Legal Protection Against Leakage of Traveloka Consumer Personal Data by the Company

Lunaraisah[1*], Adi Sulistiyono[2]

[1]Student Master of Law, Sebelas Maret University, Surakarta, 57126, Central Java, Indonesia.
[2]Teacher Master of Law, Sebelas Maret University, Surakarta, 57126, Central Java, Indonesia
*Corresponding Author:
Email: lunaraisahlr@gmail.com

Abstract.
The number of incidents of misuse of personal data for loan applications on the Paylater e-commerce platform is currently caused by the lack of a strict security system in digital companies in Indonesia. Currently, data leakage problems befall Traveloka consumers. Although some of them don't use the pay later feature in the app, they still find it difficult to get approval from banks due to having poor credit scores. This study aims to analyze legal protection efforts provided against misuse of consumer data on the Traveloka PayLater feature. The author uses normative legal research methods with a statutory approach and a conceptual approach analyzed through legal materials. Based on the results of the research, Traveloka as a service provider acts as a collector and manager of consumer data which is obliged to protect the data collected from the beginning until data deletion. Legal protection for consumers can be done both through internal legal protection and external legal protection, Internal legal protection can be done by considering the agreement between consumers and Traveloka companies and it is found that there is an exoneration clause in the agreement so that the agreement can be canceled. Meanwhile, external legal protection can be provided by sanctioning Traveloka as the collector and processor of consumer personal data following the provisions in Law Number 27 of 2022 concerning Personal Data Protection.

Keywords: *Legal Protection, Personal Data and Traveloka Pay Later.*

I. INTRODUCTION

The presence of the phenomenon of globalization has caused a significant influence on various sectors of human life, including technology and the Internet. Technology and the internet play a very important role in supporting various activities of human life so it has an impact on several sectors such as business or business industry. Furthermore, developments in the trade industry and financial industry in Indonesia are one of the impacts of this phenomenon, which resulted in the development of trade transactions and subsequently gave rise to an online trading system known as e-commerce. The growth of the trade sector is also accompanied by the progress of the financial sector. In e-commerce, sellers and buyers do not make transactions directly, therefore payments are made via bank transfer or using credit cards. But now, in addition to the payment methods via transfer and credit cards provided, some e-commerce businesses have also presented a payment feature without a credit card, known as the pay later feature or Pay later (Nanami, 2020). The emergence of the Paylater feature is the result of collaboration between e-commerce companies and peer-to-peer lending-based finance companies, while peer-to-peer lending itself is an information technology-based lending service that brings together lenders with *borrowers* in a container or company. The easier payment transactions using e-commerce must also be accompanied by increased protection of consumer data to prevent misuse of consumer data by irresponsible parties. Because based on the facts that occur, the presence of the pay later payment feature has opened up a new opportunity for irresponsible parties to hack consumer accounts. This is evidenced by the emergence of cases of misuse of Traveloka consumer data to make loans on Traveloka pay later.Traveloka shows the weak protection of consumer data by service providers (Sabiq, 2022).

Starting from the failure of the Twitter account owner @ridu when applying for a credit card to a bank, after being investigated, the cause was that Ridu's name was included in the Collectibility category 5 in the Bank Indonesia Financial Information Service System. He is in that category because he is considered delinquent in payment for more than 180 days. The transaction arrears themselves are reported by PT Caturnusa Sejahtera Finance, traveloka's partner in providing Traveloka pay later services. Ridu admitted

that he had never used this Traveloka PayLater service, Rindu became a koban because he was blacklisted for applying for financial institution credit. As a result, Rindu was rejected when applying for loans to official financial institutions, such as when applying for a credit card or home purchase installments (Nugroho, 2021).

A bad credit score makes it difficult for consumers to apply for loans at other financing services. A common theme in the case of Ridu, whose credit score nosedived for no apparent reason was that he did not sign up for the Traveloka pay later service facilitated by Caturnusa. Ridu only found out that his credit score was bad when he applied for a loan from a bank (Laucereno, 2021). Based on suggestions from previous studies that harmonization of regulations regarding personal data protection is needed, because often cases of personal data leakage in Indonesia end up without a complete resolution. One of the reasons that are often stated as the cause of incomplete cases of personal data leakage in Indonesia is the absence of comprehensive arrangements governing personal data protection. This is because there is no harmonization of arrangements among various government agencies. Often authorized institutions hesitate to apply sanctions for violations of personal rules because there is no clear mechanism and responsibility for personal data managers. This creates legal uncertainty and difficulty for the aggrieved party to bring claims. In this study, researchers will further examine legal protection against personal data leakage based on Law Number 27 of 2022 concerning Personal Data Protection. Departing from the case of data misuse experienced by Taveloka consumers, resulting in many consumers becoming victims and experiencing bad credit, if it is related to the provisions regarding the responsibility of the controller and processor of personal data, this case of misuse of consumer personal data should be dealt with strictly to cause a deterrent effect for the perpetrators and also the company as the controller and processor of personal data. So it requires companies to improve the security system in their applications so that they are not easily crossed by irresponsible parties, besides that the imposition of sanctions for violators will provide legal protection for consumers who are harmed in this case.

II. METHODS

This research uses normative research methods The reason for using normative research in this study is because, in the problems studied, the author will identify regulations related to legal protection against legal protection for misuse of consumer data on the Traveloka pay later feature (Prasetyo, 2019). This research uses a statutory approach and a conceptual approach (used in this study include primary legal sources, which come from various legal regulations governing personal data protection. In addition, this research also utilizes secondary legal sources such as books, journals, and scientific articles on personal data protection (Tan, 2021).

The technical collection of legal sources used in this study is a literature study (*Library Research*) carried out by collecting primary and secondary materials related to legal issues contained in this study, then it will be analyzed based on theories that can be used as guidelines (Burhan Ashofa, 2004). Legal material analysis techniques are carried out deductively. The material obtained from the literature study will be analyzed based on related problems, then alternative solutions are given. Furthermore, the data is analyzed by looking at the legal rules that should apply then conclusions are drawn using a deductive approach method by taking into account the concept of the legal protection of consumer personal data (Benuf et al., 2019).

III. RESULT AND DISCUSSION

In its development, the use of pay later as a payment method does not always bring convenience, along with the increasing number of pay later users, it also opens a gap for irresponsible parties to hack e-commerce user accounts that activate the pay later feature, there are even some users who do not activate the pay later feature but get billed on their accounts for the use of pay later used by parties who do not Responsible. Looking at these various cases, it can be concluded that the Traveloka company is still weak in terms of consumer data security protection. Therefore, it must be further analyzed regarding the agreement made by the service provider and the consumer, so that it can be seen the legal relationship that arises between the two, and later an answer will be obtained regarding the party who must be responsible for the

misuse of Traveloka consumer data. Previously, in terms of legal relations that exist in the pay later service, it involved three parties, including account users, namely Traveloka account owners, namely those who are interested in buying services on the Traveloka application, if the account user or buyer buys services with pay later facilities, then he will act as a debtor. Paylater service provider application platform, which is a company in the field of e-commerce that offers a variety of services. Fintech, in this case as a lender provider, namely fintech companies in collaboration with Traveloka companies. Plays a role in distributing loan funds and will also collect the loan. This fintech also determines how big the facility and various other lending and borrowing conditions (Fitriyani Pakpahan et al., 2020).

Referring to the position of the Traveloka company as a pay later service provider, lending through pay later services was born based on a partnership agreement between Traveloka companies and peer-to-peer lending-based online loan companies. A financial technology company (peer-to-peer lending) is a non-bank financial institution that disburses loans online and is under the supervision of the Financial Services Authority as regulated in the Financial Services Authority Regulation Number 10/POJK.05/2022 concerning Information Technology-Based Joint Funding Services. In peer-to-peer lending companies, investor funds that have been raised are then managed by peer-to-peer lending companies where they join and then channeled back to prospective borrowers who need funds. In the partnership cooperation agreement between e-commerce companies and financial technology-based online loan companies, the investor funds are then distributed to pay later service users. There is traveloka, the presence of pay-later services or features is first based on a partnership cooperation agreement with PT. Pasar Dana Lending and PT. Caturnusa Prosperous Finance. The partnership agreement in question is PT. Pasar Dana Lending and PT. Caturnusa Sejahtera Finance is the lender, while Traveloka is the loan channel. The existence of a guarantee of legal protection for pay-later service users provides an obligation for Traveloka companies as pay-later feature providers based on the Personal Data Protection Law as an electronic system operator› to be responsible for the operation of electronic systems, especially for the protection of customer personal data which is A thing that must be a top priority. The goal is none other than to prevent problems regarding the misuse of service users' personal data information which leads to losses. This must be done, especially by service providers and peer-to-peer lending companies that work together considering the personal data of service users uploaded when registering for pay later *which must* be kept confidential as a form of security in transactions through the Traveloka application with payments using the pay later feature. The legal relationship between the borrower and the borrower and the lender is the existence of a civil relationship where both are said to be parties to an information technology-based loan agreement (Ronaldo Siahaan, 2022).

The obligation to include a privacy policy by service providers is useful to protect consumers because it involves the right to consumer security. In general, the privacy policy is contained in the terms and conditions which are the result of the interpretation of electronic contracts made in standard form by service providers. In pay later transactions, standard contract requirements can be achieved through *click-wrap* licenses that appear when the service provider is first used. Usually, users are asked about their willingness to accept the standard contract through the alternative "I accept" or "I don't accept" so that service providers only need one or two clicks to get consumer approval. This consent is correlated with an electronic signature which is the identity of the sender of data or information and aims to assure the party sending the data that the person sending the data is indeed sourced from the person who should (Fadhli, 2022). According to M.Isnaeni, Internal legal protection explains that the agreement is carried out by Traveloka and the account owner. The agreement made by the parties creates a legal relationship between Traveloka and the account owner that binds each other. Making an agreement made by Traveloka in the terms and conditions must pay attention to the terms of validity of the agreement contained in Article 1320 of the Civil Code (Isnaeni, 2016).

Terms and conditions made by Traveloka regarding what must be done by the account owner to the account that has been registered by filling in personal data. The account owner may not allow other parties to use their account or transfer to other parties to make transactions if there is no permission from Traveloka.

The terms and conditions made by Traveloka as the account owner are fully responsible and explain that Traveloka is not responsible for any loss or damage that occurs to the account owner due to misuse of the misused account based on Law Number 27 of 2022 concerning Personal Data Protection. The problem of losses arising from cases of account breaches as still charged to service users is a waiver of service provider responsibility which has generally been determined unilaterally in the electronic agreement that has been agreed upon at the beginning of account registration. As with Traveloka, it has been determined in the terms and conditions of use of the Traveloka application which contains clauses that:

a) If the user no longer has control over the user's account, the user must immediately notify Traveloka (for example, without limitation: the user's account is hacked in any way or the user's phone is stolen) so that Traveloka can temporarily block and/or deactivate the user's account as necessary. Please note that the user is responsible for the use of the user account and may be responsible for the user account even if the user account is misused by another party.
b) Users shall maintain the security and confidentiality of user account passwords and identifications that raveloka provides to users. In the event of disclosure of the user's password, in any case, that causes the unauthorized user to account or user identity, orders received for such unauthorized use will still be considered valid orders and Traveloka will process such orders. The user hereby declares that Traveloka is not responsible for any loss or damage arising from the misuse of the user's account.

Such clauses are referred to as exoneration clauses whose function is to limit or even remove the responsibility that should be imposed on the producer or business actor. This kind of clause is certainly detrimental to consumers because consumers are forced to comply with rules that harm consumers and benefit business actors, Therefore, it can be said that the provisions made by Traveloka which state that Traveloka is not responsible and users will not prosecute traveloka for any damage and loss arising from hacking actions carried out based on Law Number 27 of 2022 concerning Personal Data Protection to user accounts are declared null and void. Traveloka automatically becomes a party that can be charged with responsibility related to the misuse of users' data (Rohaya, 2018).

External legal protection states that in terms of protecting account owners, a law has been issued to prevent imbalances in buying and selling transactions through technology in the terms and conditions made by Traveloka if there is account misuse carried out based on Law Number 27 of 2022 concerning Personal Data Protection to the detriment of traveloka account owners (Tasya,2022). The account itself has an understanding that contains data belonging to a person such as a name, password data, and personal data or someone's identity contained in cyberspace, and the account in it has contained certain personal data such as NIK, date of birth, residence, credit card number, and the data must be maintained, maintained the truth that has been identified in the electronic system. The protection of personal data contained in the account must be kept confidential to avoid the threat of crime in cyberspace such as misuse of accounts by irresponsible parties (Agus, 2019). Article 65 of the Personal Data Protection Law mentions the prohibition on the use of personal data, According to Article 65 paragraph (1), any person is prohibited by unauthorized means from obtaining or collecting personal data that does not belong to him for the benefit of himself or others which may result in the loss of the personal data subject. Then, Article 65 paragraph (2) prohibits any person from unlawfully disclosing personal data that does not belong to him. Finally, Article 65 paragraph (3) confirms that unauthorized use of personal data that does not apply to the person is prohibited.In this context, Traveloka is responsible as a processor and manager of consumers' data. In carrying out data processing, Traveloka must comply with the terms and conditions stipulated in Law Number 27 of 2022 concerning Personal Data Protection (Yulia, Neta 2022).

Personal data controllers carried out by 2 or more personal data controllers must meet the minimum requirements specified in Article 18 paragraph (2) which include there is an agreement between the personal data controllers containing roles, responsibilities, and relationships between personal data controllers, there are interrelated purposes and ways of processing personal data that are determined jointly and there is a jointly appointed contact person. Regarding the obligations of the personal data controller described in According to Article 20 of the Personal Data Protection Law, personal data managers must have a clear legal basis for processing personal data. The basis for such processing may be based on the explicit consent of the

personal data subject for one or more specific purposes described by the personal data manager to the personal data subject, the fulfillment of contractual obligations if the personal data subject is a party, or to fulfill the personal data subject's requests in carrying out his role and the fulfillment of the personal data manager's legal obligations by applicable laws and regulations.

In an incident that befalls a Traveloka customer, Traveloka as the regulator of the customer's data should prevent unauthorized access to personal data by Article 39 of the Personal Data Protection Law. Prevention efforts must be carried out with a reliable, secure, and responsible security system for personal data processed or processed electronically. If the security of personal information is compromised, the personal information regulatory body shall immediately notify the user of the personal information and the relevant institution in writing within three times twenty-four hours. The written notification shall include the personal information leaked, the time and method of disclosure of the personal information, and the recovery and handling measures taken by the personal information regulatory body by Article 46 of the Law on Personal Information Protection. Article 47 stipulates that personal information regulatory bodies are responsible for the processing of personal information and must demonstrate responsibility for failures to protect personal information.Based on the philosophical foundation of the concept of personal rights and supervision of personal information protection, it is necessary to have a personal data protection supervisory body. The purpose of establishing the Personal Data Protection Supervisory Agency is to ensure the security of electronic systems related to the management of personal information in the company by the standards set in the rule of law. However, even though the Personal Data Protection Law has been enacted, the government has still not established a Personal Data Protection Agency (Nurmalasari, 2021).

The establishment of a personal data protection supervisory agency is important to do because several arguments underlie the importance of forming a personal data supervisory agency, namely ensuring that personal data protection rules are implemented Personal data is the right of everyone protected by the constitution Personal data protection is not intended to protect people's data alone, but also to provide guarantees that a person's basic rights and freedoms to data it remains protected. Personal data protection intends to ensure that these rights and freedoms are not violated by any other person, institution, or institution without rights by the provisions of laws and regulations. However, based on Article 58 of the Personal Data Protection Law, the government does not make this institution independent, because it places this institution directly under the President so that there will be potential for tug-of-war or abuse for political interests or rulers, at the end of the institution formed will later become a government institution that is equivalent to other government institutions, then the question is whether it is possible for a government institution sanctioning other government institutions (Muhtada & Diniyanto, 2021). Given that the birth of independent state institutions is due to public distrust in the performance of existing institutions in handling various problems that arise, in the case of data leakage that has been rife throughout this year, it is still handled by the Ministry of Communication and Information Technology but many cases of data leakage are then not resolved properly, because there is no special institution that handles it, Therefore, the data protection institution should later be used as an independent state institution that will eventually be able to fill the void in the role of pre-existing institutions (Suryono,2021). Therefore, the placement of personal data protection institutions under the President does not provide independence to these institutions to carry out maximum supervision. Therefore, Indonesia in establishing a personal data protection institution needs to reflect on the establishment of personal data protection institutions in other countries

IV. CONCLUSION

Traveloka as a service provider acts as a collector and manager of consumer data that is obliged to protect the data collected from the time the data is collected until the data is destroyed. However, in its implementation, Traveloka has failed to protect consumer data which resulted in consumers experiencing losses because their data is used to make Traveloka pay later loans, so there is a need for legal protection for consumers, either in the form of internal legal protection or external legal protection. Internal legal protection is carried out by looking at the agreement agreed between consumers and Traveloka companies and finding

that there is an exoneration clause in the agreement, because it violates the responsibility of Traveloka, in the event of misuse of consumer data, resulting in the agreement can be null and void. Meanwhile, external legal protection is carried out by sanctioning Traveloka as the collector and processor of consumer personal data by the provisions in Law Number 27 of 2022 concerning Personal Data Protection This research contributes to solving the problem of legal protection for Traveloka consumers for the actions of service providers, in addition to providing input to service providers that it is necessary to implement consumer data protection efforts starting from collection to deletion of data as described in Law Number 27 of 2022 concerning Personal Data Protection so that consumer data remains safe and not misused by irresponsible parties.

V. ACKNOWLEDGMENTS

We would like to express our gratitude to Prof. Adi Sulistiyono. S.H., M.H. as the supervisor who has provided advice, guidance, and direction as well as during this research. In addition, we would like to thank the Master of Law Study Program, at Sebelas Maret University for supporting this research.

REFERENCES

[1] Agus Sudibyo.(2019). *Jagat Digital : Pembebasan dan Penguasaan*. Jakarta: Gramedia Pustaka Utama.

[2] Benuf, K., Mahmudah, S., & Priyono, E. A. (2019). Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology Di Indonesia. ***Refleksi Hukum: Jurnal Ilmu Hukum***, *3*(2), 145–160.

[3] Burhan Ashofa. (2004). *Metode Penelitian Hukum*. Yogyakarta:PT.Rineka Cipta.

[4] Fadhli, Z., Rahayu, S. W., & Gani, I. A. (2022).Perlindungan Data Pribadi Konsumen Pada Transaksi Paylater. ***Jurnal Hukum Magnum Opus***,*5*(1), 120.

[5] Fitriyani Pakpahan, E., Jessica, J., Winar, C., & Andriaman, A.(2020).Peran Otoritas Jasa Keuangan (OJK) dalam Mengawasi Maraknya Pelayanan Financial Technology (Fintech) di Indonesia. ***Udayana Master Law Journal*** , *9*(3), 559.

[6] Isnaeni, M. (2016).*Pengantar Hukum Jaminan Kebendaan*. Surabaya: Revka Petra Media.

[7] Laucereno, S. F. (2021). accessed from *Masalah Paylater Traveloka Diretas Orang Lain Sejak 2019 BelumTerselesaikan*.https://inside.kompas.com/surat-pembaca/read/61204/Masalah-Paylater-Traveloka-Diretas-Orang-Lain-Sejak-2019-Belum-Terselesaikan, accessed on April 02, 2023 at 10.30 WIB

[8] Marzuki, Peter Mahmud. (2017). *Penelitian Hukum*. Jakarta: Prenada Media Group.

[9] Muhtada, D., & Diniyanto, A. (2021). Penataan Regulasi di Indonesia Melalui Lembaga Independen. ***Pandecta: Research Law Journal***, 16(2), 280.

[10] Nanami Satyanegara, Priyono, J., & Paulus, D. H. (2020). Perlindungan Data Pribadi Di Indonesia Dalam Rangka Perdagangan Elektronik (E-Commerce). ***Diponegoro Law Journal,*** *9*(2), 435

[11] Nugroho,W.(2021), accessed from https://infokomputer.grid.id/read/122666006/betapa-tidak-berdayanya-konsumen-di-kasus-traveloka-paylater. *Info Komputer*. accessed on April 02, 2023 at 11.00 WIB

[12] Nurmalasari.(2020).Urgensi Pengesahan Rancangan Undang-Undang Perlindungan Data Pribadi Demi Mewujudkan Kepastian Hukum. ***Paper Knowledge*** . *Toward a Media History of Documents*, *3*(2), 6.

[13] Prasetyo Teguh.(2019). *Penelitian Hukum Suatu Prespektif Teori Keadilan Bermartabat*. Bandung: Nusa Media.

[14] Rohaya, N. (2018).Pelarangan Penggunaan Klausula Baku Yang Mengandung Klausula Eksonerasi Dalam Perlindungan Konsumen. ***Jurnal Hukum Replik***, *6*(1), 23.

[15] Ronaldo, Siahaan. (2022). Makna di Balik Iklan Traveloka PayLater "Baru Dari Traveloka PayLater!" . ***Journal of Advertising and Visual Communication***, *3*(2), 127–138.

[16] Sabiq, F.(2022). Paylater di Tinjau dari Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Fatwa DSN MUI No: 117/DSN-MUI/II/2018. ***El-Hayah,*** *7(*1), 8

[17] Safiranita Raml,Tasya,et.al. (2022). The Role of E-Commerce in Escalation of Digital Economy in The New Normal Era Based on Law Number 27 of 2022 Concerning Personal Data Protection.***Journal De Jure*** **.**22(4),444

[18] Suryono,Ryan,et.al.(2021).Detection of Fintech P2P Lending Issues in indonesia***.Cellpres Journal***,7(4),5

[19] Yulia,Neta,et.al.(2022).The Urgency of Independent Supervisory Authority Towards Indonesia's Personal Data Protection.***Constitutionale,*** 3(1),24