KAMPUS AKADEMIK PUBLISING
Jurnal Multidisiplin Ilmu Akademik (JMIA)
Vol.3, No.3 Juni 2026
e-ISSN: 3032-7377, p-ISSN : 3032-7385, Hal 951-964
DOI : https://doi.org/10.61722/jmia.v3i3.10512

IMPLEMENTASI UNDANG-UNDANG NOMOR 27 TAHUN 2022 TENTANG PERLINDUNGAN DATA PRIBADI DALAM MENJAMIN KEAMANAN DATA PRIBADI DI ERA DIGITAL

Arief Budiono[1], Malika Rahma Ulya[2*], Muhamad Arifai[3], Berlina Putri Romadhani[4]
[1-4] Fakultas Hukum dan Ilmu Politik, Universitas Muhammadiyah Surakarta
*Penulis Korespondensi: c100240073@student.ums.ac.id, c100240247@student.ums.ac.id, c100240251@student.ums.ac.id

Abstract. *The rapid development of information technology in the digital era triggers vulnerabilities in personal data security, highlighted by widespread data leaks and cybercrimes. This study aims to analyze the implementation of Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) in ensuring public data security in Indonesia. The method applied is normative legal research with statutory and conceptual approaches, analyzing secondary legal materials. The results indicate that the UU PDP provides a comprehensive legal framework to protect citizens' privacy rights. However, its implementation faces severe challenges, such as hacking and phishing attacks, data leaks in e-commerce and financial technology (fintech) platforms, and weak national cyber security policy coordination within the public sector. Strengthening data controller compliance, privacy trustmark certification, and integrating artificial intelligence are essential to mitigate cyber risks. Furthermore, regulatory synchronization between the UU PDP and the ITE Law is crucial to clarify criminal and civil sanctions for violators. In conclusion, the UU PDP 2022 is a fundamental legal instrument, but its effectiveness relies heavily on cybersecurity infrastructure readiness and law enforcement commitment..*

Keywords: *Personal Data Protection, Digital Era, UU PDP, Cyber Security, Cybercrime.*

Abstrak. Perkembangan teknologi informasi di era digital memicu kerentanan terhadap keamanan data pribadi, ditandai oleh maraknya kasus kebocoran data dan kejahatan siber. Penelitian ini bertujuan untuk menganalisis implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dalam menjamin keamanan data masyarakat di Indonesia. Metode yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan dan konseptual, menganalisis bahan hukum sekunder. Hasil penelitian menunjukkan bahwa UU PDP memberikan kerangka hukum yang komprehensif untuk melindungi hak privasi warga negara. Namun, implementasinya menghadapi tantangan berat seperti serangan peretasan dan phishing, kebocoran data di platform e-commerce dan financial technology (fintech), serta lemahnya koordinasi kebijakan keamanan siber nasional di sektor publik. Diperlukan penguatan kepatuhan pengendali data, sertifikat keandalan privasi, serta integrasi teknologi kecerdasan buatan (artificial intelligence) untuk memitigasi risiko siber. Selain itu, sinkronisasi regulasi antara UU PDP dan UU ITE sangat krusial dalam memperjelas sanksi pidana dan perdata bagi pelanggar. Kesimpulannya, UU PDP 2022 merupakan instrumen hukum yang sangat fundamental, tetapi efektivitasnya sangat bergantung pada kesiapan infrastruktur siber dan komitmen penegakan hukum.

Kata kunci: Perlindungan Data Pribadi, Era Digital, UU PDP, Keamanan Siber, Kejahatan Siber

1. LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi di era globalisasi saat ini telah membawa perubahan paradigma yang sangat masif dalam hampir setiap aspek kehidupan manusia. Transformasi digital tidak lagi sekadar menjadi instrumen penunjang aktivitas sehari-hari, melainkan telah menjelma menjadi fondasi utama dalam interaksi sosial, transaksi ekonomi, pelayanan publik, hingga tata kelola pemerintahan. Dalam lanskap yang serba digital ini, data pribadi telah bergeser nilainya menjadi salah satu aset komoditas paling berharga, atau yang sering diistilahkan dalam dunia ekonomi digital

Naskah Masuk: 28 Mei 2026; Revisi: 29 Mei 2026; Diterima: 30 Mei 2026; Terbit: 03 Juni 2026

sebagai minyak baru yang sangat bernilai.[1] Nilai ekonomis dan strategis dari data pribadi memicu pengumpulan, pemrosesan, dan analisis data dalam skala raksasa oleh berbagai entitas, baik korporasi multinasional, pelaku usaha rintisan, hingga institusi pemerintah. Namun, pemanfaatan data yang begitu masif ini sering kali tidak diimbangi dengan pemahaman dan tanggung jawab yang setara mengenai pentingnya menjaga kerahasiaan dan integritas data tersebut. Akibatnya, ketergantungan yang tinggi pada teknologi informasi melahirkan kerentanan baru yang mengancam kedaulatan individu atas informasi pribadinya sendiri.[2]

Secara filosofis, perlindungan terhadap data pribadi merupakan manifestasi nyata dari perlindungan hak atas privasi, yang merupakan bagian integral dari hak asasi manusia yang sangat fundamental. Hak privasi menuntut agar setiap individu memiliki kebebasan dan otoritas penuh untuk menentukan informasi apa saja mengenai dirinya yang boleh diketahui oleh publik, bagaimana informasi tersebut digunakan, dan kepada siapa informasi itu boleh dibagikan. Di Indonesia, jaminan terhadap hak atas privasi dan perlindungan diri sejati ini secara konstitusional telah diakomodasi dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, khususnya Pasal 28G Ayat (1) yang menegaskan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi. Konsep konstitusional ini mengamanatkan kepada negara untuk hadir dan memberikan jaminan perlindungan hukum yang efektif bagi setiap warga negaranya dari segala bentuk tindakan yang dapat mencederai harkat, martabat, dan privasi mereka di ruang siber yang tanpa batas.[3]

Namun, dalam realitas empiris di era siber saat ini, jaminan perlindungan tersebut terus menghadapi tantangan dan ancaman yang semakin kompleks dan destruktif. Fenomena kebocoran data, pencurian identitas, serangan peretasan sistem, manipulasi psikologis melalui skema penipuan digital, hingga eksploitasi data secara ilegal oleh pihak ketiga telah menjadi berita harian yang mencemaskan publik. Ancaman-ancaman ini tidak hanya menyasar sektor privat, seperti platform perdagangan elektronik (e-commerce) dan layanan teknologi finansial (fintech),[4] tetapi juga telah merambah dan melumpuhkan sistem basis data vital milik instansi pemerintah di sektor publik. Kebocoran data berskala nasional yang berulang kali terjadi menunjukkan bahwa infrastruktur keamanan siber di Indonesia masih memerlukan penguatan yang signifikan agar tidak rentan terhadap infiltrasi siber yang canggih. Kerugian yang ditimbulkan dari kejahatan siber ini tidak hanya bersifat material berupa kerugian finansial langsung bagi para korban, melainkan juga kerugian immaterial yang jauh lebih besar, seperti runtuhnya kepercayaan publik terhadap ekosistem digital nasional, rusaknya reputasi institusi,

[1] W Agustina and S A Wiraguna, "Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi Dari Kejahatan Peretasan," *Media Hukum Indonesia (MHI)* 2, no. 6 (2025): 117–27, https://doi.org/10.5281/zenodo.15486554.

[2] R S Ahmad, D A Puspaningtyas, and M N K Al Ismariy, "Perlindungan Hukum Terhadap Privasi Data Pribadi Di Era Digital," *Jurnal Ilmu Hukum "THE JURIS"* 9, no. 1 (2025): 15–23.

[3] N A Alfitri, Rahmawati, and Firmansyah, "Perlindungan Terhadap Data Pribadi Di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022," *Journal Social Society* 4, no. 2 (2024): 92–111, https://doi.org/10.30605/jss.4.2.2024.511.

[4] I W C Ardika, "Tinjauan Hukum Terhadap Perlindungan Data Pribadi Di Era Digital: Kasus Kebocoran Data Pengguna Layanan E-Commerce," *Indonesian Journal of Law and Justice* 2, no. 3 (2025): 1–11, https://doi.org/10.47134/ijlj.v2i3.3601.

hingga ancaman nyata terhadap keselamatan fisik akibat penyalahgunaan data untuk aksi kriminal lainnya seperti penipuan dan intimidasi.[5]

Sebelum disahkannya regulasi yang komprehensif, kondisi hukum perlindungan data pribadi di Indonesia berada dalam keadaan yang sangat memprihatinkan dan terfragmentasi. Aturan-aturan mengenai perlindungan data pribadi tersebar secara sektoral di puluhan peraturan perundang-undangan yang berbeda, mulai dari undang-undang administrasi kependudukan, undang-undang kesehatan, undang-undang perbankan, hingga undang-undang informasi dan transaksi elektronik. Sifat regulasi yang sektoral ini melahirkan ego sektoral antarlembaga, tumpang tindih kewenangan, ketidakkonsistenan definisi dan standar pengamanan data, serta tidak adanya kepastian mengenai mekanisme penyelesaian sengketa dan penegakan sanksi yang tegas bagi para pelanggar. Ketidakpastian hukum ini memicu kondisi darurat kebocoran data, di mana para korban kebocoran data kerap kali mengalami jalan buntu dalam menuntut keadilan, sementara para pengendali data seolah dapat dengan mudah melepaskan diri dari tanggung jawab hukum dengan dalih menjadi korban serangan siber dari pihak ketiga. Kebuntuan regulasi ini menuntut adanya sebuah reformasi hukum yang progresif dan integratif guna menyatukan seluruh instrumen perlindungan data pribadi ke dalam satu payung hukum yang kokoh.[6]

Menjawab urgensi dan kebutuhan mendesak tersebut, pemerintah bersama Dewan Perwakilan Rakyat akhirnya mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Pengesahan undang-undang ini menjadi tonggak sejarah yang sangat krusial dalam pembangunan sistem hukum siber di Indonesia. UU PDP hadir sebagai regulasi induk yang komprehensif yang mengadopsi prinsip-prinsip perlindungan data global, serupa dengan standar internasional yang berlaku di berbagai belahan dunia. Melalui regulasi ini, negara secara tegas menggeser paradigma perlindungan data dari yang semula bersifat sukarela dan sektoral menjadi kewajiban hukum yang ketat dan mengikat bagi setiap pengendali data pribadi dan prosesor data pribadi, baik yang berada di sektor publik maupun privat. UU PDP tidak hanya mendefinisikan secara jelas klasifikasi data pribadi yang bersifat umum dan spesifik, tetapi juga menggariskan hak-hak subjek data yang tidak dapat dikurangi, menetapkan kewajiban kepatuhan teknis dan organisasional yang harus dipenuhi oleh pengelola data, serta mengancam pelanggar dengan sanksi administratif dan pidana yang sangat berat.[7]

Meskipun UU PDP telah diundangkan dengan segala ekspektasi tinggi yang menyertainya, proses implementasi di lapangan masih dihadapkan pada jurang pemisah yang lebar antara teks hukum yang tertulis dan realitas sosial-teknologi di masyarakat. Keberadaan regulasi yang baik tidak serta-merta menghentikan gelombang kebocoran data jika tidak ditopang oleh kesiapan infrastruktur teknologi, penguatan kelembagaan pengawas yang independen, serta peningkatan budaya kepatuhan dari entitas pengelola

[5] L S Arief and R Purwanto, "Tinjauan Yuridis Undang-Undang Perlindungan Data Pribadi Tahun 2022 Dalam Menangani Kebocoran Data Pelanggan E-Commerce," *Pemuliaan Keadilan* 2, no. 3 (2025): 85–102, https://doi.org/10.62383/pk.v2i3.1019.

[6] B F Asherli and S A Wiraguna, "Perlindungan Keamanan Data Pribadi Di Era Digital Menghadapi Serangan Phishing Ditinjau Dari Undang-Undang Pelindungan Data Pribadi Nomor 27 Tahun 2022," *Jurnal Hukum, Administrasi Publik Dan Negara* 2, no. 4 (2025): 1–14, https://doi.org/10.62383/hukum.v2i4.290.

[7] N Bahtiar, "Darurat Kebocoran Data: Kebuntuan Regulasi Pemerintah," *Development Policy and Management Review (DPMR)* 2, no. 1 (2022): 85–100.

data. Banyak korporasi, terutama usaha mikro dan menengah, serta instansi-instansi pemerintah di daerah masih menghadapi kendala terkait investasi teknologi dan sumber daya manusia yang dibutuhkan untuk memenuhi standar keamanan yang diamanatkan oleh UU PDP.[8] Selain itu, rendahnya tingkat literasi digital dan kesadaran masyarakat mengenai pentingnya menjaga kerahasiaan data pribadi mereka sendiri membuat taktik manipulasi sosial masih sangat mudah memakan korban. Oleh karena itu, masa transisi penegakan UU PDP menuntut kerja keras seluruh pemangku kepentingan untuk mengubah cara pandang dan kebiasaan dalam mengelola data informasi sensitif secara lebih aman dan bertanggung jawab.[9]

Berdasarkan dinamika permasalahan tersebut, sangat penting untuk melakukan kajian akademis yang mendalam mengenai sejauh mana implementasi Undang-Undang Nomor 27 Tahun 2022 dapat berjalan secara efektif dalam menjamin keamanan data pribadi masyarakat di era digital. Penelitian ini memiliki relevansi yang sangat krusial di tengah masa transisi penegakan penuh UU PDP, di mana kesiapan semua lini sedang diuji oleh berbagai kasus kebocoran data yang terus berlanjut. Kajian ini difokuskan pada analisis komparatif, tantangan operasional di sektor privat (seperti e-commerce dan fintech) dan sektor publik, penanganan ancaman siber peretasan serta phishing, penyelarasan regulasi dengan UU ITE, urgensi sertifikasi keandalan privasi, hingga proyeksi pemanfaatan teknologi kecerdasan buatan dalam memperkuat sistem pertahanan data masa depan.[10] Melalui pembahasan yang komprehensif ini, penelitian ini diharapkan dapat memberikan kontribusi pemikiran akademis dan rekomendasi praktis bagi perbaikan kebijakan siber nasional, penyempurnaan implementasi regulasi, serta penguatan kesadaran kolektif demi terwujudnya kedaulatan data dan keamanan digital yang hakiki bagi seluruh rakyat Indonesia.[11]

2. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif (yuridis normatif) yang berfokus pada analisis terhadap norma-norma hukum positif, asas-asas hukum, serta doktrin yang berkaitan dengan perlindungan data pribadi. Pendekatan penelitian yang digunakan meliputi pendekatan perundang-undangan (*statute approach*) dengan menelaah Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi serta peraturan terkait lainnya, dan pendekatan konseptual (*conceptual approach*) untuk memahami esensi perlindungan hak atas privasi di era digital.[12]

Sumber data yang digunakan dalam penelitian ini adalah bahan hukum sekunder yang diperoleh melalui studi kepustakaan (*library research*). Bahan hukum sekunder

---

[8] I T Bua and N I Idris, "Analisis Kebijakan Keamanan Siber Di Indonesia: Studi Kasus Kebocoran Data Nasional Pada Tahun 2024," *Desentralisasi: Jurnal Hukum, Kebijakan Publik, Dan Pemerintahan* 2, no. 2 (2025): 100–114, https://doi.org/10.62383/desentralisasi.v2i2.653.

[9] Y Daeng et al., "Perlindungan Data Pribadi Dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi," *INNOVATIVE: Journal Of Social Science Research* 3, no. 6 (2023): 2898–2905, https://j-innovative.org/index.php/Innovative.

[10] M Fikri and S Rusdiana, "Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Positif Indonesia," *Ganesha Law Review* 5, no. 1 (2023): 39–57.

[11] H S Disemadi, "Urgensi Regulasi Khusus Dan Pemanfaatan Artificial Intelligence Dalam Mewujudkan Perlindungan Data Pribadi Di Indonesia," *Jurnal Wawasan Yuridika* 5, no. 2 (2021): 177–99, https://doi.org/10.25072/jwy.v5i2.460.

[12] R A Firdaus, "Perlindungan Hukum Dan Pencegahan Kejahatan Siber Di Era Digital Dalam Sistem Hukum Di Indonesia," *STAATSRECHT: Jurnal Hukum Kenegaraan Dan Politik Islam* 4, no. 1 (2024): 79–104.

tersebut terdiri dari jurnal-jurnal ilmiah hukum terpilih yang relevan dengan focus kajian perlindungan data pribadi, kejahatan siber, transaksi elektronik, dan analisis UU PDP di Indonesia. Teknik analisis data dilakukan secara kualitatif-deskriptif dengan mereduksi data, mengelompokkan secara tematis berdasarkan sub-bab pembahasan, menginterpretasikan secara kritis kesesuaian antara regulasi (*das sollen*) dan realitas empiris (*das sein*), serta menarik kesimpulan deduktif untuk menjawab permasalahan penelitian secara komprehensif.

3. HASIL DAN PEMBAHASAN

Urgensi Yuridis Perlindungan Hak Privasi Data Pribadi berdasarkan UU No. 27 Tahun 2022

Lahirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menandai pergeseran paradigma hukum yang sangat radikal dan progresif di Indonesia. Sebelum regulasi ini disahkan, perlindungan data pribadi di tanah air hanya ditempatkan sebagai bagian sekunder dari etika bisnis, regulasi administratif sektoral yang saling tumpang tindih, atau sekadar aturan pelengkap transaksi elektronik. Akibat dari fragmentasi tersebut, posisi tawar masyarakat sebagai pemilik data sangat lemah ketika berhadapan dengan korporasi raksasa maupun lembaga publik yang menguasai basis data mereka secara dominan. Secara konstitusional, negara memiliki kewajiban mutlak untuk melindungi segenap bangsa, termasuk menjaga harkat, martabat, dan hak atas rasa aman setiap warga negara dari segala bentuk ancaman dan penyalahgunaan informasi yang bersifat privat. Oleh karena itu, secara filosofis dan teoretis, perlindungan data pribadi merupakan derivasi langsung dari hak atas privasi yang bersifat fundamental. Hak ini tidak dapat dikurangi atau diabaikan dalam kondisi apa pun karena menyangkut kebebasan dasar manusia dan integritas personal di tengah masyarakat modern.[13]

Urgensi yuridis pertama dari undang-undang ini tercermin pada keberaniannya untuk melakukan klasifikasi data pribadi secara tegas ke dalam dua kelompok utama guna memberikan perlindungan hukum yang proporsional sesuai dengan tingkat risiko penyalahgunaan. Kelompok pertama adalah data pribadi yang bersifat spesifik. Klasifikasi ini mencakup data kesehatan, informasi biometrik, data genetika, orientasi seksual, pandangan politik, data anak, hingga data keuangan pribadi.[14] Penggolongan data-data tersebut ke dalam kategori spesifik didasarkan pada kesadaran hukum bahwa penyalahgunaan jenis data ini tidak hanya berpotensi merugikan pemilik data secara finansial, melainkan juga dapat berdampak langsung pada tindakan diskriminasi sosial, pengucilan, kerugian material yang ekstrem, serta trauma psikologis yang mendalam bagi pemilik data. Sementara itu, kelompok kedua adalah data pribadi yang bersifat umum, seperti nama lengkap, jenis kelamin, kewarganegaraan, agama, dan data pribadi yang dikombinasikan untuk mengidentifikasi seseorang. Pembedaan klasifikasi ini menjadi sangat penting karena menentukan ambang batas kepatuhan teknis dan standar pengamanan siber yang wajib dipenuhi oleh setiap pihak yang mengelola data tersebut,

[13] P H Harahap, "Perlindungan Data Pribadi Dalam Transaksi Digital: Implikasi Regulasi, Keamanan, Dan Efisiensi Dalam Perspektif Hukum Ekonomi Dan Hukum Islam," *Yurisprudentia: Jurnal Hukum Ekonomi* 11, no. 1 (2025): 1–23.

[14] G R Hidayah, H D Ma'shum, and M Awaluddin, "Studi Komparatif Perlindungan Data Pribadi Dalam UU ITE 2024 Dan UU PDP 2022," *Jurnal Riset Rumpun Ilmu Sosial, Politik Dan Humaniora (JURRISH)* 4, no. 4 (2025): 61–70, https://doi.org/10.55606/jurrish.v4i4.6341.

serta mempermudah penegak hukum dalam menilai tingkat kesalahan pelaku jika terjadi kebocoran data.[15]

Urgensi yuridis kedua terletak pada pergeseran asas tanggung jawab melalui pengenalan konsep pertanggungjawaban mutlak dan akuntabilitas aktif bagi para pengendali data. Di bawah rezim hukum yang lama, pengendali data sering kali dapat dengan mudah meloloskan diri dari tanggung jawab hukum ketika terjadi kebocoran data dengan dalih bahwa mereka adalah korban dari serangan siber pihak ketiga atau dengan mengambinghitamkan keterbatasan infrastruktur teknologi.[16] Kehadiran regulasi baru ini menutup celah tersebut dengan menegaskan bahwa pengendali data memiliki kewajiban hukum untuk membuktikan secara aktif bahwa mereka telah menerapkan standar keamanan teknis dan organisasional yang memadai di setiap siklus pemrosesan data, mulai dari pemerolehan, pemrosesan, penyimpanan, pengiriman, hingga pemusnahan data. Jika mereka gagal menunjukkan bukti kepatuhan tersebut saat terjadi kebocoran, maka mereka dapat langsung dinyatakan bersalah atas kelalaian hukum tanpa harus menunggu pembuktian niat jahat. Konsep ini menempatkan beban pembuktian terbalik yang sangat menguntungkan posisi masyarakat sebagai pemilik data yang dirugikan.[17]

Urgensi yuridis ketiga adalah penguatan dan perluasan hak-hak subjek data pribadi secara konkret dan dapat dieksekusi secara hukum. Regulasi ini memberikan jaminan hak yang sangat luas kepada masyarakat, termasuk hak untuk mendapatkan informasi yang jelas mengenai tujuan pemrosesan data, hak untuk memperbaiki kesalahan data mereka, hak untuk menarik kembali persetujuan penggunaan data secara mudah tanpa adanya intimidasi atau penalti, hak untuk membatasi pemrosesan data, hingga hak atas portabilitas data yang memungkinkan pemilik data memindahkan datanya dari satu sistem ke sistem lainnya secara aman. Selain itu, yang tidak kalah krusial adalah adanya jaminan hak untuk menuntut dan menerima ganti rugi atas pelanggaran perlindungan data pribadi yang disebabkan oleh kelalaian pengendali data. Pemberian hak-hak ini secara eksplisit dalam undang-undang tidak hanya memulihkan kedaulatan individu atas data pribadinya sendiri, tetapi juga menciptakan mekanisme penyeimbang yang memaksa para pelaku industri dan lembaga publik untuk memperlakukan data masyarakat dengan penuh kehati-hatian, kejujuran, dan transparansi yang tinggi, sehingga terbentuk sebuah tatanan interaksi digital nasional yang jauh lebih adil, beradab, dan berorientasi pada perlindungan hak asasi manusia.[18]

Perlindungan Hukum terhadap Kebocoran Data dalam Transaksi E-Commerce dan Finansial (Fintech)

Sektor perdagangan elektronik atau e-commerce dan teknologi finansial yang dikenal sebagai fintech saat ini telah bertransformasi menjadi tulang punggung utama pertumbuhan ekonomi digital nasional di Indonesia. Melalui jutaan transaksi harian, kedua sektor ini mengumpulkan, mengolah, mentransfer, serta menyimpan basis data

[15] A M Junaedi, "Urgensi Perlindungan Data Pribadi Dalam Era Digital: Analisis Undang-Undang Nomor 27 Tahun 2022," *KNOWLEDGE: Jurnal Inovasi Hasil Penelitian Dan Pengembangan* 5, no. 2 (2025): 247–57.

[16] A A N D H Kesuma, I N P Budiartha, and P A S Wesna, "Perlindungan Hukum Terhadap Keamanan Data Pribadi Konsumen Teknologi Finansial Dalam Transaksi Elektronik," *Jurnal Preferensi Hukum* 2, no. 2 (2021): 411–16, https://doi.org/10.22225/jph.2.2.3350.411-416.

[17] I M Kholis, "Perlindungan Data Pribadi Dan Keamanan Siber Di Sektor Perbankan: Studi Kritis Atas Penerapan UU PDP Dan UU ITE Di Indonesia," *STAATSRECHT: Jurnal Hukum Kenegaraan Dan Politik Islam* 4, no. 2 (2024): 275–300.

[18] H Kurniawati and Y Yunanto, "Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Debitur Dalam Aktivitas Pinjaman Online," *Jurnal Ius Constituendum* 7, no. 1 (2022): 102–14.

konsumen dalam volume raksasa, yang mencakup data identitas lengkap, alamat rumah, nomor telepon aktif, riwayat transaksi belanja, hingga informasi finansial yang sangat sensitif seperti nomor rekening bank, kartu kredit, dan rekam jejak keuangan pribadi. Kendati demikian, pertumbuhan masif aktivitas ekonomi ini sayangnya belum diimbangi dengan kesiapan infrastruktur siber dan kesadaran hukum yang setara dari pihak penyelenggara platform.[19] Data pribadi konsumen kerap kali diperlakukan sebatas komoditas bisnis untuk meningkatkan margin keuntungan atau instrumen pemasaran agresif, sehingga mengabaikan aspek keamanan berlapis yang wajib melekat padanya. Akibatnya, baik e-commerce maupun fintech menjadi sektor ekonomi yang paling sering diguncang oleh insiden kebocoran data skala luas, yang tidak hanya memicu kerugian finansial yang signifikan bagi pengguna, melainkan juga meruntuhkan kepercayaan masyarakat terhadap keandalan ekosistem digital nasional.

Kerentanan data pada platform e-commerce pada umumnya berakar dari lemahnya sistem enkripsi data yang digunakan, buruknya pengawasan tata kelola data internal terhadap hak akses karyawan, serta kegagalan dalam melakukan uji celah keamanan sistem siber secara berkala. Berbagai peristiwa kebocoran data berskala masif menunjukkan betapa mudahnya peretas mengeksploitasi sistem keamanan platform e-commerce terkemuka untuk mencuri basis data pengguna guna diperdagangkan di forum pasar gelap internet. Dampak yang ditimbulkan dari kebocoran ini sangat destruktif bagi konsumen sebagai subjek data. Data pribadi yang telah bocor tersebut kerap kali disalahgunakan oleh pihak ketiga yang tidak bertanggung jawab untuk melakukan tindak pidana rekayasa sosial seperti penipuan berkedok layanan pelanggan palsu, pengiriman barang fiktif dengan metode pembayaran di tempat, hingga pengambilalihan akun belanja dan dompet digital konsumen secara sepihak. Sebelum disahkannya instrumen perlindungan data pribadi yang komprehensif, konsumen berada dalam posisi tawar yang sangat lemah, mengingat tidak adanya mekanisme tanggung jawab mutlak yang dibebankan kepada pihak e-commerce serta besarnya beban pembuktian kerugian yang harus ditanggung secara mandiri oleh pihak konsumen yang minim literasi teknologi.[20]

Sementara itu, pada sektor teknologi finansial, khususnya dalam industri pinjaman online atau peer-to-peer lending, praktik penyalahgunaan data pribadi telah meluas hingga menyentuh batas-batas pelanggaran hak-hak dasar manusia yang sangat mengkhawatirkan. Banyak penyelenggara layanan pinjaman online, terutama yang beroperasi secara ilegal tanpa izin otoritas keuangan, merancang aplikasi mereka secara licik untuk menyadap, menyalin, dan mengakses daftar kontak telepon genggam, isi galeri foto, riwayat percakapan, hingga informasi lokasi debitur secara tidak sah.[21] Data sensitif tersebut kemudian dialihfungsikan sebagai alat pemerasan, intimidasi psikologis, dan teror sosial ketika debitur mengalami keterlambatan pembayaran kewajiban keuangan. Penagih utang tidak segan-segan menghubungi seluruh kontak yang berada di telepon debitur, menyebarkan informasi keuangan debitur dengan nada ancaman, membuat grup

[19] D E Mahameru et al., "Implementasi UU Perlindungan Data Pribadi Terhadap Keamanan Informasi Identitas Di Indonesia," *Jurnal Esensi Hukum* 5, no. 2 (2023): 115–31, https://doi.org/10.35866/esensihukum.v5i2.240.

[20] D Mulyadi et al., "Implementasi Kebijakan Pemerintah Terhadap Pencegahan Kebocoran Data Pribadi Dalam Pelayanan Publik Berbasis Digital," *Jurnal ISO: Jurnal Ilmu Sosial, Politik Dan Humaniora* 6, no. 1 (2026): 1–15, https://doi.org/10.53697/iso.v6il.3473.

[21] K Puspita, "Perlindungan Hukum Data Pribadi Konsumen Dalam Perjanjian Pinjaman Online Di Indonesia," *JURISPRUDENSI: Jurnal Ilmu Syari'ah, Perundang-Undangan Dan Ekonomi Islam* 15, no. 1 (2023): 71–87, https://doi.org/10.32505/jurisprudensi.v15i1.5478.

percakapan fitnah, bahkan memanipulasi foto pribadi dari galeri untuk meruntuhkan martabat sosial debitur di lingkungan kerjanya maupun keluarga. Dampak destruktif dari tindakan non-manusiawi ini telah memicu depresi mendalam bagi para korban, memutus mata pencaharian, mengisolasi korban dari kehidupan sosial, dan dalam skenario terburuk, menyebabkan korban mengambil tindakan ekstrem yang membahayakan nyawa mereka sendiri.[22]

Hadirnya regulasi baru perlindungan data pribadi di Indonesia memberikan arah perlindungan hukum yang jauh lebih tegas dan terstruktur untuk memangkas rantai eksploitasi data di kedua sektor digital vital ini. Dari aspek preventif, undang-undang secara kaku mensyaratkan bahwa setiap aktivitas pengumpulan dan pemrosesan data konsumen dalam transaksi digital wajib dilandasi oleh persetujuan eksplisit, terperinci, dan dinamis dari pihak subjek data. Platform e-commerce maupun aplikasi keuangan dilarang keras menyembunyikan klausul penggunaan data pribadi di balik lembaran syarat dan ketentuan penggunaan aplikasi yang bertele-tele dan sengaja dirancang rumit agar langsung disetujui konsumen tanpa dibaca. Selain itu, akses data yang tidak memiliki hubungan korelasi fungsional langsung dengan kegunaan layanan aplikasi harus dilarang secara mutlak. Aplikasi pinjaman online, misalnya, di bawah pengawasan regulasi baru ini dilarang keras menjadikan izin akses daftar kontak telepon dan foto pribadi sebagai syarat mutlak pencairan pinjaman, mengingat data pribadi semacam itu sama sekali tidak memiliki hubungan logis dengan proses penilaian kemampuan kredit calon debitur.

Dari sudut pandang penegakan hukum dan aspek represif, undang-undang ini meletakkan pondasi sanksi administratif dan tuntutan perdata yang sangat progresif guna memberikan efek jera yang nyata bagi para pelaku industri digital. Pihak penyelenggara e-commerce maupun korporasi fintech yang terbukti melakukan kelalaian dalam menjaga sistem keamanan data pribadi konsumen sehingga berujung pada insiden kebocoran data terancam dijatuhi sanksi administratif yang berlapis, mulai dari teguran tertulis, penghentian sementara seluruh kegiatan pemrosesan data pribadi, perintah pemusnahan data, hingga sanksi denda administratif yang sangat besar, yakni mencapai persentase tertentu dari total pendapatan tahunan korporasi tersebut. Sanksi denda yang berbasis persentase omzet tahunan korporasi ini merupakan langkah maju yang luar biasa, karena menekan perusahaan-perusahaan skala raksasa agar tidak lagi mengabaikan pertahanan siber konsumen hanya demi mengejar efisiensi anggaran korporasi. Melalui kolaborasi penegakan hukum antara Otoritas Jasa Keuangan dengan lembaga pengawas yang dibentuk khusus, korban kebocoran data siber kini dibekali hak konstitusional yang sah untuk mengajukan gugatan ganti rugi secara materiil maupun immateriil atas segala kerugian yang mereka alami akibat kegagalan tata kelola data pelaku usaha, menciptakan keseimbangan baru yang adil di dalam lanskap transaksi digital nasional.[23]

Keamanan Siber dan Penanganan Ancaman Digital (Peretasan dan Phishing)

Perkembangan metode kejahatan siber saat ini berjalan jauh lebih cepat dibandingkan dengan pengembangan sistem hukum konvensional. Dua jenis ancaman digital yang terus menjadi momok menakutkan bagi keamanan data nasional adalah peretasan sistem pertahanan siber dan teknik penipuan berbasis manipulasi psikologis yang dikenal sebagai phishing. Peretasan menyasar langsung pada infrastruktur dan

[22] A Putri et al., "Keamanan Online Dalam Media Sosial: Pentingnya Perlindungan Data Pribadi Di Era Digital (Studi Kasus Desa Pematang Jering)," *Jurnal Pengabdian Nasional (JPN) Indonesia* 6, no. 1 (2025): 38–52, https://doi.org/10.35870/jpni.v6i1.1097.

[23] F Rifa and M N Hidayati, "Kebijakan Penal Dalam Perlindungan Data Pribadi Nasabah Fintech Lending Di Indonesia," *Binamulia Hukum* 13, no. 2 (2024): 461–81, https://doi.org/10.37893/jbh.v13i2.964.

server utama penyimpan data untuk mencuri atau merusak basis data secara massal melalui eksploitasi celah keamanan teknologi. Di sisi lain, phishing menyasar sisi terlemah dari rantai keamanan siber, yaitu manusia, dengan cara mengelabui korban melalui pesan atau tautan palsu agar secara sukarela menyerahkan informasi rahasia mereka.[24]

Sektor perbankan dan lembaga keuangan formal merupakan target utama dari kedua kejahatan siber ini. Sifat dari industri perbankan yang sangat mengandalkan kepercayaan publik menuntut adanya sistem pertahanan siber dengan keandalan tanpa celah. Kelalaian kecil dalam sistem perbankan dapat memicu kerugian finansial yang masif serta mengikis stabilitas sistem keuangan nasional. Oleh karena itu, pengamanan data tidak boleh hanya bertumpu pada pembangunan perangkat lunak pertahanan siber yang mutakhir, melainkan juga harus diiringi dengan sosialisasi dan edukasi literasi keamanan informasi yang berkelanjutan kepada seluruh nasabah sebagai pemilik data pribadi agar tidak mudah terjebak skema manipulasi digital.

Regulasi perlindungan data pribadi mengantisipasi ancaman ini dengan menetapkan kewajiban bagi setiap pengendali data untuk menerapkan standar pengamanan teknis terbaik, termasuk penggunaan enkripsi data yang kuat dan pengujian kerentanan sistem secara berkala. Hal yang paling krusial adalah kewajiban hukum untuk melaporkan setiap kejadian kegagalan sistem keamanan kepada pemilik data dan lembaga pengawas dalam waktu yang sangat singkat, yaitu tidak lebih dari tujuh puluh dua jam sejak kegagalan tersebut terdeteksi. Kewajiban pelaporan cepat ini sangat penting guna meminimalkan penyebaran dampak buruk serta memberikan kesempatan bagi pemilik data untuk segera mengambil tindakan pengamanan mandiri, seperti mengubah kata sandi atau memblokir akses keuangan mereka.[25]

Tantangan Kebocoran Data Nasional, Kebijakan Siber, dan Penerapan Kebijakan Sektor Publik

Tantangan terbesar dalam menegakkan kedaulatan data di Indonesia justru sering kali bersumber dari sektor pelayanan publik atau lembaga pemerintah itu sendiri. Berbagai kasus kebocoran data berskala nasional yang melibatkan basis data kependudukan, data jaminan kesehatan nasional, hingga lumpuhnya pusat data nasional akibat serangan siber menjadi bukti nyata bahwa infrastruktur siber sektor publik sangat rapuh. Lemahnya koordinasi antarlembaga negara, birokrasi yang kaku, serta minimnya anggaran pertahanan siber pada tingkat kementerian maupun pemerintah daerah menjadi faktor utama yang membuat data sensitif milik jutaan warga negara dengan sangat mudah diretas dan diperjualbelikan di forum pasar gelap.[26]

Proses digitalisasi pelayanan publik yang berjalan sangat masif tanpa diimbangi kesiapan pengamanan siber yang setara melahirkan bahaya baru yang mengancam ketahanan nasional. Banyak daerah yang berlomba-lomba membuat aplikasi pelayanan publik berbasis digital demi mengejar citra kemajuan administrasi, namun mengabaikan aspek keamanan data dasar penggunanya. Kurangnya pemahaman serta rendahnya standar literasi keamanan siber di kalangan aparatur sipil negara yang bertugas sebagai

[24] J N Saly et al., "Analisis Perlindungan Data Pribadi Terkait UU No. 27 Tahun 2022," *Jurnal Serina Sosial Humaniora* 1, no. 3 (2023): 145–53, https://doi.org/10.24912/jssh.v1i3.28615.
[25] Z A Savitri, M Amirulloh, and M Susanto, "Urgensi Sertifikat Keandalan Privasi Dalam Menghadapi Kebocoran Data Pribadi," *Jurnal USM Law Review* 8, no. 1 (2025): 235–53.
[26] P H Simanjuntak, "Perlindungan Hukum Terhadap Data Pribadi Pada Era Digital Di Indonesia: Studi Undang-Undang Perlindungan Data Pribadi Dan General Data Protection Regulation (GDPR)," *Jurnal Esensi Hukum* 6, no. 2 (2024): 105–24.

pengelola data membuat sistem informasi publik menjadi sasaran empuk yang sangat mudah disusupi oleh pihak-pihak yang tidak bertanggung jawab.

Berdasarkan ketentuan dalam Undang-Undang Perlindungan Data Pribadi, lembaga sektor publik memiliki kedudukan, hak, dan kewajiban hukum yang sama persis dengan badan hukum privat dalam mengelola data pribadi warga negara. Pemerintah tidak boleh memiliki kekebalan hukum atau membebaskan diri dari tanggung jawab moral dan materi ketika terjadi kebocoran data pada instansi mereka. Reformasi kebijakan siber nasional harus segera dilakukan secara radikal dengan mengintegrasikan sistem keamanan siber pada seluruh instansi negara di bawah satu komando koordinasi yang kuat. Langkah ini krusial untuk mengembalikan kepercayaan publik terhadap tata kelola pemerintahan berbasis digital serta menjamin keselamatan data seluruh rakyat Indonesia.[27]

Studi Komparatif dan Kelembagaan: UU PDP 2022, UU ITE, dan Sertifikasi Keandalan Privasi

Keberhasilan implementasi suatu undang-undang sangat bergantung pada kejelasan hubungan normatif antar-regulasi sejenis agar tidak menimbulkan tumpang tindih kewenangan atau ketidakpastian hukum di tingkat penegakan siber. Di Indonesia, terdapat irisan regulasi yang sangat tebal antara Undang-Undang Perlindungan Data Pribadi dengan Undang-Undang Informasi dan Transaksi Elektronik yang baru saja mengalami pembaruan. Ketidaksinkronan rumusan sanksi dan dualisme definisi operasional mengenai pelanggaran siber di antara kedua aturan ini berpotensi membingungkan aparat penegak hukum dan memperlambat proses pencarian keadilan bagi para korban kebocoran data.[28]

Jika dibandingkan secara global, penyusunan undang-undang perlindungan data di Indonesia banyak mengadopsi prinsip-prinsip hukum yang tertuang dalam regulasi perlindungan data milik Uni Eropa yang dikenal sangat ketat di tingkat internasional. Kedua sistem hukum ini sama-sama menganut asas ekstrateritorial yang memungkinkan hukum nasional menjangkau pelanggar data yang berada di luar batas wilayah negara asalkan tindakan mereka berdampak pada warga negara di dalam negeri. Namun, perbedaan yang sangat mendasar terletak pada kesiapan pembentukan lembaga pengawas independen yang memiliki otoritas penuh untuk menjatuhkan sanksi administratif dan melakukan audit kepatuhan tanpa campur tangan kepentingan politik praktis.

Guna menjamin kepatuhan industri secara sukarela sebelum terjadinya pelanggaran, instrumen sertifikasi keandalan privasi perlu segera didorong menjadi standar wajib baru bagi seluruh korporasi pengelola data di Indonesia. Sertifikasi ini berfungsi sebagai pengakuan resmi bahwa suatu organisasi telah menerapkan standar keamanan informasi dan perlindungan privasi yang setara dengan praktik terbaik global. Dengan adanya skema sertifikasi berkala yang diawasi langsung oleh lembaga pengawas independen, industri akan terdorong untuk terus meningkatkan kualitas pertahanan data mereka secara mandiri, sehingga dapat menurunkan risiko terjadinya kebocoran data secara signifikan di masa mendatang.[29]

---

[27] K R A Suari and I M Sarjana, "Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi Di Indonesia," *Jurnal Analisis Hukum (JAH)* 6, no. 1 (2023): 132–46, https://doi.org/10.38043/jah.v6i1.4484.

[28] S M T Situmeang, "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber," *SASI* 27, no. 1 (2021): 38–52.

[29] F Yulenrivo, B Azheri, and Yulfasni, "Perlindungan Hukum Terhadap Konsumen Pengguna Pinjaman Online Berbasis Financial Technology Oleh Otoritas Jasa Keuangan," *UNES LAW REVIEW* 6, no. 1 (2023): 1312–23, https://doi.org/10.31933/unesrev.v6i1.

Pemanfaatan Teknologi Informasi, Artificial Intelligence, dan Masa Depan Perlindungan Data di Era Digital

Menatap masa depan pertahanan siber di era digital yang semakin kompleks, pendekatan hukum yang bersifat konvensional dan pasif dinilai tidak akan pernah cukup untuk menandingi lompatan kemajuan teknologi yang berjalan secara eksponensial. Salah satu disrupsi terbesar yang membawa pengaruh sangat signifikan bagi keamanan data pribadi adalah kehadiran teknologi kecerdasan buatan. Di satu sisi, kecerdasan buatan menawarkan solusi luar biasa melalui kemampuannya mendeteksi pola serangan siber secara otomatis, menganalisis ancaman secara waktu nyata, dan melakukan enkripsi dinamis; namun di sisi lain, teknologi ini juga berpotensi disalahgunakan oleh pelaku kejahatan siber untuk merancang jenis serangan baru yang jauh lebih canggih dan sulit dideteksi.

Penyalahgunaan data pribadi di masa depan tidak lagi berupa pencurian identitas sederhana, melainkan telah berevolusi menjadi bentuk kejahatan siber yang sangat sempurna. Dengan bantuan teknologi kecerdasan buatan, data pribadi masyarakat yang bocor dianalisis secara mendalam untuk memetakan perilaku psikologis, memanipulasi opini publik secara massal melalui disinformasi yang disesuaikan secara personal, hingga menciptakan teknik penipuan berbasis rekayasa sosial yang sangat presisi dan sulit dibedakan dari komunikasi asli. Kondisi ini menuntut cakupan perlindungan hukum positif di Indonesia untuk terus diperbarui secara dinamis agar tidak tertinggal oleh cepatnya evolusi teknologi siber tersebut.

Di samping penguatan teknologi siber dan regulasi hukum, benteng pertahanan utama dan paling mendasar dari keamanan data pribadi tetap berada pada tingkat kesadaran individu itu sendiri. Kebiasaan masyarakat yang sering membagikan informasi sensitif secara berlebihan di media sosial tanpa memikirkan konsekuensi jangka panjangnya harus segera diubah melalui gerakan literasi digital nasional yang masif. Perlindungan data pribadi di masa depan tidak akan pernah tercapai secara maksimal jika hanya mengandalkan tindakan hukum yang bersifat represif setelah kebocoran terjadi. Keamanan data yang hakiki hanya dapat terwujud melalui kolaborasi yang sinergis antara regulasi hukum yang progresif, penerapan teknologi keamanan berbasis kecerdasan buatan yang andal, serta kesadaran aktif dari setiap warga negara sebagai pemilik sah atas data pribadi mereka.[30]

4. KESIMPULAN DAN SARAN

Implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan langkah revolusioner sekaligus kebutuhan mutlak dalam menjamin kedaulatan digital dan keamanan hak privasi warga negara Indonesia di era digital. Sebagai payung hukum utama, UU PDP telah menetapkan standar kewajiban yang jelas bagi pengendali data, mengkategorikan data secara spesifik, serta menyediakan instrumen sanksi administratif dan pidana yang berat bagi para pelanggar.

Namun, efektivitas implementasi UU PDP di lapangan masih dihadapkan pada tantangan besar. Pertama, rentannya sektor e-commerce dan fintech terhadap kebocoran data nasabah dan intimidasi penagihan ilegal. Kedua, tingginya intensitas serangan siber seperti peretasan dan phishing. Ketiga, masih lemahnya pertahanan siber sektor publik/lembaga negara yang terbukti dari kebocoran data nasional berulang kali.

[30] A A Zaman, J Anwar, and A Fadlian, "Pertanggung Jawaban Pidana Kebocoran Data BPJS Dalam Perspektif UU ITE," *De Juncto Delictio* 1, no. 2 (2021): 146–57.

Keempat, urgensi kelembagaan untuk segera mengoperasikan lembaga pengawas independen serta menyinkronkan UU PDP dengan regulasi lain seperti UU ITE.

Untuk memaksimalkan perlindungan data pribadi ke depan, direkomendasikan penguatan tata kelola keamanan siber berbasis kecerdasan buatan (AI), kewajiban sertifikasi keandalan privasi (*privacy trustmark*) bagi korporasi pengelola data, peningkatan kompetensi aparat penegak hukum, serta edukasi literasi digital secara konsisten kepada seluruh lapisan masyarakat Indonesia selaku subjek data pribadi.

DAFTAR REFERENSI

Agustina, W, and S A Wiraguna. "Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi Dari Kejahatan Peretasan." *Media Hukum Indonesia (MHI)* 2, no. 6 (2025): 117–27. https://doi.org/10.5281/zenodo.15486554.

Ahmad, R S, D A Puspaningtyas, and M N K Al Ismariy. "Perlindungan Hukum Terhadap Privasi Data Pribadi Di Era Digital." *Jurnal Ilmu Hukum "THE JURIS"* 9, no. 1 (2025): 15–23.

Alfitri, N A, Rahmawati, and Firmansyah. "Perlindungan Terhadap Data Pribadi Di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022." *Journal Social Society* 4, no. 2 (2024): 92–111. https://doi.org/10.30605/jss.4.2.2024.511.

Ardika, I W C. "Tinjauan Hukum Terhadap Perlindungan Data Pribadi Di Era Digital: Kasus Kebocoran Data Pengguna Layanan E-Commerce." *Indonesian Journal of Law and Justice* 2, no. 3 (2025): 1–11. https://doi.org/10.47134/ijlj.v2i3.3601.

Arief, L S, and R Purwanto. "Tinjauan Yuridis Undang-Undang Perlindungan Data Pribadi Tahun 2022 Dalam Menangani Kebocoran Data Pelanggan E-Commerce." *Pemuliaan Keadilan* 2, no. 3 (2025): 85–102. https://doi.org/10.62383/pk.v2i3.1019.

Asherli, B F, and S A Wiraguna. "Perlindungan Keamanan Data Pribadi Di Era Digital Menghadapi Serangan Phishing Ditinjau Dari Undang-Undang Pelindungan Data Pribadi Nomor 27 Tahun 2022." *Jurnal Hukum, Administrasi Publik Dan Negara* 2, no. 4 (2025): 1–14. https://doi.org/10.62383/hukum.v2i4.290.

Bahtiar, N. "Darurat Kebocoran Data: Kebuntuan Regulasi Pemerintah." *Development Policy and Management Review (DPMR)* 2, no. 1 (2022): 85–100.

Bua, I T, and N I Idris. "Analisis Kebijakan Keamanan Siber Di Indonesia: Studi Kasus Kebocoran Data Nasional Pada Tahun 2024." *Desentralisasi: Jurnal Hukum, Kebijakan Publik, Dan Pemerintahan* 2, no. 2 (2025): 100–114. https://doi.org/10.62383/desentralisasi.v2i2.653.

Daeng, Y, N Linra, A Darham, D Handrianto, R R Sianturi, D Martin, R P Putra, and H Saputra. "Perlindungan Data Pribadi Dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi." *INNOVATIVE: Journal Of Social Science Research* 3, no. 6 (2023): 2898–2905. https://j-innovative.org/index.php/Innovative.

Disemadi, H S. "Urgensi Regulasi Khusus Dan Pemanfaatan Artificial Intelligence Dalam Mewujudkan Perlindungan Data Pribadi Di Indonesia." *Jurnal Wawasan Yuridika* 5, no. 2 (2021): 177–99. https://doi.org/10.25072/jwy.v5i2.460.

Fikri, M, and S Rusdiana. "Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Positif Indonesia." *Ganesha Law Review* 5, no. 1 (2023): 39–57.

Firdaus, R A. "Perlindungan Hukum Dan Pencegahan Kejahatan Siber Di Era Digital Dalam Sistem Hukum Di Indonesia." *STAATSRECHT: Jurnal Hukum Kenegaraan Dan Politik Islam* 4, no. 1 (2024): 79–104.

Harahap, P H. "Perlindungan Data Pribadi Dalam Transaksi Digital: Implikasi Regulasi, Keamanan, Dan Efisiensi Dalam Perspektif Hukum Ekonomi Dan Hukum Islam." *Yurisprudentia: Jurnal Hukum Ekonomi* 11, no. 1 (2025): 1–23.

Hidayah, G R, H D Ma'shum, and M Awaluddin. "Studi Komparatif Perlindungan Data Pribadi Dalam UU ITE 2024 Dan UU PDP 2022." *Jurnal Riset Rumpun Ilmu Sosial, Politik Dan Humaniora (JURRISH)* 4, no. 4 (2025): 61–70. https://doi.org/10.55606/jurrish.v4i4.6341.

Junaedi, A M. "Urgensi Perlindungan Data Pribadi Dalam Era Digital: Analisis Undang-Undang Nomor 27 Tahun 2022." *KNOWLEDGE: Jurnal Inovasi Hasil Penelitian Dan Pengembangan* 5, no. 2 (2025): 247–57.

Kesuma, A A N D H, I N P Budiartha, and P A S Wesna. "Perlindungan Hukum Terhadap Keamanan Data Pribadi Konsumen Teknologi Finansial Dalam Transaksi Elektronik." *Jurnal Preferensi Hukum* 2, no. 2 (2021): 411–16. https://doi.org/10.22225/jph.2.2.3350.411-416.

Kholis, I M. "Perlindungan Data Pribadi Dan Keamanan Siber Di Sektor Perbankan: Studi Kritis Atas Penerapan UU PDP Dan UU ITE Di Indonesia." *STAATSRECHT: Jurnal Hukum Kenegaraan Dan Politik Islam* 4, no. 2 (2024): 275–300.

Kurniawati, H, and Y Yunanto. "Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Debitur Dalam Aktivitas Pinjaman Online." *Jurnal Ius Constituendum* 7, no. 1 (2022): 102–14.

Mahameru, D E, A Nurhalizah, A Wildan, M H Badjeber, and M H Rahmadia. "Implementasi UU Perlindungan Data Pribadi Terhadap Keamanan Informasi Identitas Di Indonesia." *Jurnal Esensi Hukum* 5, no. 2 (2023): 115–31. https://doi.org/10.35866/esensihukum.v5i2.240.

Mulyadi, D, A Mulyana, A Carmenita, H L Utami, K A Aulia, M Putri, and N R Alia. "Implementasi Kebijakan Pemerintah Terhadap Pencegahan Kebocoran Data Pribadi Dalam Pelayanan Publik Berbasis Digital." *Jurnal ISO: Jurnal Ilmu Sosial, Politik Dan Humaniora* 6, no. 1 (2026): 1–15. https://doi.org/10.53697/iso.v6il.3473.

Puspita, K. "Perlindungan Hukum Data Pribadi Konsumen Dalam Perjanjian Pinjaman Online Di Indonesia." *JURISPRUDENSI: Jurnal Ilmu Syari'ah, Perundang-Undangan Dan Ekonomi Islam* 15, no. 1 (2023): 71–87. https://doi.org/10.32505/jurisprudensi.v15i1.5478.

Putri, A, N Sari, P Fajrina, and S Aisyah. "Keamanan Online Dalam Media Sosial: Pentingnya Perlindungan Data Pribadi Di Era Digital (Studi Kasus Desa Pematang Jering)." *Jurnal Pengabdian Nasional (JPN) Indonesia* 6, no. 1 (2025): 38–52. https://doi.org/10.35870/jpni.v6i1.1097.

Rifa, F, and M N Hidayati. "Kebijakan Penal Dalam Perlindungan Data Pribadi Nasabah Fintech Lending Di Indonesia." *Binamulia Hukum* 13, no. 2 (2024): 461–81. https://doi.org/10.37893/jbh.v13i2.964.

Saly, J N, H Artamevia, K Kheista, B J S Gulo, E A Rhemrev, and M Christie. "Analisis Perlindungan Data Pribadi Terkait UU No. 27 Tahun 2022." *Jurnal Serina Sosial Humaniora* 1, no. 3 (2023): 145–53. https://doi.org/10.24912/jssh.v1i3.28615.

Savitri, Z A, M Amirulloh, and M Susanto. "Urgensi Sertifikat Keandalan Privasi Dalam Menghadapi Kebocoran Data Pribadi." *Jurnal USM Law Review* 8, no. 1 (2025): 235–53.

Simanjuntak, P H. "Perlindungan Hukum Terhadap Data Pribadi Pada Era Digital Di Indonesia: Studi Undang-Undang Perlindungan Data Pribadi Dan General Data Protection Regulation (GDPR)." *Jurnal Esensi Hukum* 6, no. 2 (2024): 105–24.

Situmeang, S M T. "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber." *SASI* 27, no. 1 (2021): 38–52.

Suari, K R A, and I M Sarjana. "Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi Di Indonesia." *Jurnal Analisis Hukum (JAH)* 6, no. 1 (2023): 132–46. https://doi.org/10.38043/jah.v6i1.4484.

Yulenrivo, F, B Azheri, and Yulfasni. "Perlindungan Hukum Terhadap Konsumen Pengguna Pinjaman Online Berbasis Financial Technology Oleh Otoritas Jasa Keuangan." *UNES LAW REVIEW* 6, no. 1 (2023): 1312–23. https://doi.org/10.31933/unesrev.v6i1.

Zaman, A A, J Anwar, and A Fadlian. "Pertanggung Jawaban Pidana Kebocoran Data BPJS Dalam Perspektif UU ITE." *De Juncto Delictio* 1, no. 2 (2021): 146–57