777.

breaches and unauthorized access to users' financial information. The success of the Cybersecurity Legal Policy can be attributed to its comprehensive approach to cyber security. This policy recognizes that cyber security is not just about technology but also the legal framework that supports it. Therefore, this regulation includes provisions that outline the legal rights and responsibilities of consumers and business actors in the e-commerce sector. One important aspect of this policy is its emphasis on user education and awareness. E-wallet service providers are required to educate their users about the importance of online security and provide them with guidance on how to protect their personal information. This includes regular communication with users about potential risks, providing tips on creating strong passwords, and raising awareness about common scams and phishing attempts. Additionally, the Cybersecurity Legal Policy encourages collaboration between e-wallet service providers and other stakeholders, such as financial institutions and law enforcement agencies.

By fostering partnerships and sharing information, this policy enables a more coordinated and effective response to cyber threats. This collaborative approach has proven successful in detecting and preventing cybercriminal activities that can compromise the security of e-wallet transactions. Additionally, the Cybersecurity Legal Policy ensures enforcement of cybersecurity measures through strict penalties for non-compliance. E-wallet service providers who fail to meet required security standards can face fines, license revocation, and even criminal prosecution. This creates a strong barrier for businesses to prioritize cybersecurity and take the necessary steps to protect their users' information. Overall, the success of the Cybersecurity Legal Policy in safeguarding e-wallet transactions can be attributed to its holistic approach. By combining technological measures with legal regulations, user education, collaboration and strict law enforcement, this policy provides a comprehensive framework for ensuring the security of digital transactions. As e-commerce grows in Indonesia, the Cybersecurity Legal Policy serves as a valuable model for other countries looking to improve cybersecurity measures and protect their citizens' online transactions.

The development of cybersecurity legal policy models in e-wallet transactions often reflects different approaches in various countries. One case study that can be considered successful is Singapore, which has taken progressive steps in regulating and strengthening cyber security in e-wallet transactions. Case Study: Singapore Personal Data Protection Act (PDPA): Singapore has a Personal Data Protection Act (PDPA) which involves cybersecurity regulations to protect users' personal data. The PDPA requires companies and e-wallet service providers to protect personal information and take adequate security measures.

Monetary Authority of Singapore (MAS): The Monetary Authority of Singapore (MAS) has regulations governing security in financial services, including e-wallets. MAS issues guidelines and regulations that provide direction regarding security and risk management in the financial sector, including digital payment services. Technology Risk Management Guidelines: MAS has released Technology Risk Management Guidelines which provide specific guidelines for cyber security protection in the financial sector, including e-wallets. These guidelines cover aspects such as risk identification, data protection, encryption and security incident management. Cybersecurity Act: Singapore adopted the Cybersecurity Act which provides a legal basis for protecting critical infrastructure from cyber threats, including financial services. This includes risk management policies, incident reporting, and a framework for effective cybersecurity management. Partnership with the Private Sector: Singapore encourages collaboration between the private sector and the government in overcoming cyber threats. The government is working with cybersecurity companies and security agencies to improve overall security.

Active Law Enforcement: Singapore demonstrates active law enforcement against cyber security breaches. Penalties and sanctions are imposed on companies or individuals who violate cybersecurity rules, providing incentives for compliance. User Education and Awareness: Singapore promotes user education and awareness regarding cybersecurity practices. Awareness campaigns are held to provide information to the general public about the risks and actions they can take to protect themselves. Singapore's success in confronting cyber threats in e-wallet transactions

reflects a combination of strong regulations, collaboration between the public and private sectors, and a proactive approach to compliance and enforcement. This case study shows that success in cybersecurity requires cross-sector efforts and a holistic approach to involve multiple aspects of regulation, technology, and user awareness.

e-Dompet The Prospects of Cybersecurity in e-Wallet Transactions

The significance of cybersecurity is growing, particularly in the realm of e-wallet transactions. With the progression of technology and the growing dependence on digital wallets for financial transactions, the need for robust cybersecurity measures becomes more crucial[31]. The future of cyber security in e-wallet transactions lies in the development of innovative and sophisticated security systems[32]. With the rise of digital wallets, hackers and cybercriminals have become more sophisticated in their methods of stealing personal information and financial data. This requires implementing proactive and sophisticated security measures to protect sensitive user information. One of the future cybersecurity trends is the use of biometric authentication. Biometric authentication uses unique physical or behavioral characteristics, such as fingerprints or facial recognition, to verify a user's identity. This method is very secure and provides an additional layer of protection against fraudulent activity. Another future trend is the application of artificial intelligence (AI) in cybersecurity systems. AI can analyze large amounts of data and identify patterns that human analysts might miss. This enables AI-powered cybersecurity systems to detect and prevent cyber threats more effectively. Additionally, AI can also continuously learn and adapt to new threats, making it an important tool in fighting cybercrime.

Blockchain technology also plays an important role in enhancing the security of e-wallet transactions. Blockchain is a decentralized and transparent ledger that

[31] Cusi, "American Association of Clinical Endocrinology Clinical Practice Guideline for the Diagnosis and Management of Nonalcoholic Fatty Liver Disease in Primary Care and Endocrinology Clinical Settings: Co-Sponsored by the American Association for the Study of Liver Diseases (AASLD)."

[32] Grunberger, "American Association of Clinical Endocrinology Clinical Practice Guideline: The Use of Advanced Technology in the Management of Persons With Diabetes Mellitus."

records all transactions in a tamper-proof and irreversible manner. By utilizing blockchain technology, e-wallet providers can ensure that all transactions are recorded securely and cannot be changed. Additionally, blockchain provides users with a higher level of trust and confidence, knowing that their transactions are secure and tamper-proof. In the future, collaboration between cybersecurity experts, e-wallet providers, and regulatory bodies will be critical in ensuring the security of e-wallet transactions. By working together, they can develop and implement comprehensive security frameworks and standards that protect user information and financial data. Education and awareness are also important in the future of cybersecurity in e-wallet transactions. Users should be educated on online security best practices and alert to potential threats. E-wallet providers should also invest in educating their users about the importance of strong passwords, enabling multi-factor authentication, and being careful when sharing personal information online. The future of cybersecurity in e-wallet transactions is very promising. With continued technological advancements, innovative security measures, and collective efforts from various stakeholders, we can ensure that e-wallet transactions remain safe and protected from cyber threats. As users, it is important to stay informed and take the necessary precautions to protect our financial transactions in the digital world.

The future of cyber security in e-wallet transactions will continue to evolve as technology advances and cyber threats change. Some trends and developments that can be anticipated in the context of e-wallet cybersecurity include: Stronger Authentication Technologies: The use of stronger authentication methods, such as biometrics (such as fingerprint or facial recognition), may become the standard for increasing security in accessing e-wallets. wallet. This can reduce the risk of unauthorized access and fraud. Blockchain and Distributed Ledger Technology: Adoption of blockchain technology and Distributed Ledger Technology (DLT) can help improve cybersecurity in e-wallet transactions. This technology can provide transparency, data integrity, and resilience to data changes. Enhanced Device Security: Enhanced device security will be a focus, with features such as hardware

and software encryption, better network security, and measures to protect devices from physical and cyber attacks.

Integration of Artificial Intelligence (AI) and Data Analytics: The use of artificial intelligence and data analytics to detect suspicious transaction patterns or strange activity can help improve response to cyber threats by providing early detection and predictive analysis. Global Agreement on Security Standards: Increasing reliance on cross-border transactions and digital currencies could encourage international cooperation in developing and adhering to uniform security standards. Stricter Regulation: Expect increased regulation and security requirements in the e-wallet industry to protect consumers and respond to increasingly complex cyber threats. Better User Education and Awareness: User education about cybersecurity practices will become more important. Increased user awareness of potential risks and the actions they can take to protect themselves can help reduce attacks involving user carelessness. More Comprehensive Multi-Factor Security: A multi-factor security implementation that involves a combination of something the user has (such as a password), something the user knows (such as a verification code), and something uniquely associated with the user (such as a fingerprint or facial recognition) could become standard.

Development of Rapid Detection and Response Systems: More sophisticated threat detection systems and rapid response will be critical to confronting ever-evolving cyberattacks. Cybersecurity Human Resource Development: With the increasing complexity of cyber threats, training and development of cybersecurity human resources will become a priority, including cybersecurity experts, security analysts, and information security professionals. Overall, the future of cybersecurity in e-wallet transactions will involve developing technology and policies that align with the evolution of cyber threats. Increased collaboration between the private sector, government and cybersecurity agencies will be key to creating a secure and reliable e-wallet environment.

SIMPULAN

The proliferation of e-wallet use in Indonesia has seen rapid and significant expansion, primarily due to the government's proactive efforts to establish a society that relies less on physical currency and the inherent ease provided by these digital platforms. Nevertheless, the growing use of electronic wallets increases the likelihood of encountering cyber threats and vulnerabilities. As technology advances, cybercriminals continuously develop innovative methods to exploit vulnerabilities in security systems. Therefore, it is crucial to implement robust cybersecurity policies to protect against these threats effectively. In conclusion, The Cybersecurity Legal Policy Model offers a thorough framework for enhancing the security of e-wallet transactions in Indonesia. The policy delineates a range of measures and principles that must be adhered to to safeguard the personal and financial data of e-wallet users. The procedures include robust authentication mechanisms, data transfer encryption, periodic security audits, and deployment of sophisticated firewalls and intrusion detection systems. Through implementing the Cybersecurity Legal Policy Model Conclusion, suppliers of e-wallet services may cultivate a sense of assurance and reliance among their consumers. Customers' trust in the security of their sensitive information increases their propensity to use e-wallets as a dependable and expedient means of conducting transactions. This, in turn, facilitates the achievement of the government's objective of establishing a society that operates without the need for physical currency.

DAFTAR PUSTAKA

Abdul Halim Barkatullah. “Urgensi Perlindungan Hak-Hak Konsumen Dalam Transaksi Di E-Commerce.” *Jurnal Hukum* 2, no. Hukum Bisnis (2007): 247–70.

Alfis Setyawan, Kiki Ristanto. “Tinjauan Yuridis Pertanggung Jawaban Hukum Marketplace Online Terhadap Pelanggaran Hak Cipta.” *Journal of Judicial Review* 18, no. Hukum Bisnis (2016): 160–72.

Amanullah, Bastian. “Pengaruh Persepsi Manfaat, Kemudahan Penggunaan, Dan Kepercayaan Terhadap Sikap Positif Penggunaan Layanan Mobile Banking,” 2014.

Amin, M E. “Harmonization of Cyber Crime Laws with the Constitutional Law in Indonesia.” *International Journal of Cyber Criminology* 15, no. 1 (2021): 79–94. https://doi.org/10.5281/zenodo.4766534.

Anggelia, Nur, and Putri Sulaeman. “Pengaruh Digital Marketing Dan Kepercayaan Terhadap Keputusan Pembelian Produk Hyde Beauty Skincare Di Kabupaten Karawang” 3 (2023): 8271–79.

Antonius Dwicky Cahyadi. “Kesadaran Hukum Konsumen Dalam Memperjuangkan Hak - Haknya Atas Kerugian Yang Dialami Dalam Melakukan Transaksi Elktronik.” *Skripsi Universitas Atma Jaya Yogyakarta Fakultas Hukum*, 2014.

Atta, Qamar, and Ul Haq. “Cyber Security and Analysis of Cyber-Crime Laws to Restrict Cyber Crime in Pakistan.” *Computer Network and Information Security* 1, no. 1 (2019): 62–69. https://doi.org/10.5815/ijcnis.2019.01.06.

Buchan, R. “Cyber Espionage and International Law.” *Research Handbook on International Law and Cyberspace*, 2021. https://api.elsevier.com/content/abstract/scopus_id/85127834341.

Cusi, K. “American Association of Clinical Endocrinology Clinical Practice Guideline for the Diagnosis and Management of Nonalcoholic Fatty Liver Disease in Primary Care and Endocrinology Clinical Settings: Co-Sponsored by the American Association for the Study of Liver Diseases (AASLD).” *Endocrine Practice* 28, no. 5 (2022): 528–62. https://doi.org/10.1016/j.eprac.2022.03.010.

Daeng, Y, J Levin, K Karolina, M R Prayudha, and … “Analisis Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber Di Indonesia.” *Innovative: Journal Of …*, 2023. http://j-innovative.org/index.php/Innovative/article/view/6376.

Dian Islami. “Analisis Konstekstual Pada Strategi Keamanan Siber Mesir 2017 - 2021 Dalam Upaya Pengamanan Siber Nasional.” *Pendidikan, Sejarah, Dan Ilmu - Ilmu Sosial* 5, no. 1 (2021): 159–70.

Dwi Sakti Muhamad Huda. “Tinjauan Hukum Islam Terhadap Penerapan Khiyar Dalam Jual Beli Barang Elektronik Secara Online.” *Skripsi Muamalat Fakultas Syariah Dan Hukum Universitas Islam Negeri Sunan Kalijaga Yogyakarta*, 2013.

Elina Rudiastari. “Perlindungan Hukum Terhadap Konsumen Dalam Perjanjian Jual

Beli Melalui E-Commerce Di Indonesia." *Jurnal Sosial Dan Humaniora* 5, no. Hukum Bisnis (2015): 71–81.

Ganapati, S, L Ortega Franco, and A N Le. "American State Government Cybersecurity Policies." *Proceedings of the 24th Annual …*, 2023. https://doi.org/10.1145/3598469.3598540.

Gordon, B J Barrie J. "Toepaslike Regsraamwerk Vir Geoutomatiseerde Gesigherkenningstegnologie in Suid-Afrika." *Litnet Akademies:'n Joernaal Vir Die …* 2, no. 1 (2021): 1–17. https://doi.org/10.10520/ejc-litnet-v18-n1-a20.

Grunberger, G. "American Association of Clinical Endocrinology Clinical Practice Guideline: The Use of Advanced Technology in the Management of Persons With Diabetes Mellitus." *Endocrine Practice* 27, no. 6 (2021): 505–37. https://doi.org/10.1016/j.eprac.2021.04.008.

Haikal Ramadhan, Aminah, Suradi. "Perlindungan Hukum Terhadap Penggunaan Uang Elektronik Dalam Melakukan Transaksi Ditinjau Dari Peraturan Bank Indonesia Tantang Uang Elektronik (e-Money)." *E-Journal Diponogor* 5, no. Hukum e-commerce (2016): 1–18.

Hiett, A K. "Performance of IOTA Simple Rules, Simple Rules Risk Assessment, ADNEX Model and O-RADS in Differentiating between Benign and Malignant Adnexal Lesions in North American Women." *Ultrasound in Obstetrics and Gynecology* 59, no. 5 (2022): 668–76. https://doi.org/10.1002/uog.24777.

Ita Febrihapsari. "Perlindungan Hukum Terhadap Konsumen Yang Mengalami Kerugian Akibat Promosi Potongan Harga Dalam Perjanjian Jual Beli Online." *Skripsi Kementrian Riset, Teknologi Dan Pendidikan Tinggi Universitas Jember Fakultas Hukum*, 2016.

Jadey, S. "Introduction to Cyber Security." *Methods, Implementation, and Application of Cyber Security Intelligence and Analytics*, 2022. https://doi.org/10.4018/978-1-6684-3991-3.ch001.

Jha, M. "Cyber Security: Terms, Laws, Threats and Protection." *Proceedings - 2021 International Conference on Computing Sciences, ICCS 2021*, 2021. https://doi.org/10.1109/ICCS54944.2021.00037.

Kamran, M. “Cyber Security Control Selection Based Decision Support Algorithm under Single Valued Neutrosophic Hesitant Fuzzy Einstein Aggregation Information.” *AIMS Mathematics* 8, no. 3 (2023): 5551–73. https://doi.org/10.3934/math.2023280.

Khamzina, Botagoz, Nabuova Roza, Gulsara Zhussupbekova, Aiganym Aten, and Baikulova Aigerim Meirkhanovna. “Determination of Cyber Security Issues and Awareness Training for University Students.” *Ijet* 17, no. 18 (2022): 177–91.

Laksana, Tri Ginanjar. “Perlindungan Hukum Konsumen E-Commerce Pada Produk Kesehatan: Pembelajaran Pada Kejahatan Siber.” *Indo Green Journal* 2, no. 1 (2024): 31–44. https://doi.org/https://doi.org/10.31004/green.v2i1.45.

Laksana, Tri Ginanjar, and Sri Mulyani. “Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusahaan.” *Jurnal Ilmiah Multidisplin* 3, no. 1 (2024): 109–22. https://doi.org/https://doi.org/10.56127/jukim.v3i01.1143.

Larrea, G E, and J C Quinzaños. “Report: Privacy in Latin America During COVID-19 Times and Reasonable Digital Security.” *Global Privacy Law Review* 11, no. 1 (2021): 1–21. https://kluwerlawonline.com/journalarticle/Global+Privacy+Law+Review/2.2/GPLR2021021.

Lia Catur Muliastuti. “Perlindungan Hukum Bagi Para Pihak Dalam Perjanjian Jual Beli Melalui Media Internet.” *Tesis Program Studi Magister Kenotariatan Program Pascasarjana Universitas Diponogoro*, 2010.

Lin, C L. “A Study on Anglo-American Equity Law Applied to Litigation and Arbitration in Taiwan’s Patent Dispute Solutions.” *NTUT Journal of Intellectual Property Law and Management* 11, no. 2 (2022): 87–118. https://api.elsevier.com/content/abstract/scopus_id/85166954104.

Lloyd-Jones, D M. “Status of Cardiovascular Health in US Adults and Children Using the American Heart Association’s New ‘Life’s Essential 8’ Metrics: Prevalence Estimates From the National Health and Nutrition Examination Survey (NHANES), 2013 Through 2018.” *Circulation* 146, no. 11 (2022): 822–35.

https://doi.org/10.1161/CIRCULATIONAHA.122.060911.

Mabizar. “Cyber Security Diplomacy and International Law.Pdf,” 2021.

Makunya, T M. “The Nexus between Constitutionalism, Peace and Security in the Law and Practice of the African Union.” *RiA Recht in Afrika/ Law in Africa/ Droit En Afrique* 6, no. 2 (2022): 1–16. https://doi.org/10.5771/2363-6270-2022-1-53/the-nexus-between-constitutionalism-peace-and-security-in-the-law-and-practice-of-the-african-union-jahrgang-25-2022-heft-1.

Mania, K. “American and European Perspectives on Arbitration Agreements in Online Consumer Contracts.” *Journal of International Arbitration* 36, no. 5 (2019): 659–70. https://api.elsevier.com/content/abstract/scopus_id/85081980532.

Marlien, R.A. “Pengaruh Reputasi, Privasi, Dan Keamanan Terhadap Kepercayaan (Trust) Pengguna Internet Di Semarang Dalam Sistem e-Commerce.” *Ekonomi Universitas STIKUBANK Semarang* 3, no. Ekonomi (2015): 86–101.

Melisa Monica Sumenge. “Penipuan Menggunakan Media Internet Berupa Jual Beli Online.” *Jurnal Lex Crimen* 2, no. Hukum Bisnis (2013): 102–12.

Milano, F. “Detection of Cyber-Attacks of Power Systems through Benford’s Law.” *IEEE Transactions on Smart Grid* 12, no. 3 (2021): 2741–44. https://doi.org/10.1109/TSG.2020.3042897.

Muharam, Novi Asih, and Azis Budianto. “Carding Crime Analysis as A Form of Cyber Crime in Indonesia ’ s Criminal Law.” *ICLSSEE* 1, no. 1 (2022): 1–6. https://doi.org/10.4108/eai.16-4-2022.2320085.

Nindy Ockta Mutiara Hapsari. “Peran Notaris Dalam Upaya Perlindungan Hukum Terhadap Pembeli Dalam Jual Beli Online.” *Jurnal Reportorium* 4, no. Hukum Bisnis (2017): 158–64.

Nurul Hasanah Syah. “Analisis Faktor - Faktor Yang Mempengaruhi Keputusan Pembelian Melalui Online Shop Di Kota Medan.” *Tesis Universitas Islam Negeri Sumatera Utara*, 2017.

Pudji utomo, Edang Lestariningsih, Yohanes Suhari. “Kepercayaan Terhadap Internet Serta Pengaruhnya Pada Pencarian Informasi Dan Keinginan Membeli Secara Online.” *Jurnal Ilmu Hukum*, 2004.

Purdon, L, and F Vera. “Regional Cybersecurity Approaches in Africa and Latin America.” *⋯ Handbook of International Cybersecurity* 5, no. 3 (2020): 16. https://doi.org/10.4324/9781351038904-23.

QUADRI, L A, and M O RASAQ. “Cyber Theatre: A Fifth Domain of International Politics.” *Akdeniz Havzası ve Afrika Medeniyetleri ⋯*, 2020. https://dergipark.org.tr/en/pub/akaf/issue/58349/799564.

R.A Marlien, Probo. “Pengaruh Reputasi, Privasi, Dan Keamanan Terhadap Kepercayaan (Trust) Pengguna Internet Di Semarang Dalam Sistem e-Commerce.” *Jurnal Manajemen Dan Bisnis* 14, no. 2002 (2010): 1–8.

Raymond, M. “Social Practices of Rule-Making for International Law in the Cyber Domain.” *Journal of Global Security Studies* 6, no. 2 (2021): 1–24. https://doi.org/10.1093/jogss/ogz065.

Satyanegara, N, J Priyono, and ... “Perlindungan Data Pribadi Di Indonesia Dalam Rangka Perdagangan Elektronik (E-Commerce).” *Diponegoro Law Journal* 1, no. 1 (2020): 1–15. https://ejournal3.undip.ac.id/index.php/dlr/article/view/27044.

Setiyawan. “Indonesian Online Shopping Practices in the COVID-19 Pandemic Era: A Study of Culture and Cyber Security Law.” *Jurnal Hukum Novelty* 12, no. 1 (2021): 29–44. https://doi.org/10.26555/novelty.v12i01.a16944.

Setiyawan, R. “Indonesian Online Shopping Practices in the COVID- 19 Pandemic Era : A Study of Culture and Cyber.” *Jurnal Hukum Novelty* 12, no. 01 (2021): 29–44.

Shihab, Ahmad Murtadho dan Muhammad Rifki. “Analisis Situs E- Tourism Indonesia : Studi Terhadap Persebaran Geografis, Pengklasifikasian Situs Serta Pemanfaatan Fungsi Dan Fitur.” *Universitas Indonesia* 2, no. Pariwisata (2008): 13–25.

Singh, C. “European Cyber Security Law in 2023: A Review of the Advances in the Network and Information Security 2 Directive 2022/2555.” *Cyber Security: A Peer-Reviewed Journal* 9, no. 3 (2023): 1–22. https://www.ingentaconnect.com/content/hsp/jcs/2023/00000007/00000001/art00010.

Sri Anggraeini Kusuma Dewi. “Perjanjian Jual Beli Barang Melalui Elektronik E-Commerce.” *Jurnal Ilmiah Teknologi Dan Informasia ASIA (JITIKA)* 9, no. Hukum Bisnis (2015): 1–5.

Suhendi, D. “Cyber Laws Related to Prevention of Theft of Information Related to Acquisition of Land and Infrastructure Resources in Indonesia.” *International Journal of Cyber Criminology* 15, no. 2 (2021): 135–43. https://doi.org/10.5281/zenodo.4766552.

Sukarno. “Kajian Yuridis Terhadap Perjanjian Jual Beli Melalui E-Commerce Kaitannya Dengan Perlindungan Konsumen.” *Jurnal Info Hukum* 7, no. Hukum Bisnis (2013): 47–67.

Syarief, E. “Security Concerns in Digital Transformation of Electronic Land Registration: Legal Protection in Cybersecurity Laws in Indonesia.” *International Journal of Cyber Criminology* 16, no. 2 (2022): 32–46. https://doi.org/10.5281/zenodo.4766565.

Ulya Amaliya. “E-Commerce Di Singapura Dan Indonesia : Sebuah Perbandingan Kebijakan.” *Jurnal Ilmu Sosial Dan Ilmu Politik* 1, no. e-commerce (2009): 1–21.

Walters, R. *Cyber Security, Artificial Intelligence, Data Protection & the Law*. *Cyber Security, Artificial Intelligence, Data Protection & the Law*, 2021. https://doi.org/10.1007/978-981-16-1665-5.

Watt, E. *State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law*. *State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law*, 2021. https://doi.org/10.4337/9781789900101.

Yang, M. “Cashless Transactions: A Study on Intention and Adoption of e-Wallets.” *Sustainability (Switzerland)* 13, no. 2 (2021): 1–18. https://doi.org/10.3390/su13020831.

Yusuf Karuniawan. “Pandangan Hukum Islam Terhadap Praktek Jual Beli Online Dengan Sistem Lelang.” *Skripsi Hukum Ekonomi Syariah Institut Agama Islam Negeri (IAIN) Surakarta*, 2017.

Constitution

———1945 Constitution
———Law no. 14 of 2008 concerning Openness of Public Information
———. “Republic of Indonesia Law Number 8 of 1999 concerning Consumer Protection.
_____Law no. 11 of 2020 concerning Personal Data Protection
_____Law Number 14 of 2008 concerning Openness of Public Information
_____Law Number 36 of 1999 concerning Telecommunications
———Law Number 11 of 2008 concerning Electronic Information and Transactions as amended by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions.

Government Regulations and Legal Policies

_____ Government Regulation Number 82 of 2012 concerning Implementation of Electronic Systems and Transactions.
_____Government Regulation Number 71 of 2019 concerning Implementation of the ITE Law.
_____Government Regulation Number 82 of 2012 concerning further provisions related to the operation of electronic systems, including security and protection of personal data.
_____Government Regulation Number 80 of 2019 regulates consumer rights and obligations in electronic transactions
_____ Presidential Regulation Number 53 of 2017 concerning National Cyber Security Policy.
_____Presidential Decree Number 85 of 2018 concerning the Grand Strategy for National Cyber Ecosystem Development is also important in the context of criminal liability in the cyber sector