Jurnal Ilmu Hukum Tambun Bungai
Vol. 1, No. 1, June 2026, 125-150
P-ISSN: 2502-9541 E-ISSN: 2685-9386
Published by Sekolah Tinggi Ilmu Hukum Tambun Bungai Palangka Raya

Between Efficiency And Risk: Data Security In Digital Transportation and The Legal Liability of Platform Providers

Siti Mariyam[1*], Mahmuda Pancawisma Febriharini[2], Krismiyarsi[3], Hadi Karyono[4]

[1*] Universitas 17 Agustus 1945 Semarang
Jl. Pawiyitan Luhur, Bendan Dhuwur, Kota Semarang, Jawa Tengah, Indonesia
sitimariyam@untagsmg.ac.id

[2] Universitas 17 Agustus 1945 Semarang
Jl. Pawiyitan Luhur, Bendan Dhuwur, Kota Semarang, Jawa Tengah
mahmuda-pancawisma@untagsmg.ac.id

[3] Universitas 17 Agustus 1945 Semarang
Jl. Pawiyitan Luhur, Bendan Dhuwur, Kota Semarang, Jawa Tengah
krismiyarsi@untagsmg.ac.id

[4] Universitas 17 Agustus 1945 Semarang
Jl. Pawiyitan Luhur, Bendan Dhuwur, Kota Semarang, Jawa Tengah
hadi-karyono@untagsmg.ac.id

Submitted	: 2026-04-23	Accepted	: 2026-05-22
Revision	: 2026-04-30	Publish	: 2026-06-03

Abstract: *The era of digitalization has revolutionized the transportation sector, both air and land, by bringing operational service efficiency and transaction practicality for consumers. However, this massive digital transformation poses serious challenges regarding cybersecurity vulnerabilities and the protection of users' personal data privacy. This study aims to examine the legal protection of digital personal data of ride-hailing users in Indonesia and to analyze the responsibility of application provider companies for potential data protection failures. Through a normative legal approach, the study indicates that legal protection for consumers' digital privacy remains weak. This weakness is driven by specific regulatory gaps, the implementation of standard clauses that disadvantage consumers by shifting liability, and the storage of data outside Indonesia's legal jurisdiction which complicates oversight. Furthermore, companies often claim to be merely technology platform providers, effectively positioning themselves as having no direct responsibility for consumer losses, including the potential misuse of data by third parties such as driver-partners. In conclusion, specific regulations and comprehensive legal mechanisms are urgently needed to effectively ensure the protection of users' privacy rights in the digital era.*

Keywords *: Legal Protection, Personal Data, Digital Transportation, Corporate Liability, Digital Privacy*

Introduction

The era of technological disruption has fundamentally revolutionized the transportation sector, shifting conventional paradigms toward integrated digital systems. This transformation promises massive operational efficiency; in the aviation sector, the use of artificial intelligence-based navigation systems and smart airports has drastically improved the efficiency of airport navigation and services. In the realm of land transportation, the sharing economy model promoted by online transportation services (ride-hailing) has also transformed the landscape of urban mobility, making it much faster, more practical, and more efficient. However, behind the glorification of this efficiency, this digital transportation architecture harbors a paradox of serious vulnerabilities, particularly related to cybersecurity and the protection of user data privacy. Increased reliance on electronic systems forces consumers to surrender their personal data sovereignty as an absolute prerequisite for accessing services.[1]

Constitutionally, the existence and protection of the right to privacy in Indonesia has been expressly guaranteed in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia. This fundamental regulation is then operationalized through a hierarchy of sectoral regulations, starting from Law Number 8 of 1999 concerning Consumer Protection (PK Law), Law Number 11 of 2008 which has been amended by Law Number 1 of 2024 concerning Electronic Information and Transactions (ITE Law), to the latest lex specialis instrument, namely Law Number 27 of 2022 concerning Personal Data Protection (PDP Law)[2]. These regulations cumulatively require every electronic system organizer to maintain confidentiality and system reliability, and prohibit the dissemination of data without the explicit consent of the data subject.

In practice, electronic system providers (applicators) aggregate digital user profiles—including names, identities, precise addresses, geolocation travel records, and financial data—and then store them in giant databases (Big Data). This personal data, which is intrinsically an extension of human rights, has extremely high commercial value, placing consumer privacy at

[1] G. Y. Pratama, Suradi, dan Aminah, "Perlindungan Hukum Terhadap Data Pribadi Pengguna Jasa Transportasi Online Dari Tindakan Penyalahgunaan Pihak Penyedia Jasa Berdasarkan Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen," *Diponegoro Law Journal* 5, no. 3 (2016): 4-5.

a premium.[2] The threat of data breaches stems not only from external cyberattacks such as hacking or ransomware infiltration of network infrastructure, but also from the potential for internal exploitation. User profiles can be easily accessed by third parties (driver-partners) and are highly vulnerable to commercial and criminal misuse outside the operational boundaries of transportation services.

This legal gap is further exacerbated by the applicator's business model, which hides behind its "technology platform provider" status, which is used as a legal argument to refuse to fully accept the responsibilities of public transportation operators. Applicators argue that drivers are "partners" (not employees), thus deeming the company to be vicarious liability for driver negligence. Furthermore, applicator privacy policies often allow the transfer and processing of consumer data to servers outside of Indonesian jurisdiction without adequate oversight. These cross-jurisdictional obstacles make law enforcement and consumer litigation efforts in the event of data protection failures extremely complex and run into international bureaucratic hurdles.[3]

The complexity of this issue is further compounded when it is confronted with the construction of positive legal accountability in Indonesia. Jurisprudentially and regulatoryly, app providers often seek refuge behind the argument that their business entities are purely "technology platform companies," not public transportation companies. This legal narrative is systematically used to distort employment relations into mere "partnerships," which in turn serves as a pretext for app providers to escape vicarious liability for negligent or unlawful acts committed by their drivers.[4] This systematic effort to avoid responsibility is further legitimized through the insertion of exoneration clauses in standard contracts on application privacy policies, where the application provider releases its liability for data leaks by third parties.

Academic discourse on consumer protection in the online transportation ecosystem has been extensively explored by various previous literature. The majority of research focuses on the physical protection and safety of passengers and the legal dilemma of road

[2] Sinta Dewi Rosadi, "Konsep Perlindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan Cloud Computing di Indonesia," *Yustisia Jurnal Hukum* 5, no. 1 (2016): 23-25.

[3] E. Yolanda dan R. R. Hutabarat, "Urgensi Lembaga Pelindungan Data Pribadi di Indonesia Berdasarkan Asas Hukum Responsif," *Syntax Literate: Jurnal Ilmiah Indonesia* 8, no. 6 (2023): 4176.

[4] Janus Sidabalok, *Hukum Perlindungan Konsumen di Indonesia* (Bandung: Citra Aditya Bakti, 2014), hlm. 58-60.

transportation operational permits faced by app-based business models. Furthermore, legal debates often center on employment status, with app providers positioning drivers purely as "partners" to avoid the burden of obligations stipulated in national labor laws. In the context of privacy, research conducted by Yunas and Nasution (2023) specifically highlights that Gojek consumers' personal data protection remains vulnerabilities. Drivers' free access to users' addresses and phone numbers has been shown to have the potential to trigger abuse, where driver-partners can use this data to terrorize or threaten consumers' privacy.[5]

However, these studies still leave a significant research gap. Previous studies have not comprehensively examined the limits of applicator liability from the perspective of the intersection of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) and contract law, which prohibits the inclusion of exoneration clauses in electronic transactions. In practice, applicators tend to use standard contracts containing unilateral exoneration clauses to escape legal action in the event of data leaks or exploitation by third parties. This transfer of responsibility constitutes a denial of obligations as stipulated in Article 18 of Law Number 8 of 1999 concerning Consumer Protection, which expressly prohibits business actors from including standard clauses intended to shift their responsibilities.[6]

Based on this gap, the novelty of this research rests on the construction of an analysis of the strict liability of online transportation applicators in their jurisdictional capacity as "Data Controllers." This paper strongly argues that data protection obligations—mandated by law—cannot simply be delegated or waived through standard unilateral agreement clauses, especially when procedural failures, hacking, or data exploitation by partners in the field occur.[7] In the digital data protection regime, Personal Data Controllers bear full responsibility from data collection to destruction. Therefore, this research aims to reformulate a comprehensive form of legal protection, while simultaneously demanding a fair legal accountability design for applicators amidst the current massive flow of digital disruption.

[5] Hesty Ananta Yunas dan Muhammad Irwan Padli Nasution, "Perlindungan Hukum Terhadap Privasi Data Pribadi Konsumen Pengguna Gojek di Indonesia," *SAMMAJIVA: Jurnal Penelitian Bisnis dan Manajemen* 1, no. 3 (2023): 70.

[6] Ahmadi Miru dan Sutarman Yodo, *Hukum Perlindungan Konsumen* (Jakarta: Rajawali Pers, 2015), hlm. 85.

[7] Edmon Makarim, *Kompilasi Hukum Telematika* (Jakarta: Rajawali Pers, 2004), hlm. 120-122.

This legal anomaly creates a legal vacuum that positions consumers at the weakest point in the hierarchy. Legal challenges are further exacerbated by the absence of strict jurisdictional boundaries, which allows app providers to store, process, and disseminate citizens' private data to servers located outside Indonesian jurisdiction (ex-territorial), complicating oversight and litigation mechanisms. Therefore, an in-depth, analytical, and systematic study of the legal protection of online transportation users' digital personal data is urgent. This paper specifically examines the legal construction of privacy protection in the digital economy era and formulates parameters for the absolute accountability of electronic system providers to ensure legal certainty and protect consumers' fundamental rights.

Based on the background outlined above, a significant gap is evident between the rapid pace of digital transportation innovation and current legal protection instruments. Digital transformation requires consumers to submit their personal data, which is then collected and stored in Big Data owned by application providers (applicators). However, this digital ecosystem presents serious security vulnerabilities; this private data can be easily accessed by third parties (such as driver-partners) and has significant potential for misuse outside the context of transportation services.

This situation is increasingly concerning considering that the applicator often shifts responsibility through the use of standard clauses containing exoneration clauses in their privacy policies, and hides behind the argument that the legal relationship with drivers and users is limited to a partnership relationship. Departing from the gap between legal regulations and empirical facts, this study focuses on examining two main issues, namely what form of legal protection for privacy and digital personal data of transportation service users in the digital era, especially in online transportation, based on positive law in force in Indonesia, and what form of legal accountability the electronic system organizer (applicator) and third parties in the event of misuse or failure in protecting user personal data.

This research employs a normative legal research method. This method was chosen based on the study's characteristics, which emphasize the analysis of legal principles, the synchronization of legal rules, and an in-depth review of laws and regulations governing personal data protection and the accountability of digital transportation applicators. To sharpen the analytical tool, this study employs two main approaches: a statutory approach to

examine positive legal products, and a conceptual approach to explore evolving legal views and doctrines regarding the legal standing of consumers and electronic system providers.[8]

The data sources in this study rely exclusively on secondary data, which are further classified into primary and secondary legal materials. Primary legal materials are binding authoritative regulations, including the 1945 Constitution of the Republic of Indonesia, Law Number 8 of 1999 concerning Consumer Protection, and Law Number 22 of 2009 concerning Road Traffic and Transportation. Furthermore, regulations in the cyber sector are also reviewed, including the Electronic Information and Transactions Law and its amendments, Government Regulation Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions, Regulation of the Minister of Communication and Informatics Number 20 of 2016, and the most recent crucial regulation, Law Number 27 of 2022 concerning Personal Data Protection. Meanwhile, secondary legal materials were obtained through literature searches such as law books, scientific journal articles, research reports, and other academic documents that support and provide explanations for the primary legal materials.

The data collection technique applied in this research is library research. This step is carried out systematically by inventorying, reading, recording, and reviewing various legal regulations, doctrines, and standard clauses contained in the privacy policies of online transportation applicators. All legal materials that have been constructed are then analyzed using juridical-qualitative analysis techniques. The data is described descriptively to address issues regarding the construction of digital privacy protection and test the validity of third-party waivers of liability, so that ultimately a comprehensive and proportional legal prescription can be formulated for all parties involved.[9]

Legal Protection for the Privacy and Personal Data of Online Transportation Users Under Indonesian Positive Law

Protection of personal data is now universally recognized as an integral part of human rights. At the international level, the right to privacy is firmly guaranteed through Article 12 of

[8] Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Kencana, 2017), hlm. 133-136.

[9] Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat* (Jakarta: Rajawali Pers, 2015), hlm. 13-15.

the Universal Declaration of Human Rights (UDHR), which prohibits arbitrary interference with a person's privacy, and is reinforced by Article 17 of the International Covenant on Civil and Political Rights. Within the national legal hierarchy, the fundamental basis for this protection is precisely stated in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which mandates the right of every person to protection of their personal life, family, honor, dignity, and property. This constitutional construction affirms that the state bears an absolute obligation to be present to protect the sovereignty of its citizens' private data, including in electronic transactions in the digital space.

Conceptually, privacy as a human right encompasses at least three main elements: personal privacy (the right to be left alone), personal data privacy (the right to control information related to oneself), and communication privacy. In the operational context of online transportation, personal data privacy occupies a crucial position. Consumers are required to submit primary data in the form of name, email, and telephone number, as well as secondary data such as address and travel route history, which are ultimately recorded permanently in the app company's Big Data. This information is essentially a digital dossier with high economic value. As stated by Ann Covoukian, privacy is essentially a person's right to have full control over their personal information and autonomously determine the extent to which that information may be collected and used by others.

In Indonesia, the legal framework governing digital privacy protection was initially spread across several sectoral instruments. Law No. 11 of 2008 concerning Electronic Information and Transactions (UU ITE), as amended by Law No. 1 of 2024, specifically Article 26, stipulates that the use and dissemination of personal data in electronic systems may only be carried out with the consent of the data owner. This provision is reinforced by Article 21 of Regulation of the Minister of Communication and Informatics No. 20 of 2016, which requires explicit consent. Furthermore, Article 15 of Government Regulation No. 82 of 2012 concerning the Implementation of Electronic Systems and Transactions (PP PSTE) regulates mitigation measures, whereby system administrators are required to provide written notification to data owners in the event of a failure in personal data protection.

In its application in the online transportation ecosystem, this consent provision is often distorted. When users agree to the privacy policy when registering for an application, that

agreement is legally binding only between the user and the application provider as the system organizer, not with third parties such as driver partners or advertisers. However, in reality, drivers can easily access crucial data such as phone numbers and user geolocation, leading to exploitation beyond the service's purpose without specific consent from consumers. When data misuse by drivers occurs, the mandatory reporting provisions (data breach notification) mandated by Article 15 of the PP PSTE are rarely implemented transparently by the application provider, leaving consumers vulnerable and unaware that their data has been compromised.[10]

In addition to the cyber regime, online transportation users also act as service buyers, and are therefore subject mutatis mutandis to Law Number 8 of 1999 concerning Consumer Protection (UU PK). This fundamental right is guaranteed in the PK Law, which stipulates that consumer rights include, among other things, the right to comfort, security, and safety in consuming goods and/or services. In the digital era, the term "security" is no longer limited to physical safety on the road, but extends to the security of users' digital identities and data. Furthermore, Article 19 paragraphs (1) and (2) of the PK Law require business actors to be responsible for providing compensation for losses experienced by consumers. To prevent evasion of responsibility, Article 18 of the PK Law strictly prohibits business actors from including standard clauses stating the transfer of business actor responsibility.

However, the implementation of the Consumer Protection Law in practice faces structural obstacles due to the business practices of applicators. Rather than complying with Article 18 of the Consumer Protection Law, applicator companies have inserted exoneration clauses into their privacy policies, unilaterally declaring themselves not responsible for the actions of service providers (drivers), and even asking consumers to release applicators from any claims for compensation if their data is misused. This situation demonstrates a violation of the legal principles of consumer protection, where applicators use standard digital take-it-or-leave-it contracts to unilaterally absolve themselves of their legal obligations.

As a form of harmonization and strengthening of more responsive laws, Indonesia now has Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). This lex specialis regulation unifies previously scattered regulations and demands more rigid security standards

[10] inta Dewi Rosadi, "Konsep Perlindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan Cloud Computing di Indonesia," *Yustisia Jurnal Hukum* 5, no. 1 (2016): 26.

for "Personal Data Controllers," essentially approaching the strict regime of the General Data Protection Regulation (GDPR) in the European Union. Under the PDP Law, app providers are absolutely classified as Personal Data Controllers, bearing full responsibility for data collection, processing, and deletion. While this instrument is very comprehensive on paper, actual protection remains very weak in practice. This is due to app providers' policies that frequently store and transfer user data to servers outside of Indonesian jurisdiction. Effective enforcement of administrative and criminal sanctions under the PDP Law is extremely difficult due to clashes between national jurisdictions and information asymmetries between consumers and giant tech corporations.[11]

The main weakness of this legal protection stems from the operational vulnerabilities of the apps themselves. Driver-partners can easily access the geolocation of users' homes, workplaces, and phone numbers, often connected to instant messaging apps (such as WhatsApp). This open access opens up a massive loophole for data to be exploited beyond the original purpose of the transportation service without the data owner's knowledge. This weakness is further compounded by the app's practice of storing, processing, and transferring users' personal data to servers located outside of Indonesian legal jurisdiction. This creates a serious jurisdictional dilemma, given that the process of law enforcement and monitoring cross-border data traffic is highly bureaucratic and complex, often paralyzing constitutional data protection rights when confronted by global tech giants.[12]

Legal Responsibility of Electronic System Organizers (Applicators) and Third Parties for Misuse or Failure to Protect User Personal Data

In examining the construction of legal responsibility in the online transportation ecosystem, the most fundamental legal obstacle stems from the unclear legal status of the applicator entity. App providers consistently position themselves exclusively as "technology-based companies" that only provide a connecting platform, and refuse to be classified as public transportation companies. The logical consequence of this claim is the design of the

[11] Fikri dan Rusdiana, "Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Positif Indonesia," *Ganesha Law Review* 5, no. 1 (2023): 51.

[12] Edmon Makarim, *Tanggung Jawab Penyelenggara Sistem Elektronik* (Jakarta: Rajawali Pers, 2010), hlm. 102-105.

working relationship between applicators and drivers that is not based on an employment relationship (employer-worker), but rather is constructed as a "partnership" relationship. Referring to Article 1 number 13 of the Micro, Small, and Medium Enterprises Law (UMKM Law), partnerships require equal legal standing without any subordination. This legal construction is systematically used by applicators as a shield to avoid the doctrine of vicarious liability—where employers are responsible for the unlawful acts of their workers—which is actually strictly regulated in Articles 191 and 234 of Law Number 22 of 2009 concerning Road Traffic and Transportation (LLAJ Law).

Although applicators manage to avoid operational liability under the LLAJ Law through the pretext of technological partnerships, their claim to be "technology companies" actually binds them to the legal regime of Electronic System Providers (ESOs). As EOSs and Personal Data Controllers, applicators bear an unwavering responsibility for the reliability and security of their system architecture. Pursuant to Article 15 of Government Regulation Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions (PP PSTE), electronic system providers are required to provide written notification to data owners in the event of a failure in protecting personal data. This failure is not limited to hacking by external hackers but also includes "procedural failures" in maintaining data confidentiality. Legally, the fact that third parties (driver partners) can access, store, and utilize users' geolocation data and phone numbers without specific consent is a clear manifestation of the applicator's procedural failure in designing a security system that separates access rights (access control management).[13]

In an effort to escape responsibility for these procedural failures, applicators formulate privacy policies that are characterized by exoneration clauses. In the terms and conditions of an app, a standard clause is often embedded that explicitly states that the applicator is not responsible for the actions of third parties (drivers), and users are deemed to agree to release the applicator from all claims for compensation. A legal analysis of this practice leads to nullity by law (nietig). Article 18 paragraph (1) letter a of Law Number 8 of 1999 concerning Consumer Protection (UU PK) imperatively prohibits business actors from including standard clauses that state the transfer of responsibility. Considering that the clause exempting the

[13] Edmon Makarim, *Tanggung Jawab Penyelenggara Sistem Elektronik* (Jakarta: Rajawali Pers, 2010), hlm. 142-145.

applicator from responsibility for data leaks is contrary to the prohibition of the law, then based on the doctrine of the law of obligations, such clause is null and void and is considered never to have existed, so that the applicator still bears full responsibility for redressing consumer losses.[14]

On the other hand, the legal liability of third parties (driver partners) as intellectual and material actors in data misuse also has a clear legal dimension. Drivers who store or disseminate consumer data (such as by terrorizing them via instant messaging apps) without authorization have committed an Unlawful Act (PMH) as regulated in Article 1365 of the Civil Code.[15] Furthermore, this action fulfills the elements of a criminal offense under the ITE Law and the PDP Law regarding the misuse of personal data. However, the individual liability of the driver-partner does not automatically eliminate the applicator's civil liability. Both can be drawn into a joint and several liability scheme. The applicator was proven to have committed negligence in providing a vulnerable system and failed to exercise oversight (duty of care), while the driver actively exploited the system. Therefore, positive law requires applicators to apply the principle of strict liability for failures in their digital infrastructure, whereby a harmed consumer only needs to prove a data leak without having to prove any element of intent on the part of the applicator.

Concluding Remarks

Legal protection for the privacy and digital personal data of online transportation users in Indonesia still shows a significant gap between normative legal construction and empirical implementation. Although relatively comprehensive legal instruments are available through the 1945 Constitution of the Republic of Indonesia, the Consumer Protection Law, the ITE Law, the PP PSTE, and the Personal Data Protection Law, their effectiveness is still hampered by the business model of applicators that provides data access to third parties (driver-partners), the practice of storing data on servers outside of Indonesian jurisdiction, and the use of exoneration clauses and the pretext of partnership relationships to avoid legal accountability.

[14] Ahmadi Miru dan Sutarman Yodo, *Hukum Perlindungan Konsumen* (Jakarta: Rajawali Pers, 2015), hlm. 85-88

[15] Rosa Agustina, *Perbuatan Melawan Hukum* (Jakarta: Program Pascasarjana Fakultas Hukum Universitas Indonesia, 2003), hlm. 117.

However, as Electronic System Organizers and Personal Data Controllers, applicators still bear legal responsibility, even under strict liability regimes, while driver-partners are individually responsible for any intentional misuse of data. Therefore, strengthening data protection cannot simply rely on regulations, but must be accompanied by governance reforms through regular audits of app terms and conditions and privacy policies, the elimination of unlawful exoneration clauses, revisions to transportation regulations to affirm the legal status of ride-hailing app companies, and the implementation of privacy-by-design principles through data access restrictions, the use of number masking, and the automatic deletion of geolocation footprints after a transaction is completed. Without these measures, personal data protection in the digital transportation ecosystem will remain formalistic and unable to provide legal certainty or effective protection for consumers.

References

Agustina, Rosa. *Perbuatan Melawan Hukum*. Jakarta: Program Pascasarjana Fakultas Hukum Universitas Indonesia, 2003.

Makarim, Edmon. *Kompilasi Hukum Telematika*. Jakarta: Rajawali Pers, 2004.

Makarim, Edmon. *Tanggung Jawab Penyelenggara Sistem Elektronik*. Jakarta: Rajawali Pers, 2010.

Marzuki, Peter Mahmud. *Penelitian Hukum*. Jakarta: Kencana, 2017.

Miru, Ahmadi, dan Sutarman Yodo. *Hukum Perlindungan Konsumen*. Jakarta: Rajawali Pers, 2015.

Sidabalok, Janus. *Hukum Perlindungan Konsumen di Indonesia*. Bandung: Citra Aditya Bakti, 2014.

Soekanto, Soerjono, dan Sri Mamudji. *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: Rajawali Pers, 2015.

Fikri, dan Rusdiana. "Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Positif Indonesia." *Ganesha Law Review* 5, no. 1 (2023).

Fitriyani, A., & Antasia, P. (2025). Perlindungan Konsumen atas Perbuatan Melawan Hukum oleh Pengemudi Taxi Online sebagai Mitra Aplikasi. *Forschungsforum Law Journal*, *2*(01), 29-43.

Pratama, G. Y., Suradi, dan Aminah. "Perlindungan Hukum Terhadap Data Pribadi Pengguna Jasa Transportasi Online Dari Tindakan Penyalahgunaan Pihak Penyedia Jasa Berdasarkan Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen." *Diponegoro Law Journal* 5, no. 3 (2016).

Rosadi, Sinta Dewi. "Konsep Perlindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan Cloud Computing di Indonesia." *Yustisia Jurnal Hukum* 5, no. 1 (2016).

Yolanda, E., dan R. R. Hutabarat. "Urgensi Lembaga Pelindungan Data Pribadi di Indonesia Berdasarkan Asas Hukum Responsif." *Syntax Literate: Jurnal Ilmiah Indonesia* 8, no. 6 (2023).

Yunas, Hesty Ananta, dan Muhammad Irwan Padli Nasution. "Perlindungan Hukum Terhadap Privasi Data Pribadi Konsumen Pengguna Gojek di Indonesia." *SAMMAJIVA: Jurnal Penelitian Bisnis dan Manajemen* 1, no. 3 (2023).