Adagium: Jurnal Ilmiah Hukum
E-ISSN: 2985-5128
Volume 4 Number 2 (2026), pp. 701-711
DOI: https://doi.org/10.70308/jmxfa253

Legal Protection for Merchants against Automated Marketplace Decisions Reducing Rankings and Restricting Accounts

Luthfiana Livia Happy
Universitas Jenderal Soedirman, Purwokerto, Indonesia
Correspondence: luthfiana.happy@mhs.unsoed.ac.id

Received: 28 May 2026	*Accepted: 27 August 2026*	*Published: 31 August 2026*

Abstrak

Penelitian ini mengkaji batas kewenangan penyelenggara marketplace untuk menurunkan peringkat produk dan membatasi akun pedagang melalui keputusan otomatis serta kecukupan perlindungan hukum bagi pedagang yang terdampak. Penelitian menggunakan metode hukum normatif dengan pendekatan perundang-undangan dan konseptual. Analisis mencakup pengaturan Indonesia mengenai perdagangan elektronik, pelindungan data pribadi, pemeringkatan, pembatasan akun, dan tata kelola kecerdasan artifisial, serta teori perlindungan hukum preventif dan represif Philipus M. Hadjon dan konsep ketertutupan sistem. Hasil penelitian menunjukkan bahwa regulasi telah mengakui kewajiban informasi, mekanisme pengaduan dan koreksi, tata kelola kecerdasan artifisial, serta keberatan terhadap keputusan otomatis. Namun, perlindungan pada tingkat keputusan individual belum lengkap, terutama terkait alasan yang spesifik, kesempatan klarifikasi sebelum pembatasan signifikan, pemeriksaan manusia yang substantif, batas waktu penyelesaian yang jelas, tindakan sementara yang proporsional, dan pemulihan menyeluruh. Penyelenggara tetap bertanggung jawab atas hasil otomatis karena sistem dipilih, dikelola, dan digunakan untuk kepentingan usahanya. Perlindungan yang memadai mensyaratkan keputusan yang dapat dijelaskan, ditentang, dikoreksi, dipulihkan, dan dipertanggungjawabkan secara hukum.

Kata kunci: keputusan otomatis; marketplace; perlindungan hukum; pedagang; pemeringkatan algoritmik.

Abstract

This article examines automated marketplace decisions that reduce product rankings or restrict merchant accounts through procedural fairness, explainability, human review, and legal remedies for merchants affected by automated platform governance. It uses normative legal research and a structured analysis of applicable legal materials, supported by comparative and interdisciplinary scholarship where relevant. The revised analysis distinguishes legal design from empirical claims and identifies the principal regulatory or institutional gap. The study finds that existing law provides important but fragmented safeguards and that legal certainty depends on clearer decision criteria, procedural accountability, and proportionate remedies. It proposes an operational framework that specifies legal thresholds, institutional responsibilities, safeguards, and review mechanisms. The article contributes a more explicit research gap, a reproducible doctrinal method, and a policy model calibrated to legality, proportionality, accountability, and rights protection.

Keywords: *automated decision; marketplace; legal protection; merchant; algorithmic ranking.*

INTRODUCTION

Electronic commerce has become a major part of Indonesia's economy. E-commerce transaction value increased from approximately Rp205.5 trillion in 2019 to about Rp487 trillion in 2024. This growth has deepened merchants' dependence on marketplaces to reach consumers, receive payments, market products, and build business reputations.[1]

A marketplace is more than a venue for transactions. Its operator controls the order of search results, product recommendations, access to promotions, performance ratings, and the status of merchant accounts. These powers are exercised through automated systems processing transaction and user-behavior data. A ranking reduction can diminish product visibility, while an account restriction can halt orders, access to balances, and sales activity.[2]

These effects appear in merchant complaints. One seller reported that an account was restricted and could not be restored after the system identified promotional abuse, even though earlier orders had followed customer-service instructions. Another complaint concerned approximately Rp15 million in sales proceeds retained after an account was declared permanently inactive. A Lazada seller separately complained of an unexplained account restriction and the use of sales proceeds without consent. These individual reports do not establish nationwide incidence, but they illustrate the losses account restrictions can cause.

The legal problem lies in the imbalance between the consequences of a decision and the merchant's ability to test it. A merchant can lose business access on the basis of a system assessment while receiving only general reasons such as unusual activity, promotional abuse, or policy violation. Transaction data, violation indicators, and assessment parameters remain under the operator's control. The merchant is consequently required to contest a decision without knowing the particular data or conduct deemed unlawful.[3]

This situation can be described as system opacity or a black box: an institution obtains extensive information about the evaluated party, while its evaluation process is closed to the person affected. The central problem with automated marketplace decisions is therefore not technology itself but the power to impose measures that merchants have difficulty examining and challenging.[4]

Philipus M. Hadjon distinguishes preventive from repressive legal protection. Preventive protection in this context includes notice before restriction, specific reasons, access to information underlying the assessment, and an opportunity to clarify. Repressive protection includes objection, human review, account

---

[1] M. Rani, "Pemahaman Masyarakat terhadap Ketentuan Hukum Jual Beli Online," Masalah-Masalah Hukum 51, no. 4 (2022): 355–366, https://doi.org/10.14710/mmh.51.4.2022.355-366.

[2] Alifia Jasmine, Prita Amalia, and Helitha Novianty Muchtar, "Tanggung Jawab Platform Marketplace terhadap Penjualan Ponsel (Mobile Phone) Ilegal Berdasarkan Hukum Nasional," Masalah-Masalah Hukum 51, no. 4 (2022): 378–389, https://doi.org/10.14710/mmh.51.4.2022.378-389.

[3] Irma Winarsih and Firya Oktaviarni, "Tanggung Jawab Penyedia Layanan Aplikasi Marketplace terhadap Konsumen dalam Transaksi Jual Beli Online di Provinsi Jambi," Zaaken: Journal of Civil and Business Law 2, no. 2 (2021): 349–367, https://doi.org/10.22437/zaaken.v2i2.11322.

[4] Uu Nurul Huda et al., Data Pribadi, Hak Warga, dan Negara Hukum: Menjaga Privasi di Tengah Ancaman Digital (Bandung: Penerbit Widina, 2024).

reactivation, ranking restoration, release of funds, and resolution of losses. This theory tests whether merchant protection is limited to a complaint channel or can actually prevent and remedy an erroneous decision.[5]

Indonesian law recognizes the use of automated systems in electronic commerce. Article 10 of Law Number 27 of 2022 on Personal Data Protection gives a data subject the right to object to a decision based solely on automated processing that produces legal or similarly significant effects. Minister of Trade Regulation Number 19 of 2026 also requires marketplaces to provide information about promotion and ranking features, operate complaint mechanisms, implement artificial-intelligence governance, and provide correction mechanisms for AI-generated services.[6]

These rules do not detail protection against individual decisions reducing rankings or restricting accounts. A general explanation of ranking rules does not ensure that a merchant knows why a particular product was demoted. Nor does a complaint mechanism expressly guarantee access to evidence, substantive human review, suspension of a restriction while an objection is examined, or restoration when the decision is shown to be wrong. A gap therefore remains between recognition of automated systems and legal guarantees for merchants who bear their consequences.[7]

This study examines the limits of an operator's authority to reduce rankings and restrict accounts and the adequacy of merchant protection. The assessment considers preventive measures - notice, reasons, access to information, and an opportunity to clarify - and repressive measures - review, restoration of accounts and rankings, dispute resolution, and responsibility for loss.

Indonesian marketplace scholarship has addressed platform liability, consumer protection, and personal-data governance, but less attention has been paid to procedural safeguards at the level of an individual automated decision affecting a merchant. This article contributes a decision-specific framework that separates general system transparency from the duty to provide reasons, a meaningful opportunity to contest, substantive human review, proportional interim measures, and effective restoration.

RESEARCH METHOD

This normative legal study applies statutory, conceptual, and limited comparative approaches. Indonesian rules on electronic commerce, personal-data protection, marketplace ranking, account restrictions, and artificial-intelligence governance are analyzed together with the distinction between preventive and repressive legal protection. The unit of analysis is the individual adverse platform decision rather than the algorithm in the abstract. The assessment uses six procedural criteria: notice, specificity of reasons, opportunity to clarify, meaningful human review, time-bound resolution, and restoration/remedy. Comparative

[5] Tedi Sudrajat and Endra Wijaya, Perlindungan Hukum terhadap Tindakan Pemerintahan (Jakarta: Bumi Aksara, 2021).

[6] E. Fauzy and Nabila Alif Radika Shandy, "Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi," Lex Renaissance 7, no. 3 (2022): 445–461, https://doi.org/10.20885/JLR.vol7.iss3.art1.

[7] Erna Priliasari, "Perlindungan Data Pribadi Konsumen dalam Transaksi E-Commerce," Jurnal Rechts Vinding 12, no. 2 (2023), https://doi.org/10.33331/rechtsvinding.v12i2.1285.

platform-governance literature is used to test the adequacy of these safeguards without treating foreign rules as binding Indonesian law.

Primary materials include Law Number 27 of 2022 on Personal Data Protection, Government Regulation Number 71 of 2019, Government Regulation Number 80 of 2019, and Minister of Trade Regulation Number 19 of 2026. Secondary materials consist of books, journal articles, research, and other documents concerning automated decisions, platform governance, and protection of marketplace merchants.

The legal materials were collected through library research and analyzed qualitatively by interpreting, comparing, and connecting applicable rules with the concept of legal protection. The analysis focuses on preventive protection before a ranking reduction or account restriction and repressive protection after an automated decision causes loss.

RESULTS AND DISCUSSION

Adequacy of Preventive Legal Protection for Merchants

Hadjon describes preventive legal protection as operating before a decision causes harm. It allows the affected party to know the basis of a proposed measure and object before the decision is made. In the merchant-platform relationship, preventive protection is not satisfied merely by terms of use or general ranking information. It depends on whether the merchant receives notice, sufficient reasons, access to decision-related information, and an opportunity to explain before a ranking reduction or account restriction is imposed.[8]

Minister of Trade Regulation Number 19 of 2026 requires marketplaces to provide information about promotion and ranking features, recognizing that ranking is not merely an internal technical matter. A ranking system determines product position, store visibility, and opportunities to reach consumers. Because these effects directly concern business activity, an operator cannot make system changes in complete secrecy. General information about ranking factors nevertheless does not explain why a particular product was demoted at a particular time.

The distinction between system transparency and decision transparency is central. System transparency identifies general factors such as cancellation rates, delivery delays, consumer reviews, store performance, or policy compliance. Decision transparency identifies the product or transaction examined, assessment period, problematic data, and relationship between that data and the imposed measure. General information helps merchants adapt their conduct; an individual explanation enables them to test the decision. Without it, a merchant knows only that the system acted and cannot identify the facts to explain or contest.[9]

This structure reflects a black box. The operator collects transaction data, account history, promotional use, device locations, cancellation rates, and

---

[8] Hanifan Niffari, “Perlindungan Data Pribadi sebagai Bagian dari Hak Asasi Manusia atas Perlindungan Diri Pribadi,” Jurnal Yuridis 7, no. 1 (2020): 105–119, https://doi.org/10.35586/jyur.v7i1.1846.

[9] Andi Putri Denisa, “Sertifikat Keandalan Privasi sebagai Salah Satu Bentuk Perlindungan Data Pribadi dalam Transaksi E-Commerce,” Jurnal Rechts Vinding 12, no. 2 (2023), https://doi.org/10.33331/rechtsvinding.v12i2.1286.

performance indicators, while the merchant receives only the final ranking reduction or account restriction. The decision maker also controls the information needed to test the decision. Merchants do not require source code, precise parameter weights, or security mechanisms; they require information explaining the basis of the individual decision without disclosure of all platform trade secrets.[10]

Automated systems have operational justifications. Marketplaces manage too many products and transactions for complete manual monitoring. Systems can identify fictitious transactions, promotional abuse, intellectual-property violations, prohibited products, or risk patterns. Speed and efficiency do not eliminate error. Algorithms rely on categories and data that may miss commercial context: a promotional sales surge may look suspicious; a shared device may suggest linked accounts although used by an employee or family member; and delivery delays may reduce an account score even when caused by a logistics provider.[11]

If a system result is implemented without clarification, the merchant bears the risk of error while the operator receives the benefit of automation. The merchant can explain only after loss occurs, contrary to preventive protection. For administrative breaches, performance reductions, or disputed facts, a merchant should be able to provide transaction documents, shipment evidence, proof of product ownership, or an explanation of account activity before a significant measure takes effect.[12]

An opportunity to clarify does not require every decision to await merchant consent. Immediate restriction may be justified by suspected serious fraud, dangerous goods, system attacks, or direct consumer risk. The exception must be limited to urgent circumstances and followed promptly by notice and review. Treating every alleged violation as an emergency deprives preventive protection of its function.

Proportionality is also essential. An operator must match the measure to the severity and risk of the violation. An error involving one product should not automatically close an entire account. Measures can progress from warning and correction request to product deactivation, feature restriction, temporary suspension, and permanent closure. Closure should be reserved for serious, repeated, or high-risk violations; without graduated measures, an automated response may be more severe than its basis.[13]

Article 10 of the Personal Data Protection Law permits a data subject to object to a decision based solely on automated processing that has legal or significant effects. Ranking reductions and account restrictions may be significant when they

---

[10] Sinta Dewi Rosadi and Garry Gumelar Pratama, "Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital di Indonesia," Veritas et Justitia 4, no. 1 (2018): 88–110, https://doi.org/10.25123/vej.2916.

[11] Kornelius Benuf, "Hambatan Formal Penegakan Hukum Pidana terhadap Kejahatan Pencurian Data Pribadi," Majalah Hukum Nasional 51, no. 2 (2021): 261–279, https://doi.org/10.33331/mhn.v51i2.148.

[12] Mutia Rahma Wardani, Joko Priyono, and Fifiana Wisnaeni, "Perlindungan Konsumen dalam Transaksi Elektronik melalui Instagram," Notarius 13, no. 2 (2020): 848–864, https://doi.org/10.14710/nts.v13i2.31183.

[13] Sekararum Intan Munggaran, Sudjana, and Bambang Daru Nugroho, "Perlindungan Konsumen terhadap Pencantuman Klausula Baku dalam Perjanjian," ACTA DIURNAL Jurnal Ilmu Hukum Kenotariatan 2, no. 2 (2019): 187–199.

reduce access to consumers, stop transactions, or retain sales proceeds. This strengthens protection for individual merchants but not necessarily for every merchant, because a corporate entity is not always a personal-data subject.[14]

A further limitation lies in the word 'solely.' An operator may claim that a staff member participated in the final decision even if the person merely approved a system result. Human involvement must be assessed by function and authority. Review is substantive only when the person understands the recommendation, accesses the data, considers the merchant's explanation, and has authority to change the outcome. Rubber-stamping an algorithm does not materially alter the automated character of the decision.[15]

Minister of Trade Regulation Number 19 of 2026 also requires AI governance proportionate to risk and a complaint or correction mechanism. This should support different oversight standards according to consequences. An ordinary recommendation system may warrant lighter oversight, while a system capable of reducing rank, restricting an account, or retaining funds requires stronger records, testing, and human review. The greater the impact on business activity, the higher the operator's duty of care.[16]

Regulation therefore recognizes information duties, AI governance, and objections to automated decisions but does not yet create complete preventive protection for individual decisions. It lacks firm duties to give concrete reasons and pre-decision clarification, distinguish ordinary from significantly harmful decisions, and provide substantive human review. Under Hadjon's theory, adequate protection requires individual notice, an explanation of the basis, an opportunity to clarify, proportionate measures, and human review with authority to alter the system result. Without these elements, the merchant remains the object of algorithmic assessment while the operator controls both process and consequence.

Effectiveness of Repressive Legal Protection and Operator Responsibility

Hadjon's repressive protection operates after a decision causes dispute or loss. In the marketplace relationship, it applies after an automated system reduces product ranking, restricts trading features, freezes an account, or withholds funds. Protection is measured not by the existence of a help center or appeal button, but by whether the procedure reveals the basis, conducts a new review, cancels an erroneous measure, and restores merchant rights. A response merely stating that the account violated policy under the system is communication, not legal correction.[17]

Merchant complaints show repeated patterns: restrictions based on alleged promotional abuse or unusual transactions without a detailed explanation of the

[14] B. A. Iswandari, "Jaminan Atas Pemenuhan Hak Keamanan Data Pribadi dalam Penyelenggaraan E-Government Guna Mewujudkan Good Governance," Jurnal Hukum IUS QUIA IUSTUM 28, no. 1 (2021): 115–138, https://doi.org/10.20885/iustum.vol28.iss1.art6.

[15] Edi Saputra Hasibuan and Elfirda Ade Putri, "Perlindungan Keamanan Atas Data Pribadi di Dunia Maya," Jurnal Hukum Sasana 10, no. 1 (2024): 70–83, https://doi.org/10.31599/sasana.v10i1.2134.

[16] Erlina Maria Christin Sinaga and Mery Christian Putri, "Formulasi Legislasi Perlindungan Data Pribadi dalam Revolusi Industri 4.0," Jurnal Rechts Vinding 9, no. 2 (2020): 237–256, https://doi.org/10.33331/rechtsvinding.v9i2.428.

[17] David M. L. Tobing, Klausula Baku: Paradoks dalam Penegakan Hukum Perlindungan Konsumen (Jakarta: Gramedia Pustaka Utama, 2019).

evidence, sometimes followed by withheld balances and accounts remaining unrestored after appeal. Individual complaints cannot establish national prevalence, but they reveal the concrete problem that platform decisions cause immediate economic effects while merchants lack the information needed to contest them.

Minister of Trade Regulation Number 19 of 2026 requires operators to provide accessible electronic complaint services and dispute-resolution mechanisms for merchants, with response times and documented outcomes. It also makes the operator responsible for AI use in electronic commerce. An automated result cannot be separated from operator responsibility: an algorithm is not a legal subject that can explain itself or provide redress. It is used within the organization for the operator's business interests, so legal consequences remain with the party operating and benefiting from it.[18]

A complaint duty alone does not cure the imbalance. A right to complain differs from a right to review. Review requires reassessment of data, evidence, transaction context, and the appropriateness of the measure, which is possible only if the merchant knows what must be contested. The operator should identify the relevant product or transaction, timing, allegedly violated rule, and principal factor triggering the decision. This does not require source-code disclosure; it makes an individual decision testable.[19] When the basis remains closed, the evidentiary burden is unbalanced. The operator controls transaction data, system records, risk parameters, and account-assessment history, while the merchant must prove the absence of a violation. The merchant can formally object but lacks knowledge of the material to contest, reproducing the black-box condition.

Article 10 of the Personal Data Protection Law may assist an individual merchant when automated processing of personal data stops transactions or access to funds. Its reach remains limited because corporate merchants are not always data subjects and the phrase 'based solely on automated processing' invites dispute when an operator claims staff involvement.

A staff member's presence does not itself establish substantive human review. The reviewer must access the system's reasons, assess merchant evidence, consider business context, and have authority to cancel or modify the measure. A staff member who merely approves the algorithm or repeats its explanation does not perform a new review. Separating the decision-making unit from the objection unit is also desirable because the operator simultaneously makes policy, holds the data, applies restrictions, and adjudicates internal disputes.[20]

Effectiveness also depends on deadlines and interim measures. A customer-service response time is not the same as a deadline for resolving an objection. An initial answer may be prompt while the restriction continues indefinitely and daily losses accumulate. Full restriction need not always remain during review:

---

[18] Gunardi Lie, Dylan Aldianza Ramadhan, and Ahmad Redi, "Komisi Independen Perlindungan Data Pribadi: Quasi Peradilan dan Upaya Terciptanya Right to Be Forgotten di Indonesia," Jurnal Yudisial 15, no. 2 (2022): 227–246, https://doi.org/10.29123/jy.v15i2.530.

[19] Faiz Rahman, "Kerangka Hukum Perlindungan Data Pribadi dalam Penerapan Sistem Pemerintahan Berbasis Elektronik di Indonesia," Jurnal Legislasi Indonesia 18, no. 1 (2021): 81–102, https://doi.org/10.54629/jli.v18i1.736.

[20] Asa Pramudya Kristanto, "Perlindungan terhadap Data Pribadi dalam Aplikasi Digital sebagai Bentuk Perlindungan Hak Asasi Manusia," UNES Law Review 5, no. 3 (2023): 952–960, https://doi.org/10.31933/unesrev.v5i3.367.

immediate measures may continue for fraud or direct consumer threats, while administrative or disputed matters can be narrowed to specified products or features pending a decision.

A successful objection requires more than account reactivation. An erroneous decision may leave a violation record, lower performance scores, remove promotional access, retain funds, or influence later decisions. Redress should track all consequences. For ranking reduction it may include removing penalties, restoring product status, and correcting ranking data; for account restriction it may include reactivation, release of funds, restoration of trading features, and deletion of unsubstantiated violation records. Without internal data correction, harm persists after the appeal succeeds.

Operator liability may arise in contract or tort. Contractual liability applies when the operator fails to follow objection, notice, or restoration procedures in the electronic contract. Tortious liability applies when a decision violates a legal duty, merchant right, propriety, or due care and causes loss. Fault may lie not in an individual staff member but in system design, inaccurate data, overbroad parameters, inadequate supervision, or failure to correct a known error. The fact that an algorithm produced the measure does not eliminate responsibility because the operator selected, managed, and used the system for its business.[21]

Proof of loss remains difficult because the marketplace controls most relevant data. Withheld funds and canceled orders can be quantified, but losses from ranking reduction are harder because sales also depend on price, competition, season, and demand. Product position, impressions, visits, conversions, and performance before and after the measure can support causation, yet merchants may lack full access. Repressive protection should therefore require disclosure of dispute-specific data so that the right to redress is practical rather than merely formal.[22]

Existing rules provide a basis for complaints, correction, dispute resolution, and objections to automated decisions but do not specify human-review standards, individual reasons, resolution deadlines, adjustment of restrictions during review, or forms of restoration. Under Hadjon's theory, adequate repressive protection requires correction through a review capable of changing the decision, restoration of account, ranking, funds, and merchant data, and responsibility through compensation or dispute resolution. Without all three, a complaint channel remains an administrative procedure unable to balance the operator's power over a merchant's account and business.

Comparative and Doctrinal Calibration

A merchant-facing explanation need not disclose source code. What procedural fairness requires is enough decision-specific information to understand the factual trigger, the relevant rule or ranking factor, the period examined, and the route to challenge the outcome. This distinction between system transparency and decision transparency is central to avoiding both opacity and over-disclosure.

Where an automated restriction has significant economic effects, formal availability of a complaint channel is insufficient if review merely repeats the

[21] Addam Hartono Putra and Nabitatus Sa'adah, "Analisa Penggunaan Klausula Baku dalam Jual Beli," Notarius 17, no. 1 (2024): 142–154, https://doi.org/10.14710/nts.v17i1.44570.

[22] Danrivanto Budhijanto, Hukum Pelindungan Data Pribadi di Indonesia: Cyberlaw & Cybersecurity (Bandung: Refika Aditama, 2023).

automated output. Effective protection requires a reviewer who can reassess the evidence, consider contextual information supplied by the merchant, and restore ranking, account functionality, or financial position when the original decision is erroneous.

Table 1. Procedural Safeguards for Automated Marketplace Decisions

Stage	Required safeguard	Legal function
Before significant restriction	Notice and opportunity to clarify	Prevent avoidable error and permit contextual information
At the decision	Specific reasons and relevant data/factors	Make the decision intelligible and contestable
After objection	Substantive human review within a defined period	Provide an effective remedy rather than automated repetition
If error is found	Restoration of account/ranking and correction of affected records	Return the merchant as closely as possible to the lawful position
Throughout	Audit trail and proportional interim measures	Support accountability and prevent excessive economic harm

Table 1 translates the preventive/repressive protection framework into a decision lifecycle. It shows that legal protection is cumulative: general information about ranking cannot substitute for specific reasons, and a complaint channel cannot substitute for meaningful review and restoration.

CONCLUSION

Marketplace operators may legitimately use automated systems to manage ranking, integrity, fraud, and account compliance, but automation does not displace legal responsibility for the resulting business decision. Existing Indonesian rules provide important building blocks information duties, complaint mechanisms, correction rights, data-governance obligations, and emerging AI principles but safeguards remain fragmented at the level of an individual adverse decision. Adequate protection requires specific reasons, prior clarification where feasible, meaningful human review for significant restrictions, defined resolution periods, proportionate interim measures, and restoration when the decision is wrong. The article therefore reframes transparency as a procedural right attached to a consequential decision rather than a demand for full algorithmic disclosure.

Limitation and future research: because this article is normative, claims about implementation, prevalence, user behavior, institutional performance, or causal effectiveness require separate empirical study. Future research should test the proposed framework through systematic case-law coding, institutional data, stakeholder interviews, or comparative regulatory evaluation. The principal weakness is therefore not the total absence of rules but the incompleteness of procedures for individual decisions. Adequate protection must ensure that every ranking reduction and account restriction can be explained, challenged, corrected, restored, and legally accounted for.

REFERENCES

Acharya, Shibanee, Binay Das, Ashish Mishra, and Omkar Acharya. "Transparency and Explainability of Algorithms from a Consumer Law Perspective." Asian

Journal of Interdisciplinary Research (2025). https://doi.org/10.63363/aijfr.2025.v06i06.2652.

Benuf, Kornelius. "Hambatan Formal Penegakan Hukum Pidana terhadap Kejahatan Pencurian Data Pribadi." Majalah Hukum Nasional 51, no. 2 (2021): 261-279. https://doi.org/10.33331/mhn.v51i2.148.

Busch, Christoph. "From Algorithmic Transparency to Algorithmic Choice: European Perspectives on Recommender Systems and Platform Regulation." In The International Library of Ethics, Law and Technology (2023). https://doi.org/10.1007/978-3-031-34804-4_3.

Denisa, Andi Putri. "Sertifikat Keandalan Privasi sebagai Salah Satu Bentuk Perlindungan Data Pribadi dalam Transaksi E-Commerce." Jurnal Rechts Vinding 12, no. 2 (2023). https://doi.org/10.33331/rechtsvinding.v12i2.1286.

Fabbri, Matteo, and Ludovico Boratto. "Auditing Recommender Systems for User Empowerment in Very Large Online Platforms under the Digital Services Act." ACM (2025). https://doi.org/10.1145/3705328.3748074.

Fauzy, E., and Nabila Alif Radika Shandy. "Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi." Lex Renaissance 7, no. 3 (2022): 445-461. https://doi.org/10.20885/JLR.vol7.iss3.art1.

Hasibuan, Edi Saputra, and Elfirda Ade Putri. "Perlindungan Keamanan Atas Data Pribadi di Dunia Maya." Jurnal Hukum Sasana 10, no. 1 (2024): 70-83. https://doi.org/10.31599/sasana.v10i1.2134.

Iswandari, B. A. "Jaminan Atas Pemenuhan Hak Keamanan Data Pribadi dalam Penyelenggaraan E-Government Guna Mewujudkan Good Governance." Jurnal Hukum IUS QUIA IUSTUM 28, no. 1 (2021): 115-138. https://doi.org/10.20885/iustum.vol28.iss1.art6.

Jasmine, Alifia, Prita Amalia, and Helitha Novianty Muchtar. "Tanggung Jawab Platform Marketplace terhadap Penjualan Ponsel (Mobile Phone) Ilegal Berdasarkan Hukum Nasional." Masalah-Masalah Hukum 51, no. 4 (2022): 378-389. https://doi.org/10.14710/mmh.51.4.2022.378-389.

Kristanto, Asa Pramudya. "Perlindungan terhadap Data Pribadi dalam Aplikasi Digital sebagai Bentuk Perlindungan Hak Asasi Manusia." UNES Law Review 5, no. 3 (2023): 952-960. https://doi.org/10.31933/unesrev.v5i3.367.

Lie, Gunardi, Dylan Aldianza Ramadhan, and Ahmad Redi. "Komisi Independen Perlindungan Data Pribadi: Quasi Peradilan dan Upaya Terciptanya Right to Be Forgotten di Indonesia." Jurnal Yudisial 15, no. 2 (2022): 227-246. https://doi.org/10.29123/jy.v15i2.530.

Magrani, Eduardo, and Paula Guedes Fernandes da Silva. "The Ethical and Legal Challenges of Recommender Systems Driven by Artificial Intelligence." Law, Governance and Technology Series (2023). https://doi.org/10.1007/978-3-031-41264-6_8.

Niffari, Hanifan. "Perlindungan Data Pribadi sebagai Bagian dari Hak Asasi Manusia atas Perlindungan Diri Pribadi: Suatu Tinjauan Komparatif dengan Peraturan Perundang-Undangan di Negara Lain." Jurnal Yuridis 7, no. 1 (2020): 105-119. https://doi.org/10.35586/jyur.v7i1.1846.

Pasrija, Vatesh, and Supriya Pasrija. "Demystifying Recommendations: Transparency and Explainability in Recommendation Systems." International Journal for Research in Applied Science and Engineering Technology (2024). https://doi.org/10.22214/ijraset.2024.58541.

Priliasari, Erna. "Perlindungan Data Pribadi Konsumen dalam Transaksi E-Commerce." Jurnal Rechts Vinding 12, no. 2 (2023). https://doi.org/10.33331/rechtsvinding.v12i2.1285.

Putra, Addam Hartono, and Nabitatus Sa'adah. "Analisa Penggunaan Klausula Baku dalam Jual Beli." Notarius 17, no. 1 (2024): 142-154. https://doi.org/10.14710/nts.v17i1.44570.

Rahman, Faiz. "Kerangka Hukum Perlindungan Data Pribadi dalam Penerapan Sistem Pemerintahan Berbasis Elektronik di Indonesia." Jurnal Legislasi Indonesia 18, no. 1 (2021): 81-102. https://doi.org/10.54629/jli.v18i1.736.

Rani, M. "Pemahaman Masyarakat terhadap Ketentuan Hukum Jual Beli Online." Masalah-Masalah Hukum 51, no. 4 (2022): 355-366. https://doi.org/10.14710/mmh.51.4.2022.355-366.

Rosadi, Sinta Dewi, and Garry Gumelar Pratama. "Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital di Indonesia." Veritas et Justitia 4, no. 1 (2018): 88-110. https://doi.org/10.25123/vej.2916.

Sarkar, Malay. "Explainable AI in E-Commerce: Enhancing Trust and Transparency in AI-Driven Decisions." Information Technology & Engineering Journal 2, no. 1 (2024). https://doi.org/10.70937/itej.v2i01.53.

Sinaga, Erlina Maria Christin, and Mery Christian Putri. "Formulasi Legislasi Perlindungan Data Pribadi dalam Revolusi Industri 4.0." Jurnal Rechts Vinding 9, no. 2 (2020): 237-256. https://doi.org/10.33331/rechtsvinding.v9i2.428.

Wagner, Gerhard, and Horst Eidenmueller. "Down by Algorithms? Siphoning Rents, Exploiting Biases and Shaping Preferences—The Dark Side of Personalized Transactions." SSRN (2018). https://doi.org/10.2139/SSRN.3160276.

Wardani, Mutia Rahma, Joko Priyono, and Fifiana Wisnaeni. "Perlindungan Konsumen dalam Transaksi Elektronik melalui Instagram." Notarius 13, no. 2 (2020): 848-864. https://doi.org/10.14710/nts.v13i2.31183.

Winarsih, Irma, and Firya Oktaviarni. "Tanggung Jawab Penyedia Layanan Aplikasi Marketplace terhadap Konsumen dalam Transaksi Jual Beli Online di Provinsi Jambi." Zaaken: Journal of Civil and Business Law 2, no. 2 (2021): 349-367. https://doi.org/10.22437/zaaken.v2i2.11322.

Zilbershtein, Dina. "Fair and Transparent Recommender Systems for Advertisements." ACM (2025). https://doi.org/10.1145/3705328.3748755.