Volume 02 No. 02, Desember 2025
E-ISSN: 3090-6199

Lex Mercatoria. Fakultas Hukum, Universitas PGRI Palembang.
Open Acces at: https://jurnal.univpgri-palembang.ac.id/index.php/lexmercatoria

Analisis Hukum Atas Penyalahgunaan Data Oleh Perusahaan Platform Dalam Perspektif Hukum Bisnis dan *Cyber Law*

Sri Husnulwati[1], Sri Wahyuningsih[2], Sundari[3]
[1,2,3]Fakultas Hukum Universitas PGRI Palembang, Sumatera Selatan, Indonesia
Email: srihusnulwati05@gmail.com, wsri7896@gmail.com, sundarinanung@gmail.com
[*]**No HP/WA: 081373222125**

Submitted:
Accepted:
Published:

Keywords:
Misuse; Data; Platform Companies; Business Law; Cyber Law

Abstract- This study aims to analyze the misuse of data by platform companies from the perspectives of business law and cyber law. It adopts a normative juridical approach with a descriptive-analytical method, focusing on conceptual and doctrinal analysis of applicable legal norms. Primary data sources are derived from national and international legislation, while secondary data sources encompass legal literature, scholarly journals, and case reports from relevant institutions. Data collection techniques involve the inventory of legal documents and qualitative content analysis. This approach enables the researcher not only to describe the phenomenon of data misuse but also to formulate reconstructive recommendations, while upholding research ethics through principles of confidentiality and interpretive objectivity. The findings of this study indicate that, overall, the business law perspective portrays data misuse as an economic power imbalance that disrupts data-based business models, wherein the integration of the Personal Data Protection Law (UU PDP) with business law serves as the key to compliance, thereby avoiding fines of up to IDR 2 billion and class action litigation. The cyber law perspective concludes that data misuse constitutes an existential cybercrime threatening national security and system integrity, governed by the Electronic Information and Transactions Law (UU ITE) and the Personal Data Protection Law (UU PDP), which align with the Budapest Convention on Cybercrime; the 300% surge in breaches reported by the National Cyber and Crypto Agency (BSSN) from 2020 to 2024 underscores the intermediary responsibilities for due diligence.

Kata Kunci:
Penyalahgunaan; Data; Perusahaan Platform; Hukum Bisnis; Cyber Law

Abstrak- Penelitian ini bertujuan untuk menganalisis penyalahgunaan data oleh perusahaan platform dalam perspektif hukum bisnis dan cyber law. Penelitian ini mengadopsi pendekatan yuridis normatif dengan metode deskriptif-analitik, yang difokuskan pada analisis konseptual dan doktrinal terhadap norma hukum yang berlaku. Sumber data primer diperoleh dari peraturan perundang-undangan nasional dan internasional, sementara sumber data sekunder meliputi literatur hukum, jurnal ilmiah, dan laporan kasus dari lembaga. Teknik pengumpulan data dilakukan dengan inventarisasi dokumen hukum dan analisis konten kualitatif. Pendekatan ini memungkinkan peneliti untuk

tidak hanya mendeskripsikan fenomena penyalahgunaan data tetapi juga merumuskan rekomendasi rekonstruktif, dengan memastikan etika penelitian melalui prinsip kerahasiaan dan objektivitas interpretasi. Hasil dari penelitian ini adalah Secara keseluruhan, perspektif hukum bisnis menggambarkan penyalahgunaan data sebagai ketidakseimbangan kekuasaan ekonomi yang mengganggu model bisnis berbasis data, di mana integrasi UU PDP dengan business law menjadi kunci compliance untuk menghindari denda hingga Rp 2 miliar dan litigasi class action. Perspektif cyber law menyimpulkan penyalahgunaan data sebagai kejahatan siber eksistensial yang mengancam keamanan nasional dan integritas sistem, diatur UU ITE serta UU PDP yang selaras Budapest Convention, dengan lonjakan breach 300% oleh BSSN (2020-2024) menekankan tanggung jawab intermediary untuk due diligence.

A. PENDAHULUAN

Pada era digital yang semakin terintegrasi, perusahaan platform seperti media sosial, e-commerce, dan layanan fintech telah menjadi tulang punggung ekonomi digital global, termasuk di Indonesia, di mana pertumbuhan pengguna internet mencapai lebih dari 200 juta orang pada tahun 2024. Platform ini mengumpulkan volume data pribadi yang masif untuk mendukung model bisnis berbasis algoritma, seperti targeted advertising dan personalisasi layanan, yang pada gilirannya mendorong inovasi ekonomi tetapi juga menimbulkan risiko signifikan terhadap privasi individu. Penyalahgunaan data oleh perusahaan platform sering kali muncul dalam bentuk pengumpulan tanpa persetujuan eksplisit, pembagian data dengan pihak ketiga tanpa transparansi, atau kebocoran akibat kerentanan keamanan siber, yang tidak hanya merugikan konsumen secara finansial dan emosional tetapi juga mengancam stabilitas pasar. Menurut Lee[2] dalam analisisnya tentang kompleksitas tren AI, penyalahgunaan data oleh platform teknologi sering kali berakar pada ketidakseimbangan kekuasaan antara korporasi raksasa dan pengguna individu, di mana algoritma prediktif digunakan untuk memanipulasi perilaku konsumen tanpa mekanisme akuntabilitas yang memadai. Di Indonesia, kasus kebocoran data Tokopedia pada Mei 2020 yang memengaruhi jutaan pengguna menjadi contoh nyata bagaimana platform digital gagal dalam menjaga integritas data, menyebabkan penyalahgunaan identitas digital dan kerugian ekonomi mencapai miliaran rupiah[3]. Fenomena ini tidak terisolasi; laporan Badan Siber dan Sandi Negara (BSSN) mencatat peningkatan 300% kasus kebocoran data antara 2020 dan 2024, yang menekankan urgensi analisis hukum yang holistik untuk mengintegrasikan perspektif hukum bisnis dan *cyber law* guna membangun kerangka regulasi yang adaptif.

---

[2] J Lee, "Complexities of AI Trends: Threats to Data Privacy Legal Compliance," *Seattle Journal of Technology, Environmental & Innovation Law* 15, no. 2 (2025): 210–35.

[3] A Nuranisa and D Lukitasari, "Analisa Kasus Kebocoran Data Pengguna Tokopedia," *Jurnal Hukum Progresif* 11, no. 2 (2024): 1928–40.

Evolusi penyalahgunaan data oleh perusahaan platform dapat ditelusuri ke transformasi ekonomi digital pasca-pandemi COVID-19, di mana ketergantungan pada layanan online melonjak, mendorong platform untuk memperluas pengumpulan data demi keunggulan kompetitif. Dari perspektif hukum bisnis, hal ini menimbulkan dilema etis-kontraktual, di mana klausul privasi dalam perjanjian pengguna sering kali dirancang secara asimetris untuk melindungi kepentingan perusahaan daripada hak konsumen. Kim[4] dalam studinya tentang dampak undang-undang perlindungan data konsumen terhadap model bisnis perusahaan teknologi, menemukan bahwa regulasi ketat seperti *General Data Protection Regulation* (GDPR) di Uni Eropa telah memaksa platform seperti Meta dan Google untuk merevisi strategi monetisasi mereka, mengurangi pendapatan dari iklan berbasis data hingga 15% di wilayah yang diatur. Di konteks Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) muncul sebagai respons terhadap kekosongan regulasi sebelumnya, yang sebagian besar bergantung pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang kurang spesifik terhadap isu data pribadi. Namun, implementasi UU PDP masih menghadapi tantangan, seperti kurangnya sanksi progresif yang dapat mencegah penyalahgunaan sistematis oleh platform asing yang beroperasi di Indonesia tanpa basis hukum lokal yang kuat. Smith et al.[5] menyoroti implikasi hukum dari regulasi privasi data dan etika AI, di mana perusahaan platform sering kali menghindari tanggung jawab melalui yurisdiksi *off-shore*, yang memperburuk ketidakadilan akses keadilan bagi korban di negara berkembang seperti Indonesia. Selain itu, perspektif cyber law menambahkan lapisan kompleksitas, di mana penyalahgunaan data bukan hanya pelanggaran kontraktual tetapi juga ancaman keamanan nasional, sebagaimana dibahas dalam kerangka konvensi Budapest tentang *Cybercrime* yang diratifikasi Indonesia pada 2019.

Perspektif hukum bisnis dalam analisis penyalahgunaan data oleh perusahaan platform menekankan pada aspek liability dan governance korporat, di mana kegagalan dalam due diligence data dapat mengakibatkan tuntutan perdata yang mahal dan penurunan nilai saham. Buku panduan Lathrop GPM[6] tentang privasi dan keamanan data menjelaskan bahwa perusahaan platform harus mengadopsi pendekatan *risk-based compliance*, termasuk audit berkala dan klausul indemnitas dalam kontrak mitra, untuk memitigasi dampak finansial dari breach. Di Indonesia, kasus penyalahgunaan data oleh pinjaman online ilegal (pinjol) pada 2023, yang melibatkan pemerasan melalui data pribadi curian, mengilustrasikan bagaimana model bisnis predatory ini melanggar

[4] S Kim, "Consumer Data Protection Laws and Their Impact on Business Models of Technology Companies," *Telecommunications Policy* 48, no. 7 (2024): Article 102789, https://doi.org/10.1016/j.telpol.2024.102789.

[5] A Smith and et al., "The Legal Implications of Data Privacy Laws, Cybersecurity Regulations and AI Ethics in a Digital Society," *International Journal of Law and Information Technology* 33, no. 3 (2025): 456–78, https://doi.org/10.1093/ijlit/eaad012.

[6] Lathrop GPM, *A Legal Guide to Privacy and Data Security 2025* (Lathrop GPM LLP, 2025).

prinsip fair competition di bawah Undang-Undang Nomor 5 Tahun 1999 tentang Larangan Praktik Monopoli dan Persaingan Usaha Tidak Sehat. Analisis mendalam oleh Thompson Reuters [7] dalam *Data Security and Privacy Law*: *Combating Cyber Threats*, menggarisbawahi bahwa integrasi cyber law ke dalam strategi bisnis seperti penerapan *zero-trust architecture* dapat mengurangi insiden penyalahgunaan hingga 40%, tetapi memerlukan investasi awal yang tinggi bagi UMKM digital di negara seperti Indonesia. Lebih lanjut, dari sudut pandang cyber law, penyalahgunaan data oleh platform sering kali dikategorikan sebagai kejahatan siber transnasional, yang memerlukan harmonisasi regulasi regional melalui ASEAN *Digital Economy Framework Agreement* (DEFA). Studi komparatif oleh Johnson[8] tentang privasi data di era digital antara AS dan UE menunjukkan bahwa pendekatan berbasis sanksi pidana di UE, seperti denda hingga 4% dari omzet global, lebih efektif dalam mendorong kepatuhan dibandingkan model *self-regulatory* di AS, yang sering gagal menangani penyalahgunaan oleh big tech. Di Indonesia, Pasal 66 UU PDP menetapkan sanksi administratif hingga Rp 2 miliar dan pidana hingga enam tahun penjara, tetapi penegakan masih lemah akibat keterbatasan sumber daya forensik digital, sebagaimana dianalisis oleh Widjaja dan Pratiwi[9] dalam jurnal mereka tentang perlindungan data pribadi di fintech.

Tantangan utama dalam perspektif gabungan hukum bisnis dan cyber law adalah ketidaksinkronan antara inovasi teknologi dan kerangka hukum yang kaku, di mana platform seperti TikTok dan Shopee terus berevolusi dengan fitur AI-driven profiling yang berpotensi menyalahgunakan data untuk manipulasi perilaku. Hal ini diperparah oleh rendahnya literasi digital di kalangan pengguna Indonesia, di mana hanya 40% responden survei BSSN tahun 2024 memahami hak mereka atas data pribadi. Buku *Proskauer on Privacy* oleh Arkell *et al.*[10] menyediakan panduan komprehensif tentang pengembangan program kepatuhan yang mengintegrasikan etika bisnis dengan standar cyber security, termasuk simulasi breach response yang dapat diterapkan oleh platform lokal untuk menghindari litigasi massal. Sementara itu, analisis oleh Garcia[11] dalam jurnal tentang dimensi kolektif perlindungan data melalui *predictive analytics* menekankan perlunya pendekatan interdisipliner yang melibatkan etika, hukum, dan teknologi untuk mengatasi bias algoritma yang diskriminatif, yang sering kali menjadi alat penyalahgunaan data di platform sosial. Di tingkat nasional, implementasi UU PDP sejak Oktober 2022 telah mendorong

[7] Thompson Reuters, *Data Security and Privacy Law: Combating Cyber Threats*, ed. 2024-2025 ed. (Thomson Reuters, 2024).

[8] R Johnson, "Data Privacy in the Digital Age: A Comparative Analysis of U.S. and EU Regulations," *UCLA Law Review* 72, no. 1 (2025): 45–78.

[9] T Widjaja and R Pratiwi, "Implikasi Hukum Terhadap Perlindungan Data Pribadi Dalam Transaksi Fintech Di Indonesia," *Jurnal Hukum Indonesia* 14, no. 2 (2023): 132–36.

[10] J Arkell and et al., *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age*, ed. 3rd ed. (Practising Law Institute, 2023).

[11] M Garcia, "Predictive Analytics and the Collective Dimensions of Data Protection," *New Media & Society* 26, no. 5 (2024): 1234–56, https://doi.org/10.1080/17579961.2024.2313794.

pembentukan Dewan Perlindungan Data Pribadi, tetapi kurangnya kolaborasi dengan Otoritas Jasa Keuangan (OJK) untuk sektor *fintech* menimbulkan celah regulasi, seperti yang dibahas dalam studi kasus kebocoran data BPJS Kesehatan yang memengaruhi 279 juta warga pada 2021. [12] Perspektif ini semakin relevan mengingat proyeksi pertumbuhan ekonomi digital Indonesia mencapai USD 130 miliar pada 2025, di mana kegagalan mengatasi penyalahgunaan data dapat menghambat investasi asing dan kepercayaan konsumen.

Secara keseluruhan, analisis hukum atas penyalahgunaan data oleh perusahaan platform dalam perspektif hukum bisnis dan cyber law bukan hanya kebutuhan akademis, tetapi imperatif strategis untuk membangun ekosistem digital yang berkelanjutan. Dengan mengintegrasikan prinsip-prinsip dari UU PDP, GDPR, dan kerangka internasional lainnya, Indonesia dapat mengembangkan model regulasi yang seimbang, di mana inovasi bisnis didukung oleh perlindungan cyber yang kuat. Seperti yang dikemukakan oleh Cohen [13] dalam tinjauan tahunan cybersecurity dan privasi data AS, transisi ke era post-GDPR menuntut perusahaan platform untuk mengadopsi "*privacy by design*" sebagai *core value*, bukan sekadar *compliance tool*, guna mencegah eskalasi konflik hukum yang dapat merusak fondasi ekonomi digital. Di Indonesia, di mana platform digital berkontribusi 10% terhadap PDB nasional, pendekatan ini akan memastikan bahwa pertumbuhan teknologi tidak dikorbankan atas nama privasi, melainkan saling memperkuat melalui governance yang inklusif dan adaptif terhadap ancaman siber yang terus berkembang.

B. METODE PENELITIAN

Penelitian ini mengadopsi pendekatan yuridis normatif dengan metode deskriptif-analitik, yang difokuskan pada analisis konseptual dan doktrinal terhadap norma hukum yang berlaku, termasuk Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), untuk mengungkap ketidaksesuaian regulasi dalam konteks penyalahgunaan data oleh perusahaan platform dari perspektif hukum bisnis dan *cyber law*. Sumber data primer diperoleh dari peraturan perundang-undangan nasional dan internasional seperti General Data Protection Regulation (GDPR) Uni Eropa, sementara sumber data sekunder meliputi literatur hukum, jurnal ilmiah, dan laporan kasus dari lembaga seperti Badan Siber dan Sandi Negara (BSSN), yang dikumpulkan melalui studi pustaka secara sistematis untuk memastikan komprehensivitas analisis. Teknik pengumpulan data dilakukan dengan inventarisasi dokumen hukum dan analisis konten kualitatif, di mana konsep-konsep seperti *vicarious liability* dan *privacy by design* dieksplorasi untuk

[12] H Siregar, "Perlindungan Hukum Bagi Pengguna Aplikasi Tokopedia Dari Penyalahgunaan Data Pribadi," *Jurnal Konstitusi Hukum Dan Kebijakan* 5, no. 1 (2024): 67–85.
[13] J Cohen, "U.S. Cybersecurity and Data Privacy Review and Outlook – 2025" (Gibson Dunn & Crutcher LLP, 2025).

membangun argumen normatif, sebagaimana direkomendasikan oleh Marzuki[14] dalam bukunya yang menekankan bahwa pendekatan yuridis normatif efektif untuk mengintegrasikan teori hukum dengan praktik empiris dalam studi cyber law. Selain itu, analisis komparatif terhadap regulasi ASEAN *Digital Economy Framework Agreement* (DEFA) diterapkan untuk memperkaya perspektif lintas yurisdiksi, sesuai dengan metodologi yang diuraikan oleh Santoso[15] dalam jurnalnya, yang menyoroti pentingnya triangulasi sumber untuk validasi interpretasi hukum dalam era digital. Pendekatan ini memungkinkan peneliti untuk tidak hanya mendeskripsikan fenomena penyalahgunaan data tetapi juga merumuskan rekomendasi rekonstruktif, dengan memastikan etika penelitian melalui prinsip kerahasiaan dan objektivitas interpretasi.

C. HASIL DAN PEMBAHASAN

1. Definisi dan Bentuk Penyalahgunaan Data Pribadi

Dalam konteks perkembangan teknologi digital yang pesat, data pribadi telah menjadi aset berharga bagi perusahaan platform seperti media sosial, e-commerce, dan layanan fintech, yang mengandalkannya untuk inovasi bisnis seperti personalisasi layanan dan targeted advertising. Namun, ketergantungan ini sering kali melahirkan penyalahgunaan data pribadi, yang tidak hanya mengancam privasi individu tetapi juga menimbulkan risiko hukum signifikan dari perspektif hukum bisnis dan *cyber law*. Definisi data pribadi secara umum merujuk pada informasi yang mengidentifikasi atau dapat digunakan untuk mengidentifikasi individu, seperti nama, alamat, nomor telepon, riwayat transaksi, atau data biometrik, sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) di Indonesia. Penyalahgunaan data pribadi, oleh karena itu, dapat didefinisikan sebagai segala tindakan yang melanggar prinsip pengolahan data yang sah, termasuk pengumpulan, penyimpanan, penggunaan, atau pengungkapan data tanpa persetujuan pemilik, yang mengakibatkan kerugian materil maupun immateril. Menurut Wijaya dan Anggriawan[16] penyalahgunaan data pribadi terjadi ketika data tersebut "dikumpulkan, diperdagangkan, atau digunakan untuk tujuan selain berbagi atau mentransmisikan data tanpa pengetahuan dan izin pemilik", yang sering kali berujung pada pelanggaran hak asasi manusia terkait privasi. Definisi ini selaras dengan kerangka *cyber law internasional*, seperti *General Data Protection Regulation* (GDPR) Uni Eropa, yang menekankan bahwa penyalahgunaan mencakup pelanggaran keamanan data yang menyebabkan akses tidak sah oleh pihak ketiga. Dari perspektif hukum bisnis, penyalahgunaan ini bukan hanya isu etis, melainkan risiko operasional yang dapat memicu

[14] P M Marzuki, *Penelitian Hukum: Edisi Revisi* (Prenada Media Group, 2023).

[15] B Santoso, "Metodologi Penelitian Yuridis Normatif Dalam Analisis Cyber Law: Pendekatan Komparatif ASEAN," *Jurnal Hukum Dan Pembangunan* 54, no. 2 (2024): 245–67, https://doi.org/10.21143/jhp.vol54.no2.3456.

[16] A D Wijaya and T P Anggriawan, "Perlindungan Hukum Terhadap Data Pribadi Dalam Penggunaan Aplikasi Di Smartphone," *Inicio Legis* 5, no. 1 (2022): 45–62.

litigasi perdata dan penurunan reputasi, sementara dalam *cyber law*, ia dikategorikan sebagai bentuk kejahatan siber yang memerlukan penegakan pidana untuk mencegah eskalasi ancaman nasional.

Lebih lanjut, definisi penyalahgunaan data pribadi dalam literatur hukum kontemporer menyoroti dimensi multidimensi, yang melibatkan aspek teknis, etis, dan yuridis. Luthiya *et al.* [17] mendefinisikan penyalahgunaan sebagai "kegiatan memperoleh data komputer secara tidak sah, baik untuk digunakan sendiri maupun diberikan kepada orang lain, sering diikuti dengan kejahatan penipuan (*fraud*) atau data leakage". Definisi ini menekankan elemen akses ilegal, yang mencakup tidak hanya pencurian langsung tetapi juga manipulasi data untuk tujuan komersial atau kriminal. Buku *Privacy and Cybersecurity Law Deskbook* [18] memperluasnya dengan menjelaskan bahwa penyalahgunaan mencakup "*unauthorized disclosures and security violations*", di mana perusahaan platform gagal menerapkan langkah-langkah keamanan yang memadai, seperti enkripsi atau audit rutin, sehingga data menjadi rentan terhadap breach. Dalam konteks Indonesia, UU PDP Pasal 3 mendefinisikan data pribadi sebagai "data tentang orang perseorangan yang terkumpul atau dihasilkan dari aktivitas perseorangan", dan penyalahgunaannya diatur dalam Pasal 16 yang melarang pengolahan data tanpa dasar hukum yang sah. Perspektif hukum bisnis melihat definisi ini sebagai kewajiban kontraktual, di mana klausul privasi dalam terms of service harus melindungi data sebagai aset bisnis, sementara cyber law menambahkan lapisan pidana melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) Pasal 26, yang menyatakan bahwa "setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan" termasuk penyalahgunaan data. Schwartz [19] dalam *Privacy Law Fundamentals*, menambahkan bahwa definisi penyalahgunaan harus mencakup "systemic misuse" di mana algoritma AI platform secara tidak sengaja mendiskriminasi pengguna berdasarkan data pribadi, yang menimbulkan implikasi etis-bisnis seperti hilangnya kepercayaan konsumen.

Untuk memahami bentuk-bentuk penyalahgunaan data pribadi secara lebih terstruktur, dapat dikategorikan sebagai berikut, dengan masing-masing diilustrasikan melalui contoh dan implikasi hukum:

a) Pengumpulan Data Tanpa Persetujuan Eksplisit
   Bentuk ini terjadi ketika platform mengumpulkan data lebih dari yang diperlukan atau tanpa informed consent, seperti saat aplikasi meminta akses

[17] A N Luthiya, B Irawan, and R Yulia, "Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi," *Jurnal Hukum Pidana & Kriminologi* 12, no. 2 (2021): 150–70.

[18] Privacy and Cybersecurity Law Deskbook (2025 Edition), *Privacy and Cybersecurity Law Deskbook*, ed. 2025 Edition (American Bar Association, 2025).

[19] P M Schwartz, *Privacy Law Fundamentals* (IAPP, 2024).

ke kontak atau lokasi tanpa alasan jelas. Wijaya dan Anggriawan [20] menyebutkan bahwa "pelaku usaha mengumpulkan data pribadi dari pelanggan secara offline atau online, memungkinkan data diperdagangkan atau disalahgunakan tanpa izin", yang sering terlihat pada platform e-commerce seperti Tokopedia yang mendaftarkan data KTP tanpa batasan penggunaan. Dari perspektif hukum bisnis, ini melanggar prinsip fair trade dan dapat memicu tuntutan ganti rugi berdasarkan Kitab Undang-Undang Hukum Perdata (KUHPerdata) Pasal 1365 tentang perbuatan melawan hukum. Dalam cyber law, UU PDP Pasal 18 mewajibkan persetujuan tertulis, dan pelanggarannya dapat dikenai sanksi administratif hingga Rp 2 miliar.

b) Pembagian atau Penjualan Data dengan Pihak Ketiga
Platform sering berbagi data dengan mitra iklan tanpa transparansi, yang mengarah pada penjualan di dark web. Luthiya *et al.*[21] menggambarkan ini sebagai "pencurian data melalui internet: mengambil data milik orang lain yang tersimpan di sistem elektronik tanpa seizin", di mana data dijual untuk kejahatan lanjutan seperti penipuan. Contoh kasus kebocoran data BPJS Kesehatan 2021 menunjukkan bagaimana data 279 juta warga dijual secara ilegal, menyebabkan kerugian ekonomi nasional. Hukum bisnis memandang ini sebagai *breach of contract* yang merusak model *revenue sharing*, sementara cyber law mengklasifikasikannya sebagai illegal interception di bawah Konvensi Budapest tentang Cybercrime, yang diratifikasi Indonesia.

c) Kebocoran Data Akibat Kerentanan Keamanan
Bentuk pasif ini melibatkan hack atau ransomware yang mengeksploitasi kelemahan sistem platform. *Privacy and Cybersecurity Law Deskbook* [22] mendefinisikannya sebagai "data *breaches involving unauthorized access*", dengan contoh *ransomware* yang menargetkan server fintech, seperti kasus Gojek 2023. Implikasi bisnis termasuk biaya mitigasi hingga miliaran rupiah dan penurunan saham, sedangkan *cyber law* menerapkan UU ITE Pasal 32 tentang akses ilegal, dengan ancaman pidana hingga 6 tahun penjara.

d) Penggunaan Data untuk Profiling atau Manipulasi Ilegal
Platform menggunakan data untuk membangun profil psikologis guna manipulasi perilaku, seperti iklan targeted yang diskriminatif. Kim (2024), dalam jurnal Telecommunications Policy, menyatakan bahwa "regulasi ketat seperti GDPR telah memaksa platform merevisi strategi monetisasi dari iklan berbasis data", yang di Indonesia sering melanggar UU PDP Pasal 20 tentang profiling otomatis. Hukum bisnis melihat ini sebagai risiko reputasi, sementara *cyber law* menyoroti ancaman terhadap demokrasi digital melalui misinformation.

e) Pemalsuan atau Interferensi Data

[20] Wijaya and Anggriawan, "Perlindungan Hukum Terhadap Data Pribadi Dalam Penggunaan Aplikasi Di Smartphone."
[21] Luthiya, Irawan, and Yulia, "Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi."
[22] Edition), *Privacy and Cybersecurity Law Deskbook*.

Termasuk skimming atau data interference, di mana data diubah untuk fraud. Luthiya *et al.*[23] menjelaskan "skimming sebagai aktivitas mencuri data dari pita magnetik kartu secara ilegal", yang kini berevolusi ke malware di *e-commerce*. Bentuk ini memicu vicarious liability bagi platform sebagai pengendali sistem, dengan sanksi pidana di UU ITE Pasal 35.

Bentuk-bentuk ini saling terkait dan sering kali bersifat transnasional, di mana platform asing seperti Meta atau Google beroperasi di Indonesia tanpa compliance penuh, memperburuk penegakan hukum. Garcia[24] dalam *New Media & Society* menekankan bahwa "predictive analytics dapat memperburuk bias algoritma yang diskriminatif", yang menjadi alat penyalahgunaan kolektif. Dari perspektif hukum bisnis, perusahaan harus mengadopsi *privacy by design* untuk mitigasi, sementara *cyber law* menuntut kolaborasi internasional melalui ASEAN DEFA. Secara keseluruhan, definisi dan bentuk penyalahgunaan data pribadi ini menuntut reformasi regulasi yang adaptif, di mana UU PDP harus diperkuat dengan mekanisme forensik digital untuk melindungi ekosistem bisnis digital Indonesia yang diproyeksikan mencapai USD 130 miliar pada 2025. Kegagalan mengatasi hal ini tidak hanya merugikan individu tetapi juga menghambat pertumbuhan ekonomi berkelanjutan.

2. Analisis Hukum atas Penyalahgunaan Data oleh Perusahaan Platform dalam Perspektif Hukum Bisnis

Dalam perspektif hukum bisnis, penyalahgunaan data oleh perusahaan platform digital seperti media sosial, *e-commerce*, dan layanan streaming merupakan manifestasi dari ketidakseimbangan kekuasaan ekonomi yang melibatkan aset data sebagai inti model bisnis, di mana pengumpulan masif data pribadi untuk targeted advertising sering kali melanggar prinsip kontraktual dan fiduciary duties terhadap konsumen. Hukum bisnis memandang penyalahgunaan ini bukan sekadar pelanggaran privasi, melainkan risiko sistemik yang memengaruhi governance korporat, liability, dan daya saing pasar, di mana platform seperti Meta atau Amazon memanfaatkan data untuk mendominasi ekosistem digital, tetapi berpotensi menghadapi tuntutan perdata berdasarkan *breach of contract* atau *unfair trade practices*. Analisis hukum ini menekankan bahwa regulasi seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) No. 27 Tahun 2022 di Indonesia harus diintegrasikan dengan kerangka business law untuk memastikan compliance yang berkelanjutan, di mana kegagalan dalam data protection dapat mengakibatkan denda administratif hingga Rp 2 miliar dan tuntutan class action yang merusak nilai saham. Menurut Khan[25] dalam esainya tentang antimonopoli dan privasi data, "*data privacy law and antitrust intersect in ways that challenge the dominant business models of platform companies, forcing a reevaluation of how data extraction fuels market power*". Pendekatan ini relevan di Indonesia, di mana pertumbuhan platform

[23] Luthiya, Irawan, and Yulia, "Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi."
[24] Garcia, "Predictive Analytics and the Collective Dimensions of Data Protection."
[25] L M Khan, "The New Antitrust/Data Privacy Law Interface," *Yale Law Journal Forum* 130 (2021): 388–414, https://yalelawjournal.org/pdf/DouglasEssay_pv1pt6ak.pdf.

digital berkontribusi 10% terhadap PDB, tetapi kasus kebocoran data Tokopedia 2020 menunjukkan bagaimana penyalahgunaan data dapat mengerosi kepercayaan investor dan memicu litigasi yang mahal.

Analisis hukum bisnis lebih lanjut mengungkap bahwa tanggung jawab platform atas penyalahgunaan data bersifat vicarious, di mana direktur dan eksekutif bertanggung jawab secara pribadi jika gagal menerapkan due diligence dalam pengelolaan data sebagai aset inti bisnis. Dari sudut pandang ini, penyalahgunaan data seperti pembagian ilegal dengan pihak ketiga untuk iklan targeted melanggar prinsip fair competition di bawah Undang-Undang No. 5 Tahun 1999 tentang Persaingan Usaha Tidak Sehat, yang selaras dengan analisis OECD[26] tentang persimpangan kompetisi dan privasi data, di mana "*online platforms leverage data for anticompetitive practices, necessitating integrated regulatory frameworks to balance innovation and consumer protection*". Di tingkat internasional, General Data Protection Regulation (GDPR) Uni Eropa telah memaksa platform global merevisi model bisnis mereka, dengan denda hingga 4% dari omzet global untuk pelanggaran, yang memengaruhi strategi ekspansi di pasar berkembang seperti Indonesia. Buku *Privacy and Cybersecurity Law Deskbook*[27] menekankan bahwa perusahaan platform harus mengadopsi "*risk-based compliance strategies*" untuk mitigasi liability, termasuk audit data rutin dan klausul indemnitas dalam kontrak mitra, guna menghindari tuntutan perdata yang dapat mencapai miliaran dolar, seperti kasus *Cambridge Analytica* yang merugikan Facebook hingga penurunan saham 10% pada 2018 dampak serupa yang terlihat pada platform lokal pasca-kasus BPJS Kesehatan 2021.

Untuk memperdalam analisis, berikut adalah poin-poin utama perspektif hukum bisnis terhadap penyalahgunaan data oleh perusahaan platform:

a) Dampak Ekonomi dan Governance Korporat
   Penyalahgunaan data menciptakan biaya tersembunyi bagi platform, termasuk peningkatan premi asuransi cyber dan penurunan valuasi merger & acquisition. Studi Liu dan Babar[28] dalam tinjauan sistematis tentang risiko cybersecurity korporat menemukan bahwa "*data breaches correlate with a 5-15% drop in market capitalization, underscoring the need for board-level oversight in business law frameworks*". Di Indonesia, ini berimplikasi pada Otoritas Jasa Keuangan (OJK) yang mewajibkan fintech menerapkan governance data untuk mencegah kegagalan sistemik, di mana UU PDP Pasal 35 memperkuat fiduciary duties direktur untuk melindungi data sebagai aset bisnis.
b) Persaingan Usaha dan Antimonopoli
   Platform sering menggunakan data untuk entry barriers, seperti algoritma yang memprioritaskan konten berbayar, yang melanggar prinsip non-

[26] Organisation for Economic Co-operation and Development (OECD), "The Intersection between Competition and Data Privacy" (OECD Publishing, 2024), https://one.oecd.org/document/DAF/COMP(2024)4/en/pdf.
[27] Edition), *Privacy and Cybersecurity Law Deskbook*.
[28] C Liu and M A Babar, "Corporate Cybersecurity Risk and Data Breaches: A Systematic Review of Empirical Research," *Australian Journal of Management*, 2024, https://doi.org/10.1177/03128962241293658.

discrimination. Griffin[29] dalam analisis Cornell Law Review menyatakan bahwa "*systemically important platforms must adhere to heightened corporate duties to prevent manipulative data practices that distort competition*". Di konteks Indonesia, Komisi Pengawas Persaingan Usaha (KPPU) dapat menerapkan Pasal 17 UU Persaingan Usaha untuk menangani kasus di mana data misuse menghambat UMKM bersaing dengan raksasa seperti Shopee.

c) Liability Perdata dan Pidana dalam Model Bisnis
Hukum bisnis menilai penyalahgunaan data sebagai perbuatan melawan hukum (*onrechtmatige daad*) di bawah KUHPerdata Pasal 1365, di mana konsumen dapat menuntut ganti rugi atas kerugian emosional dari profiling ilegal. Kim[30] dalam *Telecommunications Policy* menganalisis bahwa "*consumer data protection laws like CCPA force tech firms to pivot business models, reducing ad revenue by up to 20% while enhancing long-term sustainability*". Buku *A Legal Guide to Privacy and Data Security* 2025[31] merekomendasikan "*proactive contractual safeguard*s" untuk platform, termasuk privacy by design, guna mengurangi eksposur pidana di bawah UU ITE Pasal 32.

d) Implikasi Internasional dan Harmonisasi
Platform transnasional menghadapi fragmentasi regulasi, di mana GDPR bertabrakan dengan UU PDP, memerlukan strategi compliance global. Wang[32] dalam Encyclopedia MDPI berargumen bahwa "*regulation of data abuse in digital platforms requires a business-oriented approach to enforce user rights without stifling innovation*". Untuk ASEAN, *Digital Economy Framework Agreement* (DEFA) dapat menjadi model untuk Indonesia, memastikan platform seperti TikTok bertanggung jawab atas data lintas batas.

e) Rekomendasi Bisnis-Hukum
Perusahaan platform disarankan mengintegrasikan etika data ke dalam corporate social responsibility (CSR), dengan audit independen untuk mencegah breach. FTC[33] dalam laporan tentang praktik data media sosial menemukan bahwa "*platforms' failure to limit data collection creates avenues for abuse, impacting business ethics and regulatory scrutiny*".

Secara keseluruhan, analisis hukum bisnis menyoroti bahwa penyalahgunaan data oleh perusahaan platform bukan hanya ancaman hukum, melainkan peluang untuk reformasi model bisnis yang berkelanjutan, di mana compliance menjadi competitive advantage. Dengan mengadopsi kerangka seperti yang diuraikan dalam *Privacy and Cybersecurity Law Deskbook*[34], platform

[29] J P Griffin, "Systemically Important Platforms," *Cornell Law Review* 107, no. 5 (2022): 1265–1320, https://www.cornelllawreview.org/wp-content/uploads/2022/04/Griffin-final-1.pdf.
[30] Kim, "Consumer Data Protection Laws and Their Impact on Business Models of Technology Companies."
[31] GPM, *A Legal Guide to Privacy and Data Security 2025*.
[32] Z Wang, "Regulation of Data Abuse in Digital Platforms," *Encyclopedia* 3, no. 4 (2023): 1567–78, https://doi.org/10.3390/encyclopedia3040087.
[33] Federal Trade Commission (FTC), "Examining the Data Practices of Social Media and Video Streaming Services" (U.S. Federal Trade Commission, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf.
[34] Edition), *Privacy and Cybersecurity Law Deskbook*.

Indonesia dapat memitigasi risiko sambil mendukung pertumbuhan ekonomi digital yang diproyeksikan mencapai USD 130 miliar pada 2025. Namun, tanpa penegakan yang kuat dari Kementerian Kominfo dan KPPU, ketidakseimbangan ini akan terus merugikan konsumen dan UMKM, menuntut amendemen regulasi untuk sanksi progresif yang selaras dengan dinamika bisnis global.

3. Analisis Hukum atas Penyalahgunaan Data oleh Perusahaan Platform dalam Perspektif Cyber Law

Dalam perspektif cyber law, penyalahgunaan data oleh perusahaan platform digital seperti social media, e-commerce, dan fintech merupakan bentuk kejahatan siber yang mengancam keamanan nasional, privasi individu, dan integritas sistem informasi, di mana pengumpulan dan distribusi data tanpa otorisasi sering kali dieksploitasi untuk tujuan komersial ilegal atau serangan cyber. Cyber law memandang fenomena ini sebagai pelanggaran terhadap kerangka regulasi yang dirancang untuk melindungi ruang siber, termasuk Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) di Indonesia, yang selaras dengan konvensi internasional seperti Budapest Convention on Cybercrime. Analisis hukum ini menekankan tanggung jawab platform sebagai intermediary yang harus menerapkan *due diligence siber*, di mana kegagalan dalam pencegahan breach dapat dikategorikan sebagai akses ilegal atau distribusi informasi yang melanggar kesusilaan, dengan sanksi pidana hingga 6 tahun penjara berdasarkan UU ITE Pasal 32. Pada tingkat global, evolusi cyber law menyoroti peningkatan ancaman AI-driven data misuse, di mana platform seperti TikTok atau Meta menjadi target enforcement karena membagikan data sensitif tanpa consent, sebagaimana dibahas dalam laporan Gibson Dunn[35] yang menyatakan bahwa "*state comprehensive privacy laws continued to expand, with eight new laws taking effect... imposing obligations on data controllers (platforms) such as consumer rights to access, correct, delete data, and opt out of targeted advertising and sales.*" Perspektif ini krusial di Indonesia, di mana Badan Siber dan Sandi Negara (BSSN) mencatat lonjakan 300% kasus data breach antara 2020-2024, menuntut harmonisasi regulasi untuk menangani transnasionalitas platform asing.

Analisis hukum cyber law lebih lanjut mengungkap bahwa penyalahgunaan data oleh platform sering kali melibatkan elemen forensik digital dan traceability, di mana UU PDP Pasal 65 mewajibkan pelaporan breach dalam 72 jam, sementara UU ITE Pasal 26 melarang distribusi data pribadi tanpa hak. Dari sudut pandang ini, platform bertindak sebagai "*data fiduciaries*" yang rentan terhadap liability pidana jika gagal menerapkan enkripsi atau *zero-trust architecture*, mirip dengan kasus kebocoran data BPJS Kesehatan 2021 yang

[35] Gibson Dunn, "U.S. Cybersecurity and Data Privacy Review and Outlook – 2025," 2025, https://www.gibsondunn.com/us-cybersecurity-and-data-privacy-review-and-outlook-2025/.

memengaruhi 279 juta pengguna. Nag [36] dalam analisisnya tentang cyber law di India yang paralel dengan konteks ASEAN menekankan bahwa "*the Digital Personal Data Protection Act*, 2023, *marks a significant milestone... to regulate the collection, storage, and processing of personal data by both private entities and government institutions,*" yang menyoroti kebutuhan consent informed dan purpose limitation untuk mencegah misuse oleh platform. Di AS, enforcement FTC terhadap platform seperti InMarket Media pada 2025 mengharuskan penghancuran data lokasi sensitif, mengilustrasikan bagaimana cyber law berevolusi untuk menangani "*bulk U.S. sensitive personal data, which includes... precise geolocation data, biometric identifiers.*" Buku Lathrop GPM[37] menambahkan bahwa "*businesses should perform data mapping to find out what personal information they collect and for what purposes,*" sebagai langkah preventif cyber untuk menghindari tuntutan di bawah regulasi state seperti *California Consumer Privacy Act* (CCPA).

Untuk memperdalam analisis, berikut adalah poin-poin utama perspektif cyber law terhadap penyalahgunaan data oleh perusahaan platform:

a) Kerangka Hukum Pidana dan Administratif
Cyber law mengklasifikasikan *misuse* sebagai *cyber offense*, dengan UU ITE Pasal 66C tentang identity theft dan Pasal 66D tentang cheating by personation, yang relevan untuk platform yang memfasilitasi phishing via data curian. Nag [38] mengkritik bahwa "*the Act lacks clarity on issues like data portability, algorithmic accountability, and the legal status of emerging technologies like blockchain*," yang memperburuk celah di regulasi India dan serupa di Indonesia. Sanksi administratif UU PDP hingga Rp 2 miliar harus dilengkapi dengan forensik siber untuk traceability, sebagaimana diwajibkan oleh Konvensi Budapest.

b) Tanggung Jawab Intermediary dan *Due Diligence*
Platform sebagai intermediary kebal dari liability primer (UU ITE Pasal 15), tapi wajib hapus konten ilegal saat notified. Kasus Google India Pvt. Ltd. v. Visaka Industries menegaskan bahwa "*intermediaries are obliged to act with due diligence and must remove unlawful material upon receiving actual knowledge.*" Di 2025, FCC AS mendenda carrier wireless $200 juta atas sharing location data tanpa consent, menekankan "platforms' failure to limit data collection creates avenues for abuse."

c) Ancaman AI dan Deepfakes dalam Misuse Data
Integrasi AI mempercepat misuse, seperti profiling otomatis yang diskriminatif. Lathrop GPM (2025) mencatat bahwa di bawah CCPA, "*a potential claim under the CCPA may exceed $37.5 million*" untuk breach 50.000 records tanpa *security reasonable*, yang relevan untuk platform AI-driven.

[36] A Nag, "Cyber Law in 2025: Challenges and Legal Responses in the Age of AI, Data Breaches, and Digital Governance," *Journal of Emerging Technologies and Innovative Research* 12, no. 6 (2025), https://www.jetir.org/papers/JETIR2506616.pdf.
[37] GPM, *A Legal Guide to Privacy and Data Security 2025*.
[38] Nag, "Cyber Law in 2025: Challenges and Legal Responses in the Age of AI, Data Breaches, and Digital Governance."

Gibson Dunn [39] menyoroti *Maryland's Online Data Privacy Act* yang "*prohibit the sale of sensitive personal information entirely,*" termasuk data minor.

d) Enforcement dan Kolaborasi Internasional: Penegakan cyber law memerlukan kerjasama, seperti ASEAN DEFA untuk harmonisasi. Di AS, HHS OCR mendenda $1.19 juta atas HIPAA violations dari ransomware, di mana "*increasing frequency and sophistication of cyberattacks... pose a direct and significant threat to patient safety*." Di Indonesia, BSSN harus perkuat kapasitas forensik untuk kasus transborder.
e) Rekomendasi *Cyber Law Forward-Looking*: Platform wajib adopsi "*privacy by design*" dan audit siber tahunan. Lathrop GPM [40] merekomendasikan "*enhanced data security, limit personal data collected/stored, multi-factor authentication,*" untuk mitigasi breach.

Secara keseluruhan, analisis cyber law menegaskan bahwa penyalahgunaan data oleh platform adalah ancaman eksistensial bagi ruang siber, yang memerlukan regulasi adaptif seperti amendemen UU ITE untuk AI threats. Dengan proyeksi ekonomi digital Indonesia USD 130 miliar pada 2025, kegagalan enforcement dapat picu krisis kepercayaan, tapi kolaborasi global seperti yang diusulkan Nag[41] dapat membangun resilience siber yang kuat.

C. PENUTUP

Merujuk pada hasil pembahasan, maka dapat disimpulkan terkait artikel ini yaitu,

1. Data pribadi sebagai informasi identifikasi individu sesuai UU PDP Pasal 3 menekankan pentingnya pengakuan data sebagai aset krusial di era digital, sementara penyalahgunaan data pribadi didefinisikan sebagai pelanggaran pengolahan data tanpa persetujuan yang menimbulkan kerugian materil dan immateril.
2. Secara keseluruhan, perspektif hukum bisnis menggambarkan penyalahgunaan data sebagai ketidakseimbangan kekuasaan ekonomi yang mengganggu model bisnis berbasis data, di mana integrasi UU PDP dengan business law menjadi kunci compliance untuk menghindari denda hingga Rp 2 miliar dan litigasi class action.
3. Perspektif *cyber law* menyimpulkan penyalahgunaan data sebagai kejahatan siber eksistensial yang mengancam keamanan nasional dan integritas sistem, diatur UU ITE serta UU PDP yang selaras *Budapest Convention*, dengan lonjakan breach 300% oleh BSSN (2020-2024) menekankan tanggung jawab intermediary untuk *due diligence.*

[39] Dunn, "U.S. Cybersecurity and Data Privacy Review and Outlook – 2025."
[40] GPM, *A Legal Guide to Privacy and Data Security 2025*.
[41] Nag, "Cyber Law in 2025: Challenges and Legal Responses in the Age of AI, Data Breaches, and Digital Governance."

DAFTAR PUSTAKA

(FTC), Federal Trade Commission. "Examining the Data Practices of Social Media and Video Streaming Services." U.S. Federal Trade Commission, 2024. https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf.

(OECD), Organisation for Economic Co-operation and Development. "The Intersection between Competition and Data Privacy." OECD Publishing, 2024. https://one.oecd.org/document/DAF/COMP(2024)4/en/pdf.

Arkell, J, and et al. *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age*. Edited by 3rd ed. Practising Law Institute, 2023.

Cohen, J. "U.S. Cybersecurity and Data Privacy Review and Outlook – 2025." Gibson Dunn & Crutcher LLP, 2025.

Dunn, Gibson. "U.S. Cybersecurity and Data Privacy Review and Outlook – 2025," 2025. https://www.gibsondunn.com/us-cybersecurity-and-data-privacy-review-and-outlook-2025/.

Edition), Privacy and Cybersecurity Law Deskbook (2025. *Privacy and Cybersecurity Law Deskbook*. Edited by 2025 Edition. American Bar Association, 2025.

Garcia, M. "Predictive Analytics and the Collective Dimensions of Data Protection." *New Media & Society* 26, no. 5 (2024): 1234–56. https://doi.org/10.1080/17579961.2024.2313794.

GPM, Lathrop. *A Legal Guide to Privacy and Data Security 2025*. Lathrop GPM LLP, 2025.

Griffin, J P. "Systemically Important Platforms." *Cornell Law Review* 107, no. 5 (2022): 1265–1320. https://www.cornelllawreview.org/wp-content/uploads/2022/04/Griffin-final-1.pdf.

Johnson, R. "Data Privacy in the Digital Age: A Comparative Analysis of U.S. and EU Regulations." *UCLA Law Review* 72, no. 1 (2025): 45–78.

Khan, L M. "The New Antitrust/Data Privacy Law Interface." *Yale Law Journal Forum* 130 (2021): 388–414. https://yalelawjournal.org/pdf/DouglasEssay_pv1pt6ak.pdf.

Kim, S. "Consumer Data Protection Laws and Their Impact on Business Models of Technology Companies." *Telecommunications Policy* 48, no. 7 (2024): Article 102789. https://doi.org/10.1016/j.telpol.2024.102789.

Lee, J. "Complexities of AI Trends: Threats to Data Privacy Legal Compliance." *Seattle Journal of Technology, Environmental & Innovation Law* 15, no. 2 (2025): 210–35.

Liu, C, and M A Babar. "Corporate Cybersecurity Risk and Data Breaches: A Systematic Review of Empirical Research." *Australian Journal of Management*, 2024. https://doi.org/10.1177/03128962241293658.

Luthiya, A N, B Irawan, and R Yulia. "Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi." *Jurnal Hukum Pidana & Kriminologi* 12, no. 2 (2021): 150–70.

Marzuki, P M. *Penelitian Hukum: Edisi Revisi*. Prenada Media Group, 2023.

Nag, A. "Cyber Law in 2025: Challenges and Legal Responses in the Age of AI, Data Breaches, and Digital Governance." *Journal of Emerging Technologies and Innovative Research* 12, no. 6 (2025). https://www.jetir.org/papers/JETIR2506616.pdf.

Nuranisa, A, and D Lukitasari. "Analisa Kasus Kebocoran Data Pengguna Tokopedia." *Jurnal Hukum Progresif* 11, no. 2 (2024): 1928–40.

Reuters, Thompson. *Data Security and Privacy Law: Combating Cyber Threats*. Edited by 2024-2025 ed. Thomson Reuters, 2024.

Santoso, B. "Metodologi Penelitian Yuridis Normatif Dalam Analisis Cyber Law: Pendekatan Komparatif ASEAN." *Jurnal Hukum Dan Pembangunan* 54, no. 2 (2024): 245–67. https://doi.org/10.21143/jhp.vol54.no2.3456.

Schwartz, P M. *Privacy Law Fundamentals*. IAPP, 2024.

Siregar, H. "Perlindungan Hukum Bagi Pengguna Aplikasi Tokopedia Dari Penyalahgunaan Data Pribadi." *Jurnal Konstitusi Hukum Dan Kebijakan* 5, no. 1 (2024): 67–85.

Smith, A, and et al. "The Legal Implications of Data Privacy Laws, Cybersecurity Regulations and AI Ethics in a Digital Society." *International Journal of Law and Information Technology* 33, no. 3 (2025): 456–78. https://doi.org/10.1093/ijlit/eaad012.

Wang, Z. "Regulation of Data Abuse in Digital Platforms." *Encyclopedia* 3, no. 4 (2023): 1567–78. https://doi.org/10.3390/encyclopedia3040087.

Widjaja, T, and R Pratiwi. "Implikasi Hukum Terhadap Perlindungan Data Pribadi Dalam Transaksi Fintech Di Indonesia." *Jurnal Hukum Indonesia* 14, no. 2 (2023): 132–36.

Wijaya, A D, and T P Anggriawan. "Perlindungan Hukum Terhadap Data Pribadi Dalam Penggunaan Aplikasi Di Smartphone." *Inicio Legis* 5, no. 1 (2022): 45–62.