IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2 . No.11, December 2025
DOI : https://doi.org/10.62872/beqpfa97

Commercialization of Citizen Data by Digital Platforms: Between Legality and Exploitation

Anis Noviya[1], Unggul Sagena[2]
Universitas Jambi,Indonesia[1]
Southeast Asia Freedom of Expression Network (SAFEnet)[2]

Received: November 27, 2025
Revised: December 12, 2025
Accepted: December 16, 2025
Published: December 30, 2025

Corresponding Author:
Author Name*: Anis Noviya
Email*:
anisnoviyanoviya@gmail.com

***Abstrak*:** *The commercialization of citizens' personal data has become a core element of digital platform business models through profiling, targeted advertising, and data analytics. The legality of such practices is commonly justified through user consent as the legal basis for data processing. In practice, however, consent is often formalistic and reflects an imbalance of bargaining power between platforms and users. This condition raises legal questions regarding the boundary between lawful data management and digital exploitation of privacy rights. This study aims to analyze the legality of data commercialization by digital platforms and to examine whether such practices constitute exploitation under personal data protection law. Using a normative juridical method with statutory, conceptual, and limited comparative approaches, this study finds a normative conflict between personal data protection principles and data driven economic practices legitimized by consent. Formal compliance does not necessarily ensure substantive privacy protection. The study concludes that restrictive interpretation of consent and stronger platform accountability are required to prevent the normalization of data exploitation in the digital economy.*
Keywords : consent; data commercialization; digital exploitation; personal data; privacy protection.

INTRODUCTION

The development of digital platforms over the past two decades has fundamentally shifted the position of citizens' personal data from mere identity information into a strategic economic asset. The business models of contemporary digital platforms are based on the large scale collection, processing, and utilization of personal data through mechanisms such as personalized advertising, behavioral profiling, and advanced data analytics. Birch, Cochrane, and Ward emphasize that personal data have undergone a conceptual transformation from an object of legal protection into an economic commodity that can be measured, valued, and traded by major technology corporations.[1] In this context, citizens' data are no

[1] Kean Birch, David Cochrane, and Callum Ward, "Data as Asset? The Measurement, Governance, and Valuation of Digital Personal Data by Big Tech," *Big Data and Society* 8 (2021), https://doi.org/10.1177/20539517211017308

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2 . No.11, December 2025
DOI : https://doi.org/10.62872/beqpfa97

longer treated as an extension of individual privacy rights, but rather as a source of economic value that is continuously extracted.

These data commercialization practices are generally legitimized through user consent mechanisms. Nearly every digital interaction is accompanied by agreement to privacy policies and terms of service that are unilaterally drafted by platforms. Normatively, consent is positioned as the legal basis for personal data processing. However, in practice, such consent is often formalistic, lacking transparency, and does not reflect equality of bargaining positions between platforms and citizens as data subjects. Schairer, Rubanovich, and Bloss demonstrate that complex privacy policies and terms of use systematically weaken the concept of informed consent, thereby stripping user consent of its substantive meaning.[2]

This phenomenon raises serious juridical concerns when data commercialization is conducted massively and continuously without a fair distribution of benefits to data subjects. Digital platforms obtain significant economic gains from citizens' data, while users merely receive access to services that are often illusory and disproportionate to the value of the data extracted. Popova describes this condition as a form of latent exploitation within the digital technology ecosystem, where economic and power relations are obscured by narratives of innovation and service convenience.[3] Accordingly, data commercialization practices can no longer be understood merely as legally neutral business activities.

In the context of Indonesian law, the regulation of personal data protection has undergone significant development with the enactment of Law Number 27 of 2022 on Personal Data Protection. This law recognizes data subject rights, the principles of lawful processing and purpose limitation, as well as the obligations of data controllers and processors. At the same time, however, the law also opens legal space for the utilization of personal data based on the consent of data subjects. Tension arises when the principle of privacy rights protection must confront the economic interests of digital platforms that treat data as their primary commodity. Lech and Durovic emphasize that modern data protection law faces a structural dilemma between protecting consumers and facilitating the data driven economy.[4]

The legal issue in this research is explicitly articulated as the existence of a normative conflict between the principles of personal data protection and citizens' privacy rights on the one hand, and the legality of data commercialization by digital platforms based on user consent on the other. On one side, data protection norms guarantee the data subject's right to control personal information. On the other side, platform business practices expand the extraction of economic value from citizens' data through mechanisms that are formally lawful but substantively problematic. This normative conflict places data protection law in an ambiguous position between an instrument of protection and a mechanism that legitimizes exploitation.

---

[2] C. Schairer, C. Rubanovich, and C. Bloss, "How Could Commercial Terms of Use and Privacy Policies Undermine Informed Consent," *AMA Journal of Ethics* 20 (2018): E864–E872, https://doi.org/10.1001/amajethics.2018.864

[3] S. Popova, "Latent Exploitation of Users of Digital Platforms," (2020), https://doi.org/10.7256/2454-0617.2020.2.33522

[4] Frederic Lech and Mateja Durovic, "A Consumer Law Perspective on the Commercialization of Data," *European Review of Private Law* (2021), https://doi.org/10.54648/erpl2021038

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2 . No.11, December 2025
DOI : https://doi.org/10.62872/beqpfa97

Constitutionally, Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia guarantees the right of every person to personal protection, honor, dignity, and property. The right to privacy as part of personal protection should function as a normative boundary for the utilization of personal data. However, when consent is treated as an absolute basis of legitimacy, such constitutional protection risks being reduced to a mere administrative formality. Sautunnida shows that without strict interpretation, personal data protection may lose its human rights function and shift into a mere instrument of administrative compliance.[5]

The gap between norms and practice is further exacerbated by power imbalances between digital platforms and citizens. Platforms exercise full control over system design, choice architecture, and consent mechanisms that often force users to choose between surrendering their data or losing access to services. Fassl, Gröber, and Krombholz describe this practice as consent theater, a situation in which consent becomes a legal ritual devoid of genuine freedom of choice.[6] Under such conditions, consent no longer reflects free will, but rather the result of structural pressure.

Academic studies on personal data law in Indonesia have so far tended to focus on normative compliance with statutory obligations, such as the duties of data controllers, sanction mechanisms, and data security procedures. Maharani and Prakoso, for example, emphasize the importance of compliance by electronic system operators with consumer data protection obligations.[7] However, such approaches have not sufficiently examined data commercialization as a legal relationship marked by inequality and the potential for exploitation. The lack of critical analysis of these power relations indicates a significant academic gap.

From a global perspective, discourse on data commercialization has increasingly shifted toward critiques of the financialization of data and power asymmetry in the digital economy. Alexander emphasizes that ownership and control over data have become new sources of power that deepen inequality between platforms and citizens.[8] The phenomenon of datafying citizens described by Sjøvaag et al. also shows that citizens are systematically positioned as data suppliers without balanced control mechanisms.[9] These findings reinforce the urgency of reassessing the legality of data commercialization from the perspective of legal protection for citizens.

Based on this discussion, the novelty of this research lies in analyzing the commercialization of citizens' data not merely as an issue of compliance with consent, but as a problem of normative conflict between the protection of privacy rights and potentially exploitative digital economic practices. This research aims to analyze the legality of the commercialization of citizens' data by digital platforms and to examine whether

[5] L. Sautunnida, "Urgensi Undang Undang Perlindungan Data Pribadi di Indonesia," *Kanun Jurnal Ilmu Hukum* 20 (2018), https://doi.org/10.24815/kanun.v20i2.11159

[6] M. Fassl, L. Gröber, and K. Krombholz, "Stop the Consent Theater," *CHI Conference on Human Factors in Computing Systems* (2021), https://doi.org/10.1145/3411763.3451230

[7] R. Maharani and A. Prakoso, "Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik," *Jurnal USM Law Review* (2024), https://doi.org/10.26623/julr.v7i1.8705

[8] A. Alexander, "Data and AI Mystification," *Big Data and Society* 12 (2025), https://doi.org/10.1177/20539517251355617

[9] H. Sjøvaag et al., "Datafying Citizens," *Nordicom Review* 46 (2025): 76–99, https://doi.org/10.2478/nor-2025-0004

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2 . No.11, December 2025
DOI : https://doi.org/10.62872/beqpfa97

such practices can be qualified as a form of exploitation from the perspective of personal data protection law. Through this approach, the research is expected to provide a critical contribution to the development of a more substantive interpretation of data protection law that is oriented toward the protection of citizens.

METODOLOGI

This research is a normative juridical legal study that focuses on the analysis of personal data protection norms and the legality of data commercialization by digital platforms. This method is chosen because the issues examined relate directly to normative conflicts within statutory regulations and the interpretation of data protection law principles in the context of the digital economy.[10]

The approaches employed include the statute approach, conceptual approach, and comparative approach. The statute approach is conducted by analyzing Law Number 27 of 2022 on Personal Data Protection, Law Number 19 of 2016 on Information and Electronic Transactions, and Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions. The conceptual approach is used to examine the concepts of privacy rights, consent, digital exploitation, and power imbalances between platforms and citizens. The comparative approach is used in a limited manner by referring to data protection principles under the GDPR as a conceptual benchmark.

The legal materials used consist of primary legal materials in the form of statutory regulations, secondary legal materials in the form of literature on data protection law and the digital economy as well as reputable journal articles, and tertiary legal materials in the form of legal dictionaries and encyclopedias. The analysis is conducted in a normative prescriptive manner using systematic and critical interpretation in order to formulate the boundaries of the legality of data commercialization and to prevent legal exploitation of data subjects.[11]

RESULTS AND DISCUSSION

Normative Conflict between the Legality of Data Commercialization and the Principles of Personal Data Protection

Law Number 27 of 2022 on Personal Data Protection is constructed on a paradigm that emphasizes the protection of data subjects' rights through the principles of lawful processing, purpose limitation, and data minimization. Normatively, the processing of personal data may only be carried out when it has a valid legal basis, one of which is the consent of the data subject. However, within the digital economy, these very principles have become the legal foundation for digital platforms to commercialize personal data on a massive scale. This situation creates a structural normative conflict between the objective of protecting privacy rights and the reality of data utilization as an economic asset. Lech and Durovic argue that modern data protection law often functions dually as an instrument of protection and as a facilitator of data markets.[12]

The legality of data commercialization based on consent rests on the assumption that consent is given freely, consciously, and in an informed manner. However, this assumption is difficult to sustain in the context of

[10] Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Kencana, 2017).
[11] Ibid.
[12] Frederic Lech and Mateja Durovic, *op. cit.*

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2 . No.11, December 2025
DOI : https://doi.org/10.62872/beqpfa97

digital platforms that rely on choice architecture and interface design to influence user behavior. Guggenberger emphasizes that consent in the digital ecosystem more closely resembles administrative friction than an expression of free will, as users are rationally compelled to agree in order to access services.[13] Consequently, the consent that serves as the legal basis for data processing often fails to reflect substantive control by data subjects.

The normative conflict becomes more evident when the principle of purpose limitation is examined in practice. The Personal Data Protection Law requires that data be processed in accordance with specific purposes that have been communicated to the data subject. In practice, however, the purposes of data processing in commercialization activities are often formulated broadly and flexibly, allowing further use for advertising, analytics, and third party partnerships. Van der Vlist and Helmond demonstrate that data partnership ecosystems among platforms expand data circulation far beyond the original purpose of collection.[14] This raises the question of whether formal compliance with the principle of purpose limitation remains aligned with the substantive protection of privacy rights.

From a constitutional perspective, this normative conflict has direct implications for the protection of the right to privacy as guaranteed by Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia. The right to privacy requires not only procedural consent, but also protection against misuse and exploitation of personal data. Rosadi asserts that personal data protection should be understood as part of human rights that cannot be reduced through unilateral contractual arrangements.[15] When consent is treated as an absolute source of legitimacy, constitutional protection risks being degraded into a mere legal formality.

The normative conflict is also apparent in the relationship between freedom of contract and digital consumer protection. Digital platforms frequently rely on the principle of freedom of contract to justify terms of service that expand their rights to utilize personal data. However, in data protection law, freedom of contract cannot stand independently without regard to inequality of bargaining power. Frolovskaya and Bondarenko emphasize that personal data collection in the digital era often exceeds the bounds of propriety due to the weak negotiating position of individuals.[16] This demonstrates that formal legality does not necessarily equate to legal justice.

Thus, the normative conflict between the legality of data commercialization and the principles of personal data protection reflects a normative crisis within data protection law. Formal compliance with consent and lawful processing principles does not necessarily guarantee substantive protection of citizens' privacy rights. Without a more restrictive and critical interpretation, data protection law risks functioning as a mechanism that legitimizes data exploitation within the digital economy.

---

[13] Nicolas Guggenberger, "Consent as Friction," *Boston College Law Review* (2025), https://doi.org/10.70167/choq9209

[14] Fernando Van der Vlist and Anne Helmond, "How Partners Mediate Platform Power," *Big Data and Society* 8 (2021), https://doi.org/10.1177/20539517211025061

[15] Siti Rosadi, "Prinsip Prinsip Perlindungan Data Pribadi," *Sosiohumaniora* 19 (2017): 206–212.

[16] Frolovskaya, Y., & Bondarenko, TProblem Issues of Collecting Personal Data in the Era of Global Digitalization. *Sociopolitical Sciences*. (2025). https://doi.org/10.33693/2223-0092-2025-15-3-182-188

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2 . No.11, December 2025
DOI : https://doi.org/10.62872/beqpfa97

Commercialization of Citizen Data as a Form of Digital Exploitation in Platform–User Relations

Exploitation in legal contexts does not always take the form of explicit violations of written norms, but may occur through mechanisms that are formally lawful yet substantively harmful to weaker parties. In the relationship between digital platforms and citizens as data subjects, data exploitation emerges through structural inequalities in access to information, technological control, and the distribution of economic benefits. Popova identifies this phenomenon as latent exploitation, where users contribute significant economic value without receiving commensurate returns.[17]

Inequality of bargaining position constitutes a key element in understanding data exploitation. Digital platforms control system design, algorithms, and privacy policies, while users are placed in a take it or leave it position. Under such conditions, consent no longer functions as a tool of control, but as a mechanism of legitimation. Fassl et al. describe this practice as consent theater, where consent serves a symbolic function without genuine freedom of choice.[18] This situation illustrates that the legal relationship between platforms and users is substantively unequal.

Data commercialization also exhibits patterns of asymmetric value extraction. Platforms generate financial profits through personalized advertising, aggregated data sales, and business partnerships, while users receive digital services that are often non exclusive and easily substitutable. Alexander emphasizes that the financialization of data creates a new form of capital accumulation based on citizen data without mechanisms for value redistribution.[19] From the perspective of legal justice, this condition is difficult to justify when consent is treated as the sole basis of legitimacy.

To clarify the characteristics of data exploitation in platform–user relations, the following table is presented:

Table 1. Data Commercialization and Power Asymmetry between Platforms and Users

Aspect	Platform Position	User Position	Legal Implication
Control over data	Full technical and economic control	No effective control after consent	Asymmetry of power
Economic benefit	Monetization and profit extraction	Limited access to services	Unequal value distribution
Consent mechanism	Designed unilaterally	Take it or leave it	Illusory consent
Legal protection	Compliance oriented	Substantive protection weak	Risk of exploitation

The table demonstrates that data exploitation does not always violate written norms, but rather emerges from imbalances in legal and economic relationships. Schairer et al. emphasize that lengthy and complex privacy policies systematically prevent users from understanding the implications of data

[17] S. Popova, *op. cit.*
[18] M. Fassl et al., *op. cit.*
[19] A. Alexander, *op. cit.*

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2 . No.11, December 2025
DOI : https://doi.org/10.62872/beqpfa97

commercialization.[20] This reinforces the argument that consent in practice often fails to meet the standard of rights protection envisioned by the law.

From the perspective of data protection law, digital exploitation must be understood as a failure of law to ensure effective control by data subjects. Sjøvaag et al. show that the process of datafying citizens positions individuals as permanent data suppliers for digital infrastructures, including within public services.[21] Without firm normative intervention, data commercialization risks becoming a new norm that is socially and legally accepted.

Accordingly, the commercialization of citizen data by digital platforms may be qualified as a form of digital exploitation when formal legality based on consent is not balanced by substantive protection and fair distribution of benefits. This analysis underscores the need for a paradigm shift from consent based compliance toward rights based protection in personal data protection law.

Implications of Normative Conflict for the Protection of Privacy Rights and the Accountability of Digital Platforms

The normative conflict between consent based legality of data commercialization and the principles of personal data protection has direct implications for the effectiveness of privacy rights protection for citizens. Within the framework of Law Number 27 of 2022 on Personal Data Protection, the rights of data subjects are formulated as the rights to be informed, to access, to rectify, and to erase personal data. However, when data commercialization is legitimized through formalistic consent, these rights are often difficult to realize substantively. Lech and Durovic emphasize that consumer protection within the data economy tends to weaken when consent is treated as comprehensive legitimacy for data utilization.[22]

The first implication is reflected in the weakness of oversight and law enforcement mechanisms against excessive data utilization practices. Data protection authorities face difficulties in distinguishing between lawful data processing and exploitative commercialization practices because the boundaries are not explicitly regulated. Although the Personal Data Protection Law provides supervisory authority and sanctions, it does not explicitly regulate limits on the commercialization of personal data. As a result, law enforcement tends to focus on procedural violations such as data breaches, rather than on structural exploitation occurring in everyday business practices. Lutrianto and Riswaldi show that the primary problem of data protection in Indonesia lies not only in technical violations, but in weak substantive control over data utilization by data controllers.[23]

The second implication relates to the difficulty faced by citizens in holding digital platforms accountable. In practice, users often lack adequate access to information regarding how their data are monetized and

[20] C. Schairer, C. Rubanovich, and C. Bloss, "How Could Commercial Terms of Use and Privacy Policies Undermine Informed Consent," *AMA Journal of Ethics* 20 (2018): E864–E872, https://doi.org/10.1001/amajethics.2018.864

[21] H. Sjøvaag et al., *op. cit.*

[22] Frederic Lech and Mateja Durovic, *op. cit.*

[23] Iwan Lutrianto and Riswaldi Riswaldi, "Legal Problems of Personal Data Protection," *Greenation International Journal of Law and Social Sciences* (2025), https://doi.org/10.38035/gijlss.v3i2.429

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2 . No.11, December 2025
DOI : https://doi.org/10.62872/beqpfa97

with whom the data are shared. This lack of transparency hampers legal remedies because the burden of proof becomes extremely heavy. Alexander emphasizes that the mystification of data within the platform economy functions to conceal power relations and economic value flows derived from personal data.[24] Without transparency regarding the economic value of data, data subject rights risk becoming purely normative and non operational.

The normative conflict also creates the risk of normalizing data exploitation through mere legal compliance. Digital platforms may claim compliance with the Personal Data Protection Law by demonstrating the existence of consent and privacy policies, even though substantively such practices harm citizens. Guggenberger refers to this phenomenon as legal compliance without justice, in which the law is formally obeyed but fails to protect the interests it is intended to safeguard.[25] This normalization is dangerous because it shifts the orientation of data protection law from rights protection toward legitimization of data markets.

From a human rights perspective, this normative conflict places the right to privacy in a vulnerable position. The right to privacy as part of the right to personal protection should not be fully subordinated to contractual logic. Sautunnida emphasizes that personal data protection must be understood as a limitation on power, both state power and corporate power.[26] When consent is treated as an absolute basis, power relations between platforms and citizens are left without adequate normative correction.

Further implications concern the accountability of digital platforms. Without progressive interpretation, platforms lack strong incentives to limit the extraction of economic value from citizen data. Hase et al. show that obligations related to data access and transparency are only effective when accompanied by clear and enforceable accountability mechanisms.[27] Therefore, the normative conflict between legality and protection must be addressed through legal interpretation that positions data subject rights as substantive limits on data commercialization.

Thus, the implications of normative conflict affect not only individuals, but also the overall trajectory of data protection law. Without normative correction, the law risks becoming an instrument that legitimizes data exploitation within the digital economy. Accordingly, restrictive interpretation of consent and strengthening of rights based protection are necessary to ensure that data commercialization does not violate the dignity and rights of citizens.

CONCLUSIONS

The commercialization of citizen data by digital platforms places data protection law in a grey area between legality and exploitation. This study demonstrates that normative conflict between the principles of privacy rights protection and the legality of consent based data processing has resulted in the failure of substantive legal protection for citizens. Formal compliance with user consent does not necessarily guarantee meaningful control over the utilization of personal data. Therefore, personal data protection law must be

[24] A. Alexander, *op. cit*
[25] Nicolas Guggenberger, *op. cit.*
[26] L. Sautunnida, *op. cit.*
[27] V. Hase et al., "Fulfilling Data Access Obligations," *Internet Policy Review* 13 (2024), https://doi.org/10.14763/2024.3.1793

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2 . No.11, December 2025
DOI : https://doi.org/10.62872/beqpfa97

interpreted restrictively and critically toward consent mechanisms so that it does not function as a means of legitimizing digital exploitation. Strengthening the role of data protection authorities, increasing transparency regarding the economic value of data, and affirming clear limits on the commercialization of personal data are essential steps to ensure that the development of the digital economy remains aligned with the protection of human rights and the dignity of citizens.

REFERENCES

Undang-Undang

Undang Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Undang Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Artikel dan Buku

Abrardi, L., Cambini, C., & Hoernig, S. (2024). “I don't care about cookies!” data disclosure and time-inconsistent users. Information Economics and Policy. https://doi.org/10.1016/j.infoecopol.2024.101112.

Alexander, A. (2025). Data and AI mystification: Ownership, control, and financialization in the platform. Big Data Soc., 12. https://doi.org/10.1177/20539517251355617.

Birch, K., Cochrane, D., & Ward, C. (2021). Data as asset? The measurement, governance, and valuation of digital personal data by Big Tech. Big Data & Society, 8. https://doi.org/10.1177/20539517211017308.

Fad, M. (2021). Perlindungan Data Pribadi Dalam Perspektif Sadd Dzari’ah. MUAMALATUNA. https://doi.org/10.37035/mua.v13i1.4674.

Fassl, M., Gröber, L., & Krombholz, K. (2021). Stop the Consent Theater. Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3411763.3451230.

Frolovskaya, Y., & Bondarenko, T. (2025). Problem Issues of Collecting Personal Data in the Era of Global Digitalization. Sociopolitical Sciences. https://doi.org/10.33693/2223-0092-2025-15-3-182-188.

Guggenberger, N. (2025). Consent as Friction. Boston College Law Review. https://doi.org/10.70167/choq9209.

Hase, V., Ausloos, J., Boeschoten, L., Pfiffner, N., Janssen, H., Araujo, T., Carrière, T., Vreese, C., Haßler, J., Loecherbach, F., Kmetty, Z., Möller, J., Ohme, J., Schmidbauer, E., Struminskaya, B., Trilling, D., Welbers, K., & Haim, M. (2024). Fulfilling data access obligations: How could (and should) platforms facilitate data donation studies?. Internet Policy Rev., 13. https://doi.org/10.14763/2024.3.1793.

Irmawati, E., Pieries, J., & Widiarty, W. (2024). Perlindungan Hukum Atas Data Pribadi Nasabah Bank Pengguna Mobile Banking dalam Perspektif Uu No 27 Tahun 2022 tentang Kebocoran Data. Jurnal Syntax Admiration. https://doi.org/10.46799/jsa.v5i1.964.

Kim, M., Jacob, Y., & Bire, C. (2025). Perlindungan Data Pribadi Pada Platform Digital Pinjaman Online Ditinjau Dari Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (Studi Kasus Di Kota Kupang, NTT). Artemis Law Journal. https://doi.org/10.35508/alj.v2i2.21070.

Lech, F., & Durovic, M. (2021). A Consumer Law Perspective on the Commercialization of Data. European Review of Private Law. https://doi.org/10.54648/erpl2021038.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2 . No.11, December 2025
DOI : https://doi.org/10.62872/beqpfa97

Lutrianto, I., & Riswaldi, R. (2025). Legal Problems of Personal Data Protection in The Digital Era in Personal Data Protection Law in Indonesia. Greenation International Journal of Law and Social Sciences. https://doi.org/10.38035/gijlss.v3i2.429.

Maharani, R., & Prakoso, A. (2024). Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital. JURNAL USM LAW REVIEW. https://doi.org/10.26623/julr.v7i1.8705.

Marzuki, P. M. (2017). Penelitian hukum (Edisi revisi). Kencana.

Noviyanti, D., , Y., & , S. (2025). Legal Protection Analysis of Personal Data Breaches in Shopee Paylater Consumer Loan Transactions. Journal of Law and Economics. https://doi.org/10.56347/jle.v4i1.240.

Popova, S. (2020). Latent exploitation of users of digital platforms as a norm of the techworld: to articulation of the problem for social research. , 11-25. https://doi.org/10.7256/2454-0617.2020.2.33522.

Putri, A., Sari, N., Fajrina, P., & Aisyah, S. (2024). Keamanan Online dalam Media Sosial: Pentingnya Perlindungan Data Pribadi di Era Digital (Studi Kasus Desa Pematang Jering). Jurnal Pengabdian Nasional (JPN) Indonesia. https://doi.org/10.35870/jpni.v6i1.1097.

Rosadi, S. (2017). PRINSIP-PRINSIP PERLINDUNGAN DATA PRIBADI NASABAH KARTU KREDIT DIKAITKAN DENGAN UNDANG-UNDANG NO 11 TAHUN 2008 TENTANG ITE DAN PERATURAN BANK INDONESIA NO 7/6/PBI/2005. , 19, 206-212. https://doi.org/10.24198/sosiohumaniora.v19i3.11380.

Sautunnida, L. (2018). Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia. Kanun Jurnal Ilmu Hukum. https://doi.org/10.24815/kanun.v20i2.11159.

Schairer, C., Rubanovich, C., & Bloss, C. (2018). How Could Commercial Terms of Use and Privacy Policies Undermine Informed Consent in the Age of Mobile Health?. AMA journal of ethics, 20 9, E864-872 . https://doi.org/10.1001/amajethics.2018.864.

Sjøvaag, H., Brantner, C., Ferrer-Conill, R., Karlsson, M., & Helles, R. (2025). Datafying citizens: Third-party trackers and data-as-payment in government infrastructure. Nordicom Review, 46, 76 - 99. https://doi.org/10.2478/nor-2025-0004.

Van Der Vlist, F., & Helmond, A. (2021). How partners mediate platform power: Mapping business and data partnerships in the social media ecosystem. Big Data & Society, 8. https://doi.org/10.1177/20539517211025061.

Yitawati, K., , S., Purwati, Y., & Sukarjono, B. (2022). IMPLIKASI DAN SOSIALISASI UNDANG-UNDANG TENTANG PERLINDUNGAN DATA PRIBADI DALAM MENJAGA KERAHASIAAN DATA PRIBADI SESEORANG. JURNAL DAYA-MAS. https://doi.org/10.33319/dymas.v7i2.92.