Amnesti: Jurnal Hukum
Vol. 6 No. 2 (2024) pp. 174-185
p-ISSN: 2656-3029 | e-ISSN: 2775 - 0604

Legal Protection of Paylater Users on E-Commerce Platforms for Personal Data Leakage

Angelia[1*], Finesse Sly Oeijono[2], Daniel Limbong[3]
[1*,2,3]Universitas Prima Indonesia, Medan, Indonesia
*email: angeliachandra003@gmail.com

DOI: https://doi.org/10.37729/amnesti.v6i2.5352

Submitted: Juni 2024 *Revision: July 2024* *Accepted: August 2024*

Keywords : *Legal Protection, Paylater, Personal Data Leakage*

ABSTRACT

The development of increasingly sophisticated technology makes it easier for us to transact and make payments electronically / online, where one of the payment methods used is Paylater. However, this system often becomes a loophole for criminal acts such as, personal data leaks that can cause data breaches and identity theft due to disclosure of customer information, bank accounts, credit card information, and other personal data by users who are not responsible for completing their administration, so that it can result in immaterial losses. This research aims to find out how legal protection efforts for paylater users who experience personal data leaks in e-commerce in Indonesia, to achieve this goal the research method used is normative research method. The results of the research obtained that if there is a violation of personal data protection, the perpetrator may be subject to sanctions in accordance with applicable provisions as stipulated in Article 67 Paragraph 2 of the PDP Law.

Kata Kunci : *Perlindungan Hukum, Paylater, Kebocoran Data Pribadi*

ABSTRAK

Perkembangan teknologi yang semakin canggih memudahkan kita untuk bertransaksi dan melakukan pembayaran dengan cara elektronik/online, dimana salah satu metode pembayaran yang digunakan yaitu Paylater. Kedati demikian, sistem ini kerap menjadi celah tindak pidana seperti, kebocoran data pribadi yang dapat menyebabkan pelanggaran data dan pencurian data identitas karena pengungkapan informasi pelanggan, rekening bank, informasi kartu kredit, dan data pribadi lainnya oleh pengguna yang tidak bertanggungjawab atas penyelesaian administrasinya, sehingga dapat mengakibatkan kerugian

immaterial. Penelitian ini bertujuan untuk mengetahui bagaimana upaya perlindungan hukum bagi pengguna paylater yang mengalami kebocoran data pribadi pada e-commerce di Indonesia, untuk mencapai tujuan tersebut metode penelitian yang digunakan yaitu metode penelitian normative. Hasil penelitian yang didapatkan bahwa apabila terjadi pelanggaran terhadap perlindungan data pribadi, maka pelaku dapat dikenakan sanksi sesuai ketentuan yang berlaku sebagaimana diatur dalam Pasal 67 Ayat 2 UU PDP.

1. INTRODUCTION

The development of increasingly sophisticated technology makes it easier for people to transact and make payments with electronic (online) systems (Aulia, 2020). Electronic system is one of the payment methods used with the help of certain applications, where this system is a method of doing business via the internet using gadgets, digital financial services, and internet networks (Putra & Nugroho, 2021), so that it can make it easier for sellers and buyers to make transactions anywhere and anytime safely and comfortably by saving time. This makes it easier to record finances without having to go to an *automated teller machine* (ATM).

Electronic payment systems offer electronic means to verify and document transactions, thus eliminating the need for physical paper records, by utilising bookkeeping tools can simplify the process of entering numbers and eliminate the need for human data entry (Manurung & Rahardjo, 2019). Electronic payment systems have several types of payments that can be made through such as: internet banking, credit cards, virtual accounts, E-money, QR codes, paylater, digital wallets. However, one of the payment methods by way of paylater has experienced a surge in popularity since the beginning of the pandemic, where paylater is useful in managing expenses and cash flow effectively in people's lives. The main elements that drive the rise of paylater services as an alternative to financial management are security and convenience considerations, so that consumers can easily fulfil their daily needs (Tsani, 2024).

It is known that more than 15 (fifteen) applications that provide services paylater that establishes partnerships with third-party service providers (Ahdiat, 2023). Nevertheless, online payment systems are often a source of criminality, one of which is personal data leakage which can lead to data breaches and identity theft due to disclosure of customer information, bank

accounts, credit card information, and other personal data by users who are not responsible for their administrative settlement, which can result in immaterial losses. Article 26 of Law Number 19 of 2016 on the Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law) states that the acquisition of any personal data using electronic means must be done in accordance with the law. This requires the consent of the data owner, so individuals who violate this clause may be subject to legal action for the harm caused.

Article 1 paragraph (1) of the Criminal Code (KUHP) explains that no act can be criminalised except on the strength of a criminal provision in the pre-existing criminal legislation. Then, in the ITE Law regarding electronic information and transactions, where this provision applies to anyone who takes legal action both inside and outside the territory of Indonesia with legal consequences. This is also regulated as in Article 30 Paragraph 3 ITE Law that *"every person intentionally and without rights or unlawfully accesses a computer and/or electronic system in any way by violating, breaking through, exceeding, or breaking into the security system."* Thus, this Article explains that accessing computers and/or devices in violation of the law is an unlawful act.

It is known that more than 2 million samples of *online* transaction users and *offline* transactions were collected from the five largest *marketplaces* from the seven largest retail *merchants* throughout Indonesia in 2023 spread across 34 provinces, as many as 43.9% of *paylater* users come from the millennial generation or those aged 26-35 years. Then, as many as 26.5% of users are from gen Z or the 18-25 age group. The survey also recorded that the majority or 63.1% of *paylater* users use the service for online transactions. Then as many as 16.5% use *paylater* for offline transactions, and as many as 20.4% use both (Muhamad, 2023). This is also in line with the return of normal post-pandemic activities, where consumers have started to return to offline shopping.

In the paylater service, the agreement is made through an electronic contract that involves personal data such as the Population Identification Number (NIK) which is very important and protected from being misused. Electronic contracts are different from conventional contracts, because electronic contracts are agreements based on the principle of freedom of contract and are approved through the use of the internet or online platforms.

Paylater services function as E-commerce service providers, where third parties are involved in the financial technology (fintech) field (Fadhli et al., 2022).

Personal data protection is a right to privacy, this is stated in Article 1 Paragraph 1 of the Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems (Permen Keminfo PDP) that personal data is certain individual data that is stored, maintained, and maintained the truth and protected confidentiality. Thus, personal data is an integral aspect of the right to privacy. Entities involved in personal data protection are referred to as parties, specifically first parties, second parties, and third parties. The first party refers to the individual or entity that takes action or holds the position as the owner of the personal data. The owner is a legal entity in the form of an individual, and the second party is the recipient of personal data from the first party and serves as the subject in this context.

However, the increasing consumptive behaviour and dependence of users in using the Paylater feature becomes a gap in leaking mobile phone data if users are not vigilant, where high installment interest of 2.95% with an additional handling fee of 1% or even more according to the Paylater used and fines for users who are late paying bills according to the repayment due date agreement of 5% (Romadhona, 2022), so it is necessary that Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) be officially implemented on 17 October 2022 as a controller of personal data in e-commerce activities, this is a form of security improvement measures to protect personal data, especially for users of E-commerce platforms in Indonesia. However, the regulation is fragmented among various laws and regulations and lacks a coherent framework.

Thus, it is important that legal protection for users or consumers is the user's right to be in the law scope of the business entity. These measures ensure smooth operations of service-based businesses and instil a sense of security and comfort among users who choose E-commerce as their preferred online transaction service. In addition to offering follow-up measures, it is imperative to immediately address concerns so that the issue does not persist as it may result in lawsuits or civil sanctions for parties involved in data leaks.

2. RESEARCH METHOD

The research method that the author uses in this research is normative juridical legal research with a qualitative approach (Marzuki, 2009). This study involves literature review as the basic material to be researched and by conducting a search for regulations and literature related to the problem under study (Suratman & Dillah, 2013). This qualitative approach method is intended to explain and understand and the legality of laws and regulations governing consumer protection relating to personal data against fraud committed by stealing data used to register for Paylater services.

3. RESULTS AND DISCUSSION

3.1 Legal Efforts to Protect Personal Data Leakage of Paylater Users in E-Commerce

The ease of paylater in e-commerce is often exploited by certain individuals with certain motives. It is important that to protect the personal data of paylater users in e-commerce, legal action is needed that can be taken based on public events (Berliana, 2023). One of these efforts is the recognition that agreements made between parties are legally binding and must be obeyed, thus requiring the existence of laws that protect. Efforts made as a consumer are to have insight as a paylater user first, such as not providing sensitive personal data information, not clicking on links that contain malware, and always being conscious in doing something (Romoadhiyah et al., 2024). As a business actor must have a sense of responsibility and not be arbitrary with consumer personal data, business actors must have a strict security system. So as not to be easily tapped by third parties who misuse or spread consumers' personal data and help centres in e-commerce for services to consumers to be able to provide clarity and immediately block or disable consumer accounts temporarily.

If there is a leak of personal data for e-commerce users, as business actors have obligations and responsibilities so that there is no leakage of consumer personal data, according to the regulations that have been passed by business actors not to take deviant actions and the business actors concerned must provide information in writing for a maximum of 3x24 hours to users or consumers containing specific user personal data (Dhewa & Yossyafaa, 2023).

In fact, there are still many Indonesians who feel that there is no form of protection or legal responsibility for the sensitive personal data of Indonesian citizens and the implementation of these regulations which can still be said to

be inadequate. This can be said because there are still many cases of irresponsible people misusing someone's personal data without the knowledge of the owner of the personal data, which triggers Indonesian citizens to not have a sense of security in this country of Indonesia, which can show that the law on personal data there is a sense of insecurity and the absence of full supervision because the laws and regulations are still not fully implemented. The form of consumer personal data in various laws currently only clarifies the content of the personal data concerned to ensure legal certainty. Article 3 of the PDP Law regulates the standard of legal certainty, which is a kind of protection of rights against arbitrary actions.

Business actors must have a data protection policy to ensure consumer protection. This policy is important because it relates to the right to security, as stated in Article 4 letter (a) of Law Number 8 Year 1999 on Consumer protection. It guarantees the security of consumers' personal data and it is the responsibility of the service provider to keep this data confidential. Thus, consumers can know how their information is stored. Businesses are involved in the acquisition, management, storage, and deletion/processing of personal property. Privacy policies usually include restrictions arising from the interpretation of electronic contracts in standardised format for paylater transactions with service providers. Standard contract terms can be agreed upon by clicking on the licence visible in the initial service section.

Article 3 of the PK Law regulates the objectives of consumer protection, among others:

1. Increase consumer awareness, ability, and independence to protect themselves;
2. Raising the dignity of consumers by preventing them from the negative excesses of using goods and/or services;
3. Increase consumer empowerment in choosing to determine and claim their rights as consumers
4. Create a consumer protection system that contains elements of legal certainty and information disclosure and access to information;
5. Raising awareness of business actors about the importance of consumer protection so as to grow an honest and responsible attitude in business;

6. Improve the quality of goods and/or services that guarantee the continuity of the business of producing goods and/or services, health, comfort, security, and safety of consumers.

Then, Article 31 of Financial Services Authority Regulation Number 1 of 2019 concerning Financial Services Consumer Data Protection stipulates that consumer protection includes the use of confidentiality and security principles in maintaining customer data and information. Therefore, every activity involving such data must be approved and closely monitored by OJK. Article 74 paragraph (1) of Government Regulation Number 71/2019 on the Implementation of Electronic Systems and Transactions (PP PSTE) explains that privacy policy is a component of a certificate of reliability that aims to safeguard consumers' personal data. Every electronic system owner must have a certificate that proves the reliability of its operation. A certificate of trust is a type of certificate issued to service providers that allows them to conduct electronic transactions securely and reliably (Setiawan, 2014). This certificate serves as official documentation verifying that the implementation of electronic transactions has successfully gone through supervision and compliance assessment conducted by a reputable certification body. This signifies the commitment of electronic system providers who have gained the trust to conduct halal electronic transactions.

Thus, it is understood that Indonesia only applies certain legal restrictions to protect against unauthorised disclosure of personal data. Therefore, a comprehensive law is needed that can address all issues relating to the misuse of one's personal data. Since there is no specific law that regulates the legal protection of personal data separately, there is a lack of legal certainty and vulnerability. By guaranteeing consumer rights in terms of paid transactions, this is further complicated by the involvement of non- bank companies in the digital paylater registration process to collect personal data in NIK format.

Article 64 paragraphs 2 and 3 of Law No. 24 of 2013 on Population Administration stipulates that NIK is a unified identity used by the state for public services, which means the importance of NIK as a protected part of population management, as it relates to personal data privacy rights. In practice, NIK can be linked to money transfer services, such as payment registration processes and other public services. There is no explanation that

NIK is one of the public personal data of citizens that must be protected in Indonesia.

Personal data protection of financial information contained in payment services is a basic consumer information right. The increasing incidence of data breaches and unauthorised use of consumers' personal information highlights the growing importance of protecting consumers' personal data, as it often contains sensitive information (Denisa et al., 2023). To prevent the filtering and misuse of personal data in payment systems that fail to guarantee the privacy of consumers' financial information. Article 14 Paragraph 1 of the PP PSTE provides the legal basis for rules governing the protection of personal data. These standards must be adhered to by electronic system operators throughout the entire process, including data collection, management, deletion and destruction. Therefore, all operations conducted by service providers including consumers' personal data must be maintained in accordance with the principles of personal data protection.

The level of consumer data leakage is caused by the behaviour of consumers in making online transactions and loans, sending personal data such as ID cards, mobile phone numbers, credit and debit cards. And at the same time, it is also seen that the cause of data leakage by financial sector players who sell consumer data, by providing information to third parties so that hackers can hack someone's data easily, and other contributing factors also include software misconfiguration, social engineering fraud, repeated passwords, theft of items containing sensitive information, software vulnerabilities, and the use of default passwords.

Not only that, there are also main factors that cause leakage of one's personal data, namely, First, the factor of human error (human error), human errors that often occur are humans who are very easily tricked, such as those who volunteer to provide their personal data information to others to websites in the form of telephone numbers or applications that are not guaranteed security, without understanding the importance of personal data. Second, malware attacks where, they are also often careless or negligent when sending and receiving WA (Whatsapp) messages from unknown numbers, it is not uncommon for the contents of the messages obtained/received to be in the form of PDFs/website links that can be the entrance to malware. Malware is basically a programme designed to infiltrate and damage computer systems. Third,

social engineering, which uses psychological manipulation to collect sensitive data such as full names, passwords and so on through electronic media by posing as trusted parties. Phishing usually uses email/Whatsapp to trick its victims. The email or Whatsapp sent by the perpetrator may contain the name of a certain party and trick the victim into clicking on the link contained therein.

3.2 The Important Role of Paylater Consumers with Business Actors in Enforcing Personal Data Protection Law due to Personal Data Leakage

Liability for personal data leakage, whether caused by third-party hacking or intentional disclosure to a party third, it lies with companies operating in the e-commerce industry as custodians of personal data. Where the loss is not the business actor but the fintech service, it should be reminded that e-commerce services only provide buying and selling services and the transaction or money comes from consumers and fintech. This can also be mitigated by requiring information system providers to provide training for electronic system users. It is important not to share highly sensitive personal information with them and to be careful when categorising the information provided. Based on Article 30 Paragraph 1 of PP 71/2019 that network providers are obliged to take appropriate measures to safeguard the rights and interests of electronic system users, taking into account the peculiarities of electronic systems.

Paylater organisers mainly focus on resolving internal disputes and imposing administrative sanctions on those who breach the Paylater user agreement. This approach is used because of the relative ease of resolving default issues. The lender in a state of consciousness also knows the loss or risk that will be fully accepted. Obligations in an agreement or default can be intentional or unintentional, and fulfilling achievements is a condition in the contract. The fulfilment of the achievement refers to the performance of the obligations set out in the contract or the agreement of the parties for the fulfilment of the conditions specified in the contract. Therefore, if the parties fail to perform the obligations specified in the contract, the debtor may be deemed not to have fulfilled its performance, which is expressed in default. Depending on the type of growth performance of the Company, this performance may be delayed, unfulfilled or incomplete and completely inefficient, thus putting the digital-based fintech service provider in legal trouble, namely the risk of default, the only action that can be taken is to step in and help resolve it. There are ways that can be done if one party does not fulfil the conditions in the

contract, because both parties must fulfil the terms of the contract agreed upon. In the event of a breach of the terms of the contract, the aggrieved party has the option of initiating legal proceedings in a civil court under the GCPL. This action is expected to give good results, because offers more than just financial benefits that prioritise the interests of consumers and entrepreneurs.

There are two kinds of interests related to legal protection and lending rights, namely preventive legal protection and repressive legal protection. The purpose of preventive protection law is to proactively prevent problems or disputes from occurring by ensuring there is legal protection for electronic transactions supervised by Indonesian banks, with the aim of preventing offences. On the other hand, the purpose of preventive protection is to provide legal protection in dispute resolution, with the ultimate goal of providing legal protection due to differences in interests.

Article 1 of Minister of Finance Regulation Number 77 Year 2016 specifically regulates the rules regarding personal data of individuals in the context of money lending and technology-based money lending services, at point 39 of this Permenku expressly prohibits service providers from sharing user data and/or information to third parties. The parties are the main entities involved in everything. In this scenario, the restriction is lifted when the user electronically signs a contract that complies with legal requirements. The financial services authority, as the governing body of the financial services industry, expressly prohibits electronic loan providers and loan payment systems in paylater from sharing personal information.

Article 65 Paragraph 1 of UU PDP regulates 4 (four) types of prohibited acts (criminal offences), namely unlawful acts, obtaining/collecting, disclosing or using personal data that does not belong to them and acts of making false/falsifying personal data. Violation of this provision will be subject to criminal sanctions in the form of imprisonment or fines as stipulated in Article 67 Paragraph 2 of the PDP Law, namely imprisonment for a maximum of 4 (four) years and/or a maximum fine of 4 billion rupiah. Thus, the parties involved include legal entities that violate personal data protection laws as well as law enforcers or competent authorities responsible for enforcing these laws, so that legal certainty can be realised and consumer convenience in electronic transactions is maintained.

4. CONCLUSIONS

In order to protect the personal data of paylater users in e-commerce, it is important to know what legal measures are taken in common incidents. One such effort is to realise that agreements made between parties are legally binding and must be respected, so laws are needed to protect them. Then consumers must have insight as paylater users first, such as not providing sensitive personal data information, by not clicking on links that contain malware, changing account passwords and always being sober in doing something. Furthermore, business actors must have a sense of responsibility and not be arbitrary with consumers' personal data, business actors must have a strict security system so that it is not easily tapped by third parties. If there is a violation of personal data protection, the perpetrator may be subject to sanctions in accordance with applicable provisions as stipulated in Article 67 Paragraph 2 of the PDP Law.

REFERENCES

Ahdiat, A. (2023). *Maraknya Layanan Paylater yang Diketahui Responden (September 2023)*. https://databoks.katadata.co.id. https://databoks.katadata.co.id/datapublish/2023/10/25/8-layanan-paylater-terpopuler-di-indonesia-shopee-paylater-juara

Aulia, S. (2020). Pola Perilaku Konsumen Digital Dalam Memanfaatkan Aplikasi Dompet Digital. *Jurnal Komunikasi*, *12*(2), 311. https://doi.org/10.24912/jk.v12i2.9829

Berliana, E. (2023). *Analisis Dampak Penggunaan E-Wallet Terhadap Transaksi Masyarakat Dalam Perspektif Ekonomi Islam (Studi Kasus Desa Pekalongan Kec. Pekalongan Kab. Lampung Timur)*. IAIN Metro.

Denisa, A. P., Amirulloh, M., & Muchtar, H. N. (2023). Sertifikat Keandalan Privasi Sebagai Salah satu Bentuk Pelindungan Konsumen di Bidang Informasi dan Transaksi Elektronik. *Jurnal Rechtsvinding Media Pembianaan Hukum Nasional*, *12*(2), 167–184.

Dhewa, A. A., & Yossyafaa, H. (2023). Aspek Hukum Perlindungan Konsumen pada Transfer Data Pribadi oleh Korpporasi dalam Hukum Positif Indonesia. *Lontar Merah*, *6*(1), 619–629.

Fadhli, Z., Rahayu, S. W., & Gani, I. A. (2022). Perlindungan Data Pribadi Konsumen Pada Transaksi Paylater. *Jurnal Hukum Magnum Opus*, *5*(1), 119–132. https://doi.org/10.1177/1024529418816525

Manurung, R., & Rahardjo, A. K. (2019). *Sistem Informasi Akuntansi Peer to Peer Lending*. Yayasan Drestanta Pelita Indonesia.

Marzuki, P. M. (2009). *Penelitian Hukum*.

Muhamad, N. (2023). *Milenial dan Gen Z Mendominasi Pengguna Paylater di Indonesia*. Https://Databoks.Katadata.Co.Id. https://databoks.katadata.co.id/datapublish/2024/07/04/milenial-dan-gen-z-mendominasi-pengguna-paylater-di-indonesia

Putra, F. A., & Nugroho, L. D. (2021). Perlindungan Hukum Terhadap Penyalahgunaan Akun Dalam Transaksi Elektronik Melalui Traveloka. *Inicio Legis*, *2*(1), 86–107. https://doi.org/10.21107/il.v2i1.11081

Romadhona, S. (2022). *Paylater, Perangkap atau Peluang? Ini Kata Studi*. Universitas Muhammadiyah Sidoarjo.

Romoadhiyah, F. T., Hartati, S., & Widyastuti, T. V. (2024). *Perlindungan Hukum bagi Konsumen Penyalahgunaan Shopee Paylater oleh Pihak Ketiga*. Penerbit NEM.

Setiawan, A. B. (2014). Studi Standardisasi Sertifikat Elektronik dan Keandalan dalam Penyelenggaraan Sistem Transaksi Elektronik. *Buletin Pos Dan Telekomunikasi*, *12*(2), 119–134.

Suratman, & Dillah, P. (2013). *Metode Penelitian Hukum*. Alfabeta.

Tsani, S. (2024). Pengaruh Fitur Paylater, Spinjam dan Affiliate terhadap Minat Kasus Pengguna Shopee pada Mahasiswa FEBI UIN SATU Tulungagung. *Al-Kharaj: Jurnal Ekonomi, Keuangan & Bisnis Syariah*, *6*(1), 173–191. https://doi.org/10.47467/alkharaj.v6i1.160