JUSTISI

Vol. 12, Issue. 2, May 2026
e-ISSN: 2686-0821, p-ISSN: 1979-7532
https://doi.org/10.33506/js.v12i2.5298
https://ejournal.um-sorong.ac.id/index.php/js/article/view/5298

Article History
Received: 12 Jan 2026
Reviewed: 02 Mar 2026
Accepted: 18 Apr 2026
Published: 24 Apr 2026

From Contractual Breach to Corporate Criminal Liability: Exploitation of Debtor Data by Account Officers in Indonesia

Afif Muhni[1]*, Muhammad Basri[2], Syarif Saddam Rivanie[3], Nuriyah Fara Muthia[4], Ulil Amri[5]

[1,2,3,4] Faculty of Law, Universitas Hasanuddin, Indonesia
[5] Faculty of Law, Universitas Mulawarman, Indonesia
* correspondence email : afif.muhni@unhas.ac.id

Abstract

The aim of this study is to analyze criminal liability for data exploitation committed by an AO in order to establish corporate liability against the receiving bank.
The method used in this study is a normative approach with legal and conceptual perspectives. This study analyzes the shift in the nature of illegality from a breach of contract to criminal data exploitation.
The novelty of this study demonstrates that recipient banks, which derive economic benefits from such illegal data, qualify as Beneficial Owners subject to corporate criminal liability under the doctrine of Vicarious Liability.
The results of this study indicate that the transfer of data without specific written consent constitutes a criminal offense under Article 65(2) of the Personal Data Protection Act.
Conclusion This study recommends the establishment of criminal policies based on Economic Analysis of Law, applying cumulative sanctions: imprisonment for individuals and substantial administrative fines for corporations. This step is crucial to eliminate the economic incentives behind data crimes and ensure legal certainty in the digital banking environment.
Keywords: Account Officers; Banking Crimes; Corporate Liability; Personal Data Protection

Abstrak

Tujuan Penelitian *ini untuk menganalisis tanggung jawab pidana atas eksploitasi data yang dilakukan oleh individu AO guna menegakkan tanggung jawab korporasi terhadap bank penerima.*
Metode Penelitian *yang digunakan adalah normatif dengan pendekatan hukum dan konseptual. Penelitian ini menganalisis pergeseran sifat ketidakabsahan dari pelanggaran kontrak menjadi eksploitasi data yang bersifat pidana.*
Kebaruan *penelitian ini menunjukkan bahwa bank penerima, yang memperoleh manfaat ekonomi dari data ilegal tersebut, memenuhi syarat sebagai Pemilik Manfaat yang tunduk pada tanggung jawab pidana korporasi berdasarkan doktrin Vicarious Liability.*
Hasil Penelitian *menunjukkan bahwa pemindahan data tanpa persetujuan tertulis yang spesifik merupakan suatu tindak pidana yang berdasarkan Pasal 65 (2) Undang-Undang Perlindungan Data Pribadi.*
Kesimpulan *penelitian ini merekomendasikan pembentukan kebijakan pidana berdasarkan Analisis Ekonomi Hukum, dengan menerapkan sanksi kumulatif: hukuman penjara bagi individu dan denda administratif besar bagi korporasi. Langkah ini sangat penting untuk*

menghilangkan insentif ekonomi di balik kejahatan data dan memastikan kepastian hukum dalam lingkungan perbankan digital.
Kata Kunci: *Account Officer; Tindak Pidana Perbankan; Pertanggungjawaban Korporasi; Perlindungan Data Pribadi*

1. INTRODUCTION

The Digital transformation in the banking sector has created space for customer data to become the most valuable economic commodity, often referred to as the "new gold mine" in the digital economy. In the fiduciary relationship between banks and customers, trust is the main foundation and the main product offered by banks to customers, whereby banks are obliged to maintain the confidentiality of personal information entrusted to them as part of prudential banking principles. However, fierce competition among financial institutions to increase market share and third-party funds often triggers business practices that disregard the ethics of privacy protection.[1]

Customer data are no longer merely viewed as administrative archives but have shifted to become strategic assets that are vulnerable to exploitation for commercial gains.[2] This phenomenon creates new vulnerabilities, where the protection of customer privacy is often sacrificed to achieve corporate profitability targets, which ultimately requires stricter legal intervention than conventional administrative regulations.

One common but problematic modus operandi in the banking industry is the phenomenon of employee transfers, particularly Account Officers (AOs), Relationship Officers (ROs), or marketing staff, which involves the transfer of customer data from the original bank to the destination bank.

In a practice known as employee "poaching," an AO is often recruited not solely for their individual competence but for their ability to bring with them a certain number or size of customer portfolios, often referred to as a pipeline in the banking world. This action involves copying, storing, and using customers' personal data, including identity, credit history, financial data, and asset-related data, without the valid consent of the customer concerned for the benefit of the new bank.

In addition, various forms of incentives are also offered by banks as referral programs to form a pipeline or customer-get-customer network that does not only come from one AO but also to other AOs from different banks, so that both the AO who processes the customer and the party who provides the referral receive incentives, which involves using customer data without the customer's consent or the knowledge of the principal or original bank. From a critical legal perspective, this incentive structure is not merely an aggressive marketing strategy, but a systemic legal circumvention that deliberately shifts criminal liability onto

[1] Hari Sutra Disemadi, "Urgensi Regulasi Khusus dan Pemanfaatan Artificial Intelligence dalam Mewujudkan Perlindungan Data Pribadi di Indonesia," *Jurnal Wawasan Yuridika* 5, no. 2 (2021): 177, https://doi.org/10.25072/jwy.v5i2.460.

[2] Abdul Risal, "Legal Protection for Debtors in Online Transactions: Evaluating Safeguards in E-Commerce," *Jurnal Hukum Bisnis Bonum Commune* 7, no. 2 (2024): 176–87, https://doi.org/10.30996/jhbbc.v7i2.11656.

individual actors while the corporation reaps the economic benefits.

This action often unknowingly opens up opportunities for individuals, in this case, customers, to become victims of personal data exploitation, which can lead to more serious criminal acts. Sometimes, this is only constructed as a labor dispute related to a breach of confidentiality clauses or trade secrets.[3] This weak legal construction is precisely the core legal problem addressed in this study, as it structurally fails to provide a deterrent effect because the economic benefits gained from acquiring new customers are far greater than the risks of civil or administrative sanctions that may arise.

The enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) marks a fundamental paradigm shift in Indonesia's information governance system. This regulation emphasizes that personal data protection is part of human rights and that violators can be subject to criminal sanctions, and no longer merely a matter of private law.[4]

Article 65 (2) of the Personal Data Protection Law expressly prohibits anyone from unlawfully disclosing personal data that does not belong to them, with serious criminal penalties as stipulated in Article 67 (2). The presence of this regulation changes the legal liability landscape for Account Officers who misuse customer data. What was once considered a marketing and economic strategy for both AO as individuals and banks as corporations has now metamorphosed into a criminal offense.[5]

This demands an urgent and in-depth reevaluation of banking practices that tolerate the exploitation and use of customer data across institutions without legal procedures to protect customers. Although a legal framework is in place, complexities arise in the application of criminal sanctions due to the conflict between the PDP Law and the Banking Law. The Banking Law tends to emphasize banking secrecy as protection for the interests of banks, while the PDP Law places full control in the hands of the data subject or customer.[6]

In the context of data transfer by AO, customers often voluntarily provide data because of a personal relationship (trust-based relationship) with the AO, not through the bank principal institution, or because they are only informed after another bank or AO from the original bank contacts them.

However, legally, consent for data processing is given by customers to the Bank as the

---

[3] Afif Muhni dkk., "MEDICOLEGAL PENGGUNAAN KADAVER MANUSIA UNTUK BEDAH ANATOMI MEDIS DAN TRANSPLANTASI ORGAN MEDICOLEGAL USE OF HUMAN CADAVERS FOR MEDICAL ANATOMICAL SURGERY AND ORGAN TRANSPLANTATION," *Jurnal Hukum dan Etika Kesehatan* 5, no. 2 (2025), https://doi.org/10.30649/jhek.v5i2.237.

[4] Mas Putra Zenno Januarsyah dkk., "The Renewal Policy of the Adultery Concept in Article 411 of the Law Number 1 of 2023 on the Indonesian Criminal Code," *Padjadjaran Jurnal Ilmu Hukum* 10, no. 1 (2023): 1–16, https://doi.org/10.22304/pjih.v10n1.a1.

[5] Viktoriia Vovk dkk., "Financial monitoring in the bank as a market instrument in the conditions of innovative development and digitalization of economy: Management and legal aspects of the risk-based approach," *International Journal of Industrial Engineering and Production Research* 31, no. 4 (2020): 559–70, https://doi.org/10.22068/ijiepr.31.4.559.

[6] Rodes Ober Adi Guna Pardosi dan Yuliana Primawardani, "Perlindungan Hak Pengguna Layanan Pinjaman Online dalam Perspektif Hak Asasi Manusia," *Jurnal HAM* 11, no. 3 (2020): 353, https://doi.org/10.30641/ham.2020.11.353-368.

data controller, not to the AO as an individual.[7] This consent should be requested from customers at the outset, not later. The ambiguity in the interpretation of "unlawful" in the context of employment relationships is often exploited to avoid criminal charges, requiring a sharp dogmatic analysis to place this case in the proper context of criminal law.

Furthermore, law enforcement in this case cannot be imposed solely on individuals or AOs but must also touch on the aspect of corporate criminal liability. The new bank that accepts the transfer of the AO and its customer data is in the position of being the beneficial owner of the crime.[8] If the new bank does not implement due diligence procedures and instead provides incentives for the AO's success in bringing the customer database from the old bank, the corporation can be considered to have facilitated the crime. The Economic Analysis of Law approach shows that criminal sanctions against individuals will not be effective as long as corporate incentives to obtain customer data instantly remain.[9] Therefore, penal policies must not only punish perpetrators in the field but also sever the chain of economic benefits enjoyed by corporations through illegal means.

Based on this description, this study has a high urgency in filling the gap in the legal literature that specifically discusses the interaction between criminal law, data protection, and banking employment practices. Previous studies such as Amilah (2024) have mostly focused on the civil or administrative aspects of consumer protection[10] and only discussed legal regulations, this article touching on the aspect of criminalization after the enactment of the Personal Data Protection Law. There is also little comprehensive discussion on the typology or forms of crime, especially in the banking sector.

Another studies by Uly and Dona (2025) analyzed the effectiveness of the Personal Data Protection Law in providing norms for consumer data misuse in the fintech sector,[11] This article then focuses on the misuse of personal data specifically to banking customers, particularly in the lending sector, which causes losses to customers and existing banks while on the other hand, provides benefits to individuals and other banking companies.

The protection of debtor customer data and information through banking secrecy rules remains relevant because the protection of personal data is a human right and has financial

---

[7] Maria Palazzo dkk., "From strategic corporate social responsibility to value creation: an analysis of corporate website communication in the banking sector," *International Journal of Bank Marketing* 38, no. 7 (2020): 1529–52, https://doi.org/10.1108/IJBM-04-2020-0168.

[8] Edmon Makarim, "Privacy and Personal Data Protection in Indonesia: The Hybrid Paradigm of the Subjective and Objective Approach," dalam *Data Protection Around the World: Privacy Laws in Action*, ed. oleh Elif Kiesow Cortez (T.M.C. Asser Press, 2021), https://doi.org/10.1007/978-94-6265-407-5_6.

[9] Víctor Gómez MARTIN, "The Criminal Liability of the Compliance Officer: An Approach Through Several Hard Cases," *Journal of Penal Law & Criminology*, advance online publication, 29 Juni 2020, https://doi.org/10.26650/jplc2020-0010.

[10] Amilah Fadhlina dkk., *Perlindungan Data Pribadi Nasabah dalam Transaksi Central Bank Digital Currency (CBDC) dalam Rupiah Digital*, 7, no. 1 (2024), https://doi.org/10.31933/unesrev.v7i1.

[11] Uly Alfinda Salsabila dan Dona Budi Kharisma, "Mechanism Law Enforcement on Fintech Personal Data Abuse Post -Law Number 27 of 2022 Concerning Personal Data Protection," dalam *Proceedings of the International Conference on Democracy and National Resilience 2025 (ICDNR 2025)*, vol. 981, ed. oleh Sunny Ummul Firdaus dkk., Advances in Social Science, Education and Humanities Research (Atlantis Press SARL, 2025), https://doi.org/10.2991/978-2-38476-529-4_11.

value. Malaysia and the United Kingdom provide more adequate protection for debtor customer data than Indonesia, which limits banking secrecy rules to depositors only.[12]

This study examines the interaction between criminal law, data protection, and employment practices in the banking sector. It addresses the lack of previous studies that focused only on civil or administrative aspects of consumer protection, the lack of criminalization aspects after the enactment of the Personal Data Protection Law (PDP Law), and the specific typology of data crimes in the banking industry. As a contribution, this article comprehensively analyzes the legal construction of criminal liability for account officers (AOs) and banking corporations, while reconstructing the ideal criminal policy formula to eradicate customer data exploitation in order to ensure legal certainty and protect privacy rights in the Indonesian banking ecosystem.

The novelty of this research reveals that recipient banks that derive economic benefits from illegal data migration legally qualify as Beneficial Owners who are subject to corporate criminal liability through the doctrine of Vicarious Liability. The recommendation is to applying cumulative sanctions in the form of imprisonment for individuals (AO) and large administrative fines for corporations to eliminate the economic incentives behind such data crimes.

This article aims to analyze the legal construction of criminal liability for account officers and banking corporations involved in the exploitation of customer data. Through a legal-normative approach, this study reconstructs the ideal penal policy formula to combat the crime of misusing someone's personal data for personal gain or the gain of others and to the detriment of service users in the banking ecosystem, as well as to ensure legal certainty and protect the privacy rights of banking customers in Indonesia.[13]

2. METHOD

This study employs a normative legal research method focusing on the dogmatic analysis of positive law. It utilizes statutory and conceptual approaches to examine Law No. 27 of 2022 (PDP Law) and related banking regulations. To elevate the analysis beyond descriptive observation, this study applies a deductive legal reasoning method. Furthermore, systematic and teleological interpretative methods are utilized to resolve the conflict of norms between the rigid bank secrecy regime and modern data protection principles, applying the lex specialis derogat legi generali principle. Primary and secondary legal materials are qualitatively analyzed to bridge the gap between theoretical criminal provisions and the operational reality of corporate banking crimes.

[12] Erma Defiana Putriyanti, et.al., *The Relevance Of Protecting Debtor Customer Data And Information Through Bank Secrecy: A Comparative Study In Indonesia, Malaysia And The United Kingdom*, 04, no. 04 (2024): 347-366. https://doi.org/10.63922/ajmesc.v4i04.1087

[13] Dewi Fatmala Putri dan Widya Ratna Sari, "ANALISIS PERLINDUNGAN NASABAH BSI TERHADAP KEBOCORAN DATA DALAM MENGGUNAKAN DIGITAL BANKING," *Jurnal Ilmiah Ekonomi dan Manajemen* 1, no. 4 (2023): 173–81, https://doi.org/10.61722/jiem.v1i4.331.

3. DISCUSSION

3.1. Legal Deconstruction of Customer Data Exploitation: From Contractual Violations to Individual Criminal Liability

The legal framework governing customer data in Indonesia's banking ecosystem has undergone a fundamental shift following the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law). Previously, under Law No. 10 of 1998 on Banking, customer data was constructed in a limited manner as part of Bank Secrecy, the ownership of which tended to be associated with intellectual property or trade secrets belonging to banking corporations.[14]

However, the PDP Law reconstructs this paradigm by emphasizing that personal data is a constitutional right inherent to the data owner, so that its processing must be based on a strict legal basis. In the context of Account Officers (AOs) or Relationship Officers (ROs) who transfer customer data to new banks, the nature of the violation is transformed from a mere contractual breach against the old bank and customers to a criminal offense.[15]

The act of controlling customer data by an AO who has no employment relationship with the original bank can no longer be viewed as a mere labor dispute but rather as a violation of personal data integrity, as stipulated in Article 4, Paragraph (2) of the PDP Law.[16]

Therefore, the ultimum remedium approach in criminal law becomes relevant when civil mechanisms are deemed inadequate to restore violated privacy rights. An analysis of the actus reus element in Article 65 (2) of the PDP Law, which states that everyone is prohibited from unlawfully obtaining, collecting, using, or disclosing personal data that does not belong to them with the intention of benefiting themselves or others, which could result in harm to the subject of the personal data.[17]

Therefore, this article needs to be interpreted systematically. An AO has legal access to customer data while still an active employee of a banking company, but the legality of such access is immediately void when the employment relationship ends or when the data used outside the original purpose (purpose limitation) of data collection.[18] From a dogmatic criminal law perspective, it is imperative to clearly distinguish between the elements of acting "without authority" and acting "unlawfully". During their active employment, an Account Officer technically possesses the legitimate "authority" to access and process customer data for internal banking operations. Consequently, the core of the criminal offense in data migration by an AO does not lie in unauthorized access or hacking (acting "without authority"). Instead,

---

[14] M. B. Taylor, "Counter corporate litigation: Remedy, regulation, and repression in the struggle for a just transition," *Sustainability*, 2021.

[15] Uswatun Hasanah dkk., "The Phenomenon of Personal Data as a 'Pseudo Guarantee' In Fintech : Legal or Not?," *JUSTISI* 11, no. 3 (2025): 763–80, https://doi.org/10.33506/js.v11i3.4247.

[16] Valentina Ancillia Simbolon dan Vishnu Juwono, "Comparative Review of Personal Data Protection Policy in Indonesia and The European Union General Data Protection Regulation," *Publik (Jurnal Ilmu Administrasi)* 11, no. 2 (2022): 178, https://doi.org/10.31314/pjia.11.2.178-190.2022.

[17] Putu Angga dkk., *URGENSI KONSEP DAN PRINSIP MENGENAI PERLINDUNGAN DATA PRIBADI DI INDONESIA* (t.t.).

[18] Pala Sari dan Pariaman Ompusunggu, "Analisis Hukum Terhadap Perlindungan Data Pribadi Nasabah dalam Layanan Perbankan Digital di Indonesia," dalam *Aufklarung: Jurnal Pendidikan*, vol. 3, no. 3 (2023).

the criminality materializes when the AO extracts, uses, or discloses this data for the commercial benefit of a rival bank. This specific action transcends a simple breach of internal policy; it constitutes a materially "unlawful" (melawan hukum) act, as it fundamentally violates the purpose limitation principle and infringes upon the privacy rights protected by Article 65 (2) of the PDP Law.

Account Officer often argue that the transfer of data is based on verbal permission or the personal closeness of the customer, which is considered a form of consent. However, from a legal standpoint, this argument is logically flawed because it obscures the distinction between personal and legal relationships. The consent to data processing signed by customers on the account opening form is consent given to the Bank as the Data Controller, not to the AO as an individual [19].

The AO's position is only valid as a data processor in the capacity of an employee of a banking company who does not have the autonomous right to transfer data to other entities without the written and specific consent of the customer regarding the use of the data.[20] The modern data protection doctrine requires explicit, informed, and specific consent. The AO's unilateral claim regarding customer consent without authentic evidence is a violation of the principles of transparency and accountability mandated by Article 35 of the PDP Law.

From a mens rea (mental state) perspective, the AO's actions in bringing customers clearly had a strong economic motive, namely, to meet lending and funding targets at the new bank to obtain bonuses or incentives in the form of cash bonuses, vacation trips, and even promotions. This intentional intent (dolus) is qualified as intentional with the aim (opzet als oogmerk) of benefiting oneself or others unlawfully, as referred to in Article 67 (2) of the PDP Law. The element of "benefiting oneself" is aggravating because it shows that the privacy violation was intended to obtain financial gains.[21]

In economic criminal law theory, the profit-oriented motive in the illegal use of data reinforces the urgency of imposing criminal sanctions of imprisonment and fines, considering that administrative sanctions alone will not eliminate the potential gains obtained by perpetrators from the misuse of such data.[22] There is a potential conflict between the obligation to maintain bank secrecy under Banking Law and the prohibition on data disclosure under the PDP Law.

However, based on the principle of lex specialis derogat legi generali, the PDP Law has a more specific position in regulating personal data management than the Banking Law, which focuses more on financial system stability.[23] If an AO who leaks customer data can be charged

[19] Wardah Yuspin dkk., "Personal Data Protection Law in Digital Banking Governance in Indonesia," *Studia Iuridica Lublinensia* 32, no. 1 (2023): 99–130, https://doi.org/10.17951/sil.2023.32.1.99-130.

[20] Galang Surya Mahendra, "Perlindungan Hukum Terhadap Korban Yang Data Pribadi Passportnya Tersebar Akibat Kelalaian Pemerintah," *Terang : Jurnal Kajian Ilmu Sosial, Politik dan Hukum* 1, no. 3 (2024): 104–11, https://doi.org/10.62383/terang.v1i3.382.

[21] Yuspin dkk., "Personal Data Protection Law in Digital Banking Governance in Indonesia."

[22] Muhammad Basri dan Afif Muhni, "Assets Depreciation as an Economic Challenge Assets Recovery from Corruption," dalam *Pakistan Journal of Criminology*, vol. 16, no. 04 (t.t.).

[23] Komang Suputra Kurniawan dan I. Gede Agus Kurniawan, "The Limitations of Lex Generalis: Analyzing the

under Article 47 of the Banking Law, which regulates bank secrecy offenses, the PDP Law now offers sharper criminal instruments that focus on the rights of data subjects, not just the interests of banks.[24]

The legal construction in the PDP Law allows prosecution to be limited not only to financial data (balances, deposits, cash flow), but also to customer profiles, contacts, and demographic data, which are often exploited for the marketing interests of new banks.[25] This provides legal certainty that customer data protection is comprehensive and not compartmentalized within the banking sector. In examining the criminal acts committed by the Account Officer, it is important to review the violation of the principles of personal data processing as stipulated in Article 16 (2) of the Personal Data Protection Law.

"(2) The processing of Personal Data referred to in paragraph (1) shall be carried out in accordance with the principles of Personal Data protection, including: The collection of Personal Data shall be limited and specific, legally valid, and transparent; The processing of Personal Data shall be carried out in accordance with its purpose; Personal Data processing shall be carried out by guaranteeing the rights of the Personal Data Subject; Personal Data processing shall be carried out accurately, completely, without deception, up-to-date, and accountable; Personal Data processing is carried out by protecting the security of Personal Data from unauthorized access, unauthorized disclosure, unauthorized alteration, misuse, destruction, and/or loss of Personal Data; Personal Data processing is carried out by notifying the purpose and activities of processing, as well as failures in Personal Data protection; Personal Data is destroyed and/or deleted after the retention period ends or based on the request of the Personal Data Subject, unless otherwise specified by law; and Personal Data processing is carried out responsibly and can be clearly proven."

One of the fundamental principles that has been violated is the principle of purpose limitation, which mandates that data may only be collected for specific, explicit, and legitimate purposes, and may not be further processed in a manner incompatible with those purposes.[26] When customer data are collected by the originating Bank A (Bank A), the specific purpose is for banking administration, such as opening accounts and analyzing creditworthiness at that institution.[27]

When AO transferred the data to Bank B, there was a radical deviation from the purpose of processing, namely, for the sake of prospects and business processes at another

Readiness of the GDPR and PDP Law for AI-Based Facial Recognition Technology," *SIGn Jurnal Hukum* 7, no. 2 (2025): 838–52, https://doi.org/10.37276/sjh.v7i2.533.

[24] Abraham Ethan Martupa dkk., "Strengthening Personal Data Protection, Cyber Security, and Improving Public Awareness in Indonesia: Progressive Legal Perspective," *International Journal of Business, Economics and Social Development* 2, no. 4 (2021): 143–52.

[25] Jessenia Hayfa dkk., *Jurnal Penelitian Ilmu-Ilmu Sosial Implementation of Data Protection Authority (DPA) in Indonesia: The Urgency of Legal Protection of Customer's Personal Data in E-Banking Service Transactions*, vol. 5, no. 1 (2024).

[26] Acep Rohendi dan Dona Budi Kharisma, "Personal data protection in fintech: A case study from Indonesia," *Journal of Infrastructure, Policy and Development* 8, no. 7 (2024), https://doi.org/10.24294/jipd.v8i7.4158.

[27] Nikita Kozodoi dkk., "Fairness in credit scoring: Assessment, implementation and profit implications," *European Journal of Operational Research* 297, no. 3 (2022): 1083–94, https://doi.org/10.1016/j.ejor.2021.06.023.

corporation. Violation of this principle is not merely maladministration but rather a constitutive element that reinforces the element of "unlawfulness" in the criminal offense under Article 65, paragraph (2) of the PDP Law.

In modern criminal law doctrine, violations of the main principles of data protection can be constructed as inherently criminal acts (mala in se) that are punishable because they violate the autonomy of the data subjects.[28] A clear demarcation must be made between the concept of "theft" in the conventional Criminal Code and "illegal data disclosure" in the PDP Law.

In Law No. 1 of 2023, concerning the Criminal Code, the object of theft (Article 476) requires a physical transfer of control. However, in the context of electronic data, the data taken by the AO is often only a copy, either in physical or electronic form, while the original data remains in the possession of the personal data owner or is stored on the original bank's server. Therefore, the application of ordinary theft articles often reaches a dead end because of the intangible and non-rivalrous characteristics of the data.[29]

The PDP Law fills this gap by focusing on unlawful or unauthorized disclosure rather than on the loss of data from the original owner. AO's action of "opening" customer data to a new banking system, even though the original data were not lost, is classified as a criminal act because the essence of personal data protection is confidentiality and access control, not merely physical possession of objects.[30]

This is in line with international jurisprudence and the General Data Protection Regulation (GDPR) standards adopted by the PDP Law, which protects data integrity from unauthorized access.[31] Further dogmatic analysis touches on the power relationship between AO and customers after the end of the employment relationship. There is a legal misconception that the obligation to maintain data confidentiality ceases immediately when an AO's employment contract ends.

The obligation to keep customer data confidential is a post-employment obligation that is lifelong as long as the data has not become a legitimate public domain. From a criminal law perspective, the AO's status as a former employee does not negate the unlawful nature of their use of data obtained while still in office. The use of data obtained from a previous position for personal gain in a new workplace constitutes a breach of trust that can increase criminal penalties. The PDP Law does not limit the legal subject to active employees, but rather "every person," which includes former employees who illegally exploit their residual access to information.[32]

---

[28] Literasi &. Wawasan dkk., *HUKUM PIDANA INDONESIA* (2025).

[29] Viani B. Djeundje dkk., "Enhancing credit scoring with alternative data," *Expert Systems with Applications* 163 (Januari 2021), https://doi.org/10.1016/j.eswa.2020.113766.

[30] Atmari Atmari dkk., "Legal Protection of Resigning Workers' Right Over Separation Pay Compensation in Justice Perspective," *International Journal of Multicultural and Multireligious Understanding* 7, no. 8 (2020): 713, https://doi.org/10.18415/ijmmu.v7i8.1998.

[31] Hieronymus Febrian Rukmana Aji dan Abraham Ferry Rosando, "PERLINDUNGAN HUKUM TERHADAP HASIL FOTO PRIBADI YANG DIGUNAKAN ORANG LAIN DI INSTAGRAM," dalam *Jurnal Hukum Bisnis Bonum Commune*, vol. 2 (t.t.).

[32] Kukun Abdul Syakur Munawar dkk., "Reversed Burden of Proof in Online Gambling Fraud: Consumer Protection Based on Islamic Law in West Java," *Jurnal Hukum Bisnis Bonum Commune* 8, no. 2 (2025): 243–61,

From a criminal evidence perspective, digital traces are crucial in prosecuting AO. The data transfer process usually leaves audit trails on the originating bank's system, such as download logs, last data access, printer usage with the last scanned or printed document, or transmission to the AO's personal device before resigning.[33] Criminal Procedure Law No. 20 of 2025 recognizes electronic evidence as valid evidence, as stipulated in Article 235, paragraph (1), which is also accommodated in the PDP Law and the ITE Law.

In the context of the element of "intent" (opzet), this can be proven through AO's systematic behavior patterns, such as downloading large volumes of data that are unreasonable prior to resignation or the existence of electronic communication with the new bank regarding customer offers.[34] Various objective patterns negate the AO's defense of claiming ignorance or negligence (culpa) and further confirm the existence of mens rea to exploit data for economic gain.

From the perspective of the Economic Analysis of Law doctrine, the presence of law must be efficient or able to reduce costs and prevent social losses (Muhammad Basri & Afif, 2024). If the AO's actions are only subject to civil or administrative sanctions, then the "cost" of committing the crime is lower than the benefits obtained in the form of bonuses and commissions at the new bank.

Criminal sanctions in the PDP Law include imprisonment and fines of up to billions of rupiah, which serve as instruments for changing behavior and suppressing crime. This is important considering that banking customer data is highly sensitive and, if leaked, can be used for further crimes such as phishing or other fraud. Therefore, legal protection must be preventive and repressive to the maximum extent possible.[35]

In conclusion, it can be concluded that the criminalization of account officers under the PDP Law is not excessive or over-criminalization, but rather a necessary legal harmonization to respond to the dynamics of white-collar crime in the digital era.

The construction of articles in the PDP Law covers the entire spectrum of customer data transfer modus operandi, ranging from illegal collection and unauthorized disclosure to exploitation for economic gain. Consistent law enforcement against AO is the first step, but this analysis is incomplete without touching on the intellectual actors or the main beneficiaries of this. The next discussion focuses on the criminal liability of corporations as entities that stimulate these illegal practices through aggressive recruitment policies.[36]

---

https://doi.org/10.30996/jhbbc.v8i2.12886.

[33] A. Muhni, *Strategi Penegakan Hukum Tindak Pidana Pencucian Uang pada Lembaga Perbankan* (repository.unhas.ac.id, 2020).

[34] Jia Luo dkk., "Design and Implementation of an Efficient Electronic Bank Management Information System Based Data Warehouse and Data Mining Processing," *Information Processing and Management* 59, no. 6 (2022), https://doi.org/10.1016/j.ipm.2022.103086.

[35] Nuriyah Fara Muthia dkk., "Dual use satellites in the Ukraine conflict: The dilemma between state sovereignty and the principle of non-militarization of outer space," *Priviet Social Sciences Journal* 5, no. 10 (2025): 146–55, https://doi.org/10.55942/pssj.v5i10.715.

[36] Alfa Dera dan Fauzie Yusuf Hasibuan, "Dominus Litis Restorative Model: Reconstruction of the Role of the Prosecutor in Criminal Procedure Law Against Perpetrators with Mental and/or Intellectual Disabilities," dalam *Advances in Social Humanities Research*, vol. 3, no. 7 (2025).

Despite the robust dogmatic construction of actus reus and mens rea under the PDP Law, real enforcement and judicial practice in Indonesia face significant hurdles. In actual judicial practice, law enforcement agencies often default to utilizing the Electronic Information and Transactions (ITE) Law or treating data theft by AOs as conventional trade secret disputes under civil law. This is primarily because the PDP Law is relatively new and lacks mature jurisprudence. Furthermore, originating banks are often reluctant to report data breaches due to reputational risks (bank runs), creating an enforcement vacuum. Therefore, a progressive shift in prosecutorial strategy is urgently needed to establish strong jurisprudence applying Article 65 (2) of the PDP Law in the banking sector.

3.2. Corporate Responsibility Through Vicarious Liability and the Doctrine of Beneficial Ownership Regarding Banking Personal Data Crimes

Account Officers (AOs) involved in criminal acts of customer data exploitation often fail to address the root causes of structural problems within the banking industry. In the context of criminology, the actions of AOs to transfer customer data from old banks to new banks rarely stand alone as individual initiatives; rather, they are a response to the performance targets imposed by the corporations they work for. Therefore, the doctrine of Vicarious Liability is relevant.

This doctrine asserts that corporations can be held criminally liable for crimes committed by their employees or staff, as long as the actions are carried out within the scope of their work or are intended to benefit the corporation.[37] In an aggressive banking competition ecosystem, new banks that accept AO along with their customer portfolios or databases cannot escape legal responsibility by hiding behind the excuse that data theft is an act of individuals. This is because new banks consciously encourage and stimulate deviant behavior to accumulate third-party funds.[38]

In Indonesia, the legal basis for prosecuting corporations for criminal acts is strictly regulated by Supreme Court Regulation (PERMA) Number 13 of 2016 concerning Procedures for Handling Corporate Criminal Cases. Article 4, paragraph (2) of PERMA provides clear parameters regarding when a corporation can be held liable, namely, if the corporation obtains profit or benefit from a criminal act or if the corporation allows a criminal act to occur without making any effort to prevent it.

In the case of customer data migration, the new bank only meets these liability criteria when management accepts account-opening applications based on data obtained illegally. The new bank management, which turned a blind eye to the source of customer data brought in by the new AO, qualifies as negligent. This is especially true if they provided incentives or promises during the initial interview with prospective employees, promising benefits, even to the point of stating how much of the portfolio or database could be taken over from the

[37] Siti Mariyam dkk., "Corporate Liability of Ride-Hailing Services: An Analysis of Partnership Legal Fiction and the Reconstruction of Passenger Safety Regulation," *SIGn Jurnal Hukum* 7, no. 2 (2025): 803–20, https://doi.org/10.37276/sjh.v7i2.529.

[38] Hartono Tasir Irwanto dkk., "Ethics and Law of Personal Data Protection for Smartwatches in the Healthcare Sector," *SIGn Jurnal Hukum* 7, no. 1 (2025): 421–36, https://doi.org/10.37276/sjh.v7i1.489.

previous bank.

Thus, the element of corporate negligence has been fulfilled, not because the corporation had malicious intent in running the company, but through the attribution of negligence by management or permissive policies towards legal violations.[39] The application of vicarious liability in this case is also in line with the mandate of Article 70 of the Personal Data Protection Law (PDP Law), which explicitly stipulates that criminal penalties can be imposed on corporations. However, the biggest challenge arises in proving the causal relationship between a bank's recruitment policy and data theft. Using the identification theory, AO's actions can be considered corporate actions if they are approved or ordered by the brain of the corporation, such as the branch manager or directors.[40]

When the manager recruitment stage requires prospective AOs to bring a customer portfolio database as a condition of acceptance or salary negotiation to increase third-party funds to the new bank, malicious intent (mens rea) has shifted from the individual to the institution. This construction confirms that the new bank is not merely a passive vessel but an intellectual perpetrator (intellectual dader) that drives data crime through the instrument of employment.[41]Furthermore, the analysis must touch on the concept of the beneficial owner in economic crimes.[42] In the customer data transfer scheme, the economic benefits obtained by the AO in the form of bonuses, commissions, and job promotions are only a small part of the total profit enjoyed by the new bank.

The new bank enjoys long-term benefits in the form of interest spread profits, administrative fees, and liquidity from customer funds that have been successfully acquired or taken over without spending more on marketing costs.[43] Therefore, placing the new bank as a subject of criminal law is a manifestation of the principle of Cuis est commodum, eius est incommodum, whoever benefits bears the burden of responsibility.

Using the Economic Analysis of Law approach to assess the effectiveness of sanctions, perpetrators of crimes such as banking corporations are rational actors who weigh the costs and benefits of recruiting AO. Imprisonment imposed on AOs is ineffective in deterring such crimes due to the principal-agent problem.

---

[39] Afif Muhni dkk., "Integration of Anti-SLAPP in the Reform of the Indonesian Criminal Procedure Code in an Effort to Protect Human Rights," *SIGn Jurnal Hukum* 7, no. 1 (2025): 437–53, https://doi.org/10.37276/sjh.v7i1.485.

[40] Renny Ariyanny dkk., "Disgorgement of Profits: An Alternative Solution to Stolen State Assets' Recovery from Corporate Financial Crimes," *Hasanuddin Law Review* 9, no. 2 (2023): 139–54, https://doi.org/10.20956/halrev.v9i2.4622.

[41] Rachmadi Usman, "Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) Exploration of nexus between legal liability and corporate fraud: where do business laws and criminology converge?," *International Journal of Criminal Justice Sciences. Criminal Justice Sciences (IJCJS)-Official Journal of the South Asian Society of Criminology and Victimology* 18, no. 1 (t.t.): 232–43, https://doi.org/10.5281/zenodo.4756251/IJCJS.

[42] Agustianto, "Pentingnya Transparansi Beneficial Ownership Oleh Korporasi," *JUSTISI* 8, no. 2 (2019): 108–18, https://doi.org/10.33506/js.v8i2.1678.

[43] Silvia Zorzetto, "Better Regulation, Cost-Benefit Analysis and Evidence Based Legal Design: A Critical Inquiry," dalam *Developments in Law and Economics in the Italo-Iberoamerican Context*, ed. oleh Betzabé and Sotomayor Trelles José Enrique and Ferraro Francesco Zorzetto Silviaand Marciani Burgos (Springer Nature Switzerland, 2025), https://doi.org/10.1007/978-3-032-03317-8_7.

As long as new banks (principals) continue to provide high economic incentives in the form of bonuses and promotions for AOs (agents) who bring customer databases, the criminal punishment of one AO will only be replaced by another AO who is willing to take risks and use different techniques to deceive both the old banks and law enforcement.[44] Therefore, the criminal law approach needs to shift from being merely retributive to a utilitarian approach that aims to stop the economic incentive structure through massive fines and administrative penalties.

The ideal criminalization strategy applies the principle of following the profit. New banks or corporations that derive financial benefits from illegally obtained customer data must have their profits confiscated (disgorgement of profits).[45] From an administrative perspective, criminal law can impose penalties in the form of revocation or restriction of licenses, such as operational and marketing licenses, to provide a real deterrent.[46] Other additional penalties can include the announcement of court decisions to the general public, which then has the effect of social and reputational sanctions from the community.

The ideal formulation of penal policy for combating crime is through a dual sanction mechanism. This system allows judges to impose not only criminal sanctions (which are punitive) but also regulatory measures (which are preventive and educational). The AO is subject to imprisonment for moral responsibility for privacy violations. Corporations are subject to fines and the obligation to provide restitution to customers or the originating bank. Restitution is important as a form of restorative justice, given that the losses suffered by customers as a result of their data being exploited and commercialized without their knowledge of the data owner are often immaterial. Meanwhile, the originating bank risks losing its portfolio and eroding its profits as a result of unfair business operations by the agent.

The analysis shows that combating customer data exploitation by account officers cannot be done by relying solely on conventional criminal provisions against individuals. A paradigm shift in law enforcement is needed towards a functional approach that combines Vicarious Liability to prosecute corporations and an Economic Analysis of Law in formulating effective sanctions.

The ideal formulation of penal policy is a combination of imprisonment for individual perpetrators, fines for corporate beneficiaries (Beneficial Owners), and administrative sanctions. With this punishment scheme, it is hoped that the Personal Data Protection Law can be more effective in protecting the privacy rights of financial service users and creating an ethical, fair, and legally certain climate for banking competition in Indonesia. From an implementation perspective, prosecuting a recipient bank as a 'Beneficial Owner' requires operational proof of corporate complicity. Operationally, a recipient bank qualifies as a

[44] Muhammad Al Ikhwan Bintarto Sayang Bidul Zaid dkk., *Analysis of Economic Analysis of Law Principle In Purchase Fuel By Application (Study of MyPertamina)* (t.t.).

[45] Ariyanny dkk., "Disgorgement of Profits: An Alternative Solution to Stolen State Assets' Recovery from Corporate Financial Crimes."

[46] Sahur Ramsay, "Pertanggungjawaban Direksi atas Kerugian Perseroan dalam Perusahaan Grup," *JUSTISI* 8, no. 3 (2022): 209–23, https://doi.org/10.33506/jurnaljustisi.v8i3.1823.

beneficial owner when the illicitly migrated data is systematically integrated into its banking system to generate new credit portfolios or third-party funds. To enforce this practically, the Financial Services Authority (OJK) and investigators must implement forensic audits tracking anomalous surges in customer acquisition linked to newly recruited AOs. By employing a "follow the data" approach-similar to anti-money laundering tracing-authorities can operationalize the vicarious liability doctrine, moving beyond punishing low-level agents to effectively sanctioning the corporate structure that monetizes the exploitation

4. CONCLUSION

Conclusion Based on the analysis conducted, that the exploitation of customer data by Account Officers (AOs) in the practice of bank transfers has undergone a legal transformation from mere contractual default to a pure criminal offense under Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). Dogmatically, the element of "unlawfully disclosing personal data that does not belong to them" in Article 65 (2) of the PDP Law is fulfilled when the AO migrates data from the original bank to the new bank without specific written consent from the customer. Thus, the use of such data for commercial purposes at the new bank constitutes a form of abuse of access and a violation of the principle of purpose limitation, which is punishable by criminal sanctions and penalties. The Economic Analysis of Law approach emphasizes that imprisoning AO is not an effective deterrent as long as economic incentives for corporations remain open. Therefore, the application of massive criminal fines and administrative sanctions, such as license revocation and others against corporations, is the most rational penal instrument to eliminate the economic motive behind the illegal commercialization of customer data.

REFERENCE

Agustianto. "Pentingnya Transparansi Beneficial Ownership Oleh Korporasi." *JUSTISI* 8, no. 2 (2019): 108–18. https://doi.org/10.33506/js.v8i2.1678.

Angga, Putu, Pratama Sukma, dan Edmon Makarim. *URGENSI KONSEP DAN PRINSIP MENGENAI PERLINDUNGAN DATA PRIBADI DI INDONESIA*. t.t.

Ariyanny, Renny, Sung Jun Bae, Mohammad Kemal Dermawan, dan Anna Bosch. "Disgorgement of Profits: An Alternative Solution to Stolen State Assets' Recovery from Corporate Financial Crimes." *Hasanuddin Law Review* 9, no. 2 (2023): 139–54. https://doi.org/10.20956/halrev.v9i2.4622.

Atmari, Atmari, Budiarsih Budiarsih, dan Slamet Suhartono. "Legal Protection of Resigning Workers' Right Over Separation Pay Compensation in Justice Perspective." *International Journal of Multicultural and Multireligious Understanding* 7, no. 8 (2020): 713. https://doi.org/10.18415/ijmmu.v7i8.1998.

Basri, Muhammad, dan Afif Muhni. "Assets Depreciation as an Economic Challenge Assets Recovery from Corruption." Dalam *Pakistan Journal of Criminology*, vol. 16. no. 04. t.t.

Dera, Alfa, dan Fauzie Yusuf Hasibuan. "Dominus Litis Restorative Model: Reconstruction of the

Role of the Prosecutor in Criminal Procedure Law Against Perpetrators with Mental and/or Intellectual Disabilities." Dalam *Advances in Social Humanities Research*, vol. 3. no. 7. 2025.

Disemadi, Hari Sutra. "Urgensi Regulasi Khusus dan Pemanfaatan Artificial Intelligence dalam Mewujudkan Perlindungan Data Pribadi di Indonesia." *Jurnal Wawasan Yuridika* 5, no. 2 (2021): 177. https://doi.org/10.25072/jwy.v5i2.460.

Djeundje, Viani B., Jonathan Crook, Raffaella Calabrese, dan Mona Hamid. "Enhancing credit scoring with alternative data." *Expert Systems with Applications* 163 (Januari 2021). https://doi.org/10.1016/j.eswa.2020.113766.

Fadhlina, Amilah, Regina Resentia, Syarifah Fatimahtazzuhrah Rukhsal Assegaf, Herpandu Hadiwibowo, dan Alicia Shafa Azzahra. *Perlindungan Data Pribadi Nasabah dalam Transaksi Central Bank Digital Currency (CBDC) dalam Rupiah Digital*. 7, no. 1 (2024). https://doi.org/10.31933/unesrev.v7i1.

Fatmala Putri, Dewi, dan Widya Ratna Sari. "ANALISIS PERLINDUNGAN NASABAH BSI TERHADAP KEBOCORAN DATA DALAM MENGGUNAKAN DIGITAL BANKING." *Jurnal Ilmiah Ekonomi dan Manajemen* 1, no. 4 (2023): 173–81. https://doi.org/10.61722/jiem.v1i4.331.

Febrian Rukmana Aji, Hieronymus, dan Abraham Ferry Rosando. "PERLINDUNGAN HUKUM TERHADAP HASIL FOTO PRIBADI YANG DIGUNAKAN ORANG LAIN DI INSTAGRAM." Dalam *Jurnal Hukum Bisnis Bonum Commune*, vol. 2. t.t.

Galang Surya Mahendra. "Perlindungan Hukum Terhadap Korban Yang Data Pribadi Passportnya Tersebar Akibat Kelalaian Pemerintah." *Terang : Jurnal Kajian Ilmu Sosial, Politik dan Hukum* 1, no. 3 (2024): 104–11. https://doi.org/10.62383/terang.v1i3.382.

Hayfa, Jessenia, Rizky Rani, Sheren Regina Wungkana, dkk. *Jurnal Penelitian Ilmu-Ilmu Sosial Implementation of Data Protection Authority (DPA) in Indonesia: The Urgency of Legal Protection of Customer's Personal Data in E-Banking Service Transactions*. Vol. 5. no. 1. 2024.

Ikhwan Bintarto Sayang Bidul Zaid, Muhammad Al, Muhammad Al Ikhwan Bintarto, dan Sayang Bidul. *Analysis of Economic Analysis of Law Principle In Purchase Fuel By Application (Study of MyPertamina)*. t.t.

Irwanto, Hartono Tasir, Wiranti Wiranti, Muhammad Fitratallah Dahlan, dan Nadiah Khaeriah Kadir. "Ethics and Law of Personal Data Protection for Smartwatches in the Healthcare Sector." *SIGn Jurnal Hukum* 7, no. 1 (2025): 421–36. https://doi.org/10.37276/sjh.v7i1.489.

Januarsyah, Mas Putra Zenno, Dwidja Priyatno, Somawijaya, dan Widiada Gunakaya. "The Renewal Policy of the Adultery Concept in Article 411 of the Law Number 1 of 2023 on the Indonesian Criminal Code." *Padjadjaran Jurnal Ilmu Hukum* 10, no. 1 (2023): 1–16. https://doi.org/10.22304/pjih.v10n1.a1.

Kozodoi, Nikita, Johannes Jacob, dan Stefan Lessmann. "Fairness in credit scoring: Assessment,

implementation and profit implications." *European Journal of Operational Research* 297, no. 3 (2022): 1083–94. https://doi.org/10.1016/j.ejor.2021.06.023.

Kurniawan, Komang Suputra, dan I. Gede Agus Kurniawan. "The Limitations of Lex Generalis: Analyzing the Readiness of the GDPR and PDP Law for AI-Based Facial Recognition Technology." *SIGn Jurnal Hukum* 7, no. 2 (2025): 838–52. https://doi.org/10.37276/sjh.v7i2.533.

Luo, Jia, Junping Xu, Obaid Aldosari, Sara A. Althubiti, dan Wejdan Deebani. "Design and Implementation of an Efficient Electronic Bank Management Information System Based Data Warehouse and Data Mining Processing." *Information Processing and Management* 59, no. 6 (2022). https://doi.org/10.1016/j.ipm.2022.103086.

Makarim, Edmon. "Privacy and Personal Data Protection in Indonesia: The Hybrid Paradigm of the Subjective and Objective Approach." Dalam *Data Protection Around the World: Privacy Laws in Action*, disunting oleh Elif Kiesow Cortez. T.M.C. Asser Press, 2021. https://doi.org/10.1007/978-94-6265-407-5_6.

Mariyam, Siti, Sri Mulyani, dan Saryana Saryana. "Corporate Liability of Ride-Hailing Services: An Analysis of Partnership Legal Fiction and the Reconstruction of Passenger Safety Regulation." *SIGn Jurnal Hukum* 7, no. 2 (2025): 803–20. https://doi.org/10.37276/sjh.v7i2.529.

MARTIN, Víctor Gómez. "The Criminal Liability of the Compliance Officer: An Approach Through Several Hard Cases." *Journal of Penal Law & Criminology*, advance online publication, 29 Juni 2020. https://doi.org/10.26650/jplc2020-0010.

Martupa, Abraham Ethan, Sahat Marune, dan Brandon Hartanto. "Strengthening Personal Data Protection, Cyber Security, and Improving Public Awareness in Indonesia: Progressive Legal Perspective." *International Journal of Business, Economics and Social Development* 2, no. 4 (2021): 143–52.

Muhni, A. *Strategi Penegakan Hukum Tindak Pidana Pencucian Uang pada Lembaga Perbankan*. Repository.unhas.ac.id, 2020.

Muhni, Afif, Muhammad Basri, Zul Khadir Kadir, dan Zul Khaidir Kadir. "MEDICOLEGAL PENGGUNAAN KADAVER MANUSIA UNTUK BEDAH ANATOMI MEDIS DAN TRANSPLANTASI ORGAN MEDICOLEGAL USE OF HUMAN CADAVERS FOR MEDICAL ANATOMICAL SURGERY AND ORGAN TRANSPLANTATION." *Jurnal Hukum dan Etika Kesehatan* 5, no. 2 (2025). https://doi.org/10.30649/jhek.v5i2.237.

Muhni, Afif, Muhammad Basri, Syarif Saddam Rivanie, Ismail Iskandar, Audyna Mayasari Muin, dan Hijrah Adhyanti Mirzana. "Integration of Anti-SLAPP in the Reform of the Indonesian Criminal Procedure Code in an Effort to Protect Human Rights." *SIGn Jurnal Hukum* 7, no. 1 (2025): 437–53. https://doi.org/10.37276/sjh.v7i1.485.

Munawar, Kukun Abdul Syakur, Hisam Ahyani, Abdul Rahim, Ali Mutakin, dan Md Yazid Ahmad. "Reversed Burden of Proof in Online Gambling Fraud: Consumer Protection Based on Islamic Law in West Java." *Jurnal Hukum Bisnis Bonum Commune* 8, no. 2 (2025): 243–61. https://doi.org/10.30996/jhbbc.v8i2.12886.

Muthia, Nuriyah Fara, Afif Muhni, dan Nurisnah H. "Dual use satellites in the Ukraine conflict: The dilemma between state sovereignty and the principle of non-militarization of outer space." *Priviet Social Sciences Journal* 5, no. 10 (2025): 146–55. https://doi.org/10.55942/pssj.v5i10.715.

Palazzo, Maria, Agostino Vollero, dan Alfonso Siano. "From strategic corporate social responsibility to value creation: an analysis of corporate website communication in the banking sector." *International Journal of Bank Marketing* 38, no. 7 (2020): 1529–52. https://doi.org/10.1108/IJBM-04-2020-0168.

Pardosi, Rodes Ober Adi Guna, dan Yuliana Primawardani. "Perlindungan Hak Pengguna Layanan Pinjaman Online dalam Perspektif Hak Asasi Manusia." *Jurnal HAM* 11, no. 3 (2020): 353. https://doi.org/10.30641/ham.2020.11.353-368.

Putriyanti[l], Erma Defiana, Abdul Rachmad Budiono, dan Reka Dewantara. *The Relevance Of Protectıng Debtor Customer Data And Informatıon Through Bank Secrecy: A Comparatıve Study In Indonesıa, Malaysıa And The Unıted Kıngdom*. 04, no. 04 (t.t.).

Ramsay, Sahur. "Pertanggungjawaban Direksi atas Kerugian Perseroan dalam Perusahaan Grup." *JUSTISI* 8, no. 3 (2022): 209–23. https://doi.org/10.33506/jurnaljustisi.v8i3.1823.

Risal, Abdul. "Legal Protection for Debtors in Online Transactions: Evaluating Safeguards in E-Commerce." *Jurnal Hukum Bisnis Bonum Commune* 7, no. 2 (2024): 176–87. https://doi.org/10.30996/jhbbc.v7i2.11656.

Rohendi, Acep, dan Dona Budi Kharisma. "Personal data protection in fintech: A case study from Indonesia." *Journal of Infrastructure, Policy and Development* 8, no. 7 (2024). https://doi.org/10.24294/jipd.v8i7.4158.

Salsabila, Uly Alfinda, dan Dona Budi Kharisma. "Mechanism Law Enforcement on Fintech Personal Data Abuse Post -Law Number 27 of 2022 Concerning Personal Data Protection." Dalam *Proceedings of the International Conference on Democracy and National Resilience 2025 (ICDNR 2025)*, vol. 981, disunting oleh Sunny Ummul Firdaus, Gayatri Dyah Suprobowati, R. Prihandjojo Andri Putranto, dkk. Advances in Social Science, Education and Humanities Research. Atlantis Press SARL, 2025. https://doi.org/10.2991/978-2-38476-529-4_11.

Sari, Pala, dan Pariaman Ompusunggu. "Analisis Hukum Terhadap Perlindungan Data Pribadi Nasabah dalam Layanan Perbankan Digital di Indonesia." Dalam *Aufklarung: Jurnal Pendidikan*, vol. 3. no. 3. 2023.

Simbolon, Valentina Ancillia, dan Vishnu Juwono. "Comparative Review of Personal Data Protection Policy in Indonesia and The European Union General Data Protection Regulation." *Publik (Jurnal Ilmu Administrasi)* 11, no. 2 (2022): 178. https://doi.org/10.31314/pjia.11.2.178-190.2022.

Taylor, M. B. "Counter corporate litigation: Remedy, regulation, and repression in the struggle for a just transition." *Sustainability*, 2021.

Usman, Rachmadi. "Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) Exploration of nexus between legal liability and corporate fraud: where do business laws and criminology converge?" *International Journal of Criminal Justice Sciences. Criminal Justice Sciences (IJCJS)-Official Journal of the South Asian Society of Criminology and Victimology* 18, no. 1 (t.t.): 232–43. https://doi.org/10.5281/zenodo.4756251/IJCJS.

Uswatun Hasanah, Djulaeka Djulaeka, Murni Murni, dan A. Zaenurrosyid. "The Phenomenon of Personal Data as a 'Pseudo Guarantee' In Fintech : Legal or Not?" *JUSTISI* 11, no. 3 (2025): 763–80. https://doi.org/10.33506/js.v11i3.4247.

Vovk, Viktoriia, Yuliia Zhezherun, Olena Bilovodska, Vitalina Babenko, dan Alevtyna Biriukova. "Financial monitoring in the bank as a market instrument in the conditions of innovative development and digitalization of economy: Management and legal aspects of the risk-based approach." *International Journal of Industrial Engineering and Production Research* 31, no. 4 (2020): 559–70. https://doi.org/10.22068/ijiepr.31.4.559.

Wawasan, Literasi &., Komprehensif Hukum, Sitta Saraya, dkk. *HUKUM PIDANA INDONESIA*. 2025.

Yuspin, Wardah, Kelik Wardiono, Aditya Nurrahman, dan Arief Budiono. "Personal Data Protection Law in Digital Banking Governance in Indonesia." *Studia Iuridica Lublinensia* 32, no. 1 (2023): 99–130. https://doi.org/10.17951/sil.2023.32.1.99-130.

Zorzetto, Silvia. "Better Regulation, Cost-Benefit Analysis and Evidence Based Legal Design: A Critical Inquiry." Dalam *Developments in Law and Economics in the Italo-Iberoamerican Context*, disunting oleh Betzabé and Sotomayor Trelles José Enrique and Ferraro Francesco Zorzetto Silviaand Marciani Burgos. Springer Nature Switzerland, 2025. https://doi.org/10.1007/978-3-032-03317-8_7.