Pertanggungjawaban Pidana Atas Kebocoran Data Pribadi Oleh Penyelenggara Sistem Elektronik Dalam Perspektif UU Perlindungan Data Pribadi

Hasan Husri[1], La Gurusi[2], Samsul[3]
[123]Fakultas Hukum, Universitas Muhammadiyah Buton, Baubau
hasanhusri301@gmail.com[1]

ABSTRACT

The rapid advancement of information and communication technology has significantly increased the use of electronic systems in personal data management, while simultaneously heightening the risk of data breaches that may harm individuals and threaten privacy rights. This study aims to analyze the regulation of criminal liability for personal data breaches by electronic system providers and its application under Law Number 27 of 2022 on Personal Data Protection. Employing a normative juridical method, this research examines relevant legislation and legal literature. The findings indicate that the law provides a comprehensive framework governing data subject rights, data controller obligations, and criminal sanctions for violations. Criminal liability may be imposed on both individuals and corporations when unlawful conduct and fault are established. However, enforcement faces challenges, including evidentiary difficulties, technological complexity, and limited law enforcement capacity. Therefore, strengthening implementation and compliance is essential to enhance the effectiveness of personal data protection.

Keywords: *Criminal Liability; Personal Data Protection; Data Breach; Electronic Systems*

RINGKASAN

Perkembangan pesat teknologi informasi telah meningkatkan penggunaan sistem elektronik dalam pengelolaan data pribadi, namun juga memperbesar risiko kebocoran data yang dapat merugikan individu dan mengancam privasi. Penelitian ini bertujuan menganalisis pengaturan pertanggungjawaban pidana atas kebocoran data pribadi oleh penyelenggara sistem elektronik serta penerapannya dalam kerangka Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Metode yang digunakan adalah yuridis normatif dengan pendekatan peraturan perundang-undangan dan literatur terkait. Hasil penelitian menunjukkan bahwa UU PDP telah mengatur secara komprehensif hak subjek data, kewajiban pengendali data, serta sanksi pidana atas pelanggaran. Pertanggungjawaban pidana dapat dikenakan kepada individu maupun korporasi apabila terbukti adanya perbuatan melawan hukum dan kesalahan. Namun, penegakannya masih menghadapi kendala seperti pembuktian, kompleksitas teknologi, dan keterbatasan

kapasitas penegak hukum. Oleh karena itu, diperlukan penguatan implementasi dan kepatuhan untuk meningkatkan efektivitas perlindungan data pribadi.

Kata kunci: Pertanggungjawaban Pidana; Perlindungan Data Pribadi; Kebocoran Data; Sistem Elektronik

A. Pendahuluan

Indonesia Perkembangan teknologi informasi dan komunikasi pada era digital telah membawa perubahan mendasar dalam berbagai aspek kehidupan manusia, terutama dalam cara masyarakat mengolah, menyimpan, dan mendistribusikan informa[1]. Pemanfaatan sistem elektronik kini menjadi tulang punggung dalam kegiatan ekonomi, pemerintahan, pendidikan, kesehatan, hingga interaksi sosial sehari-hari. Kondisi ini mendorong lahirnya berbagai platform digital, baik dalam bentuk aplikasi maupun sistem basis data terintegrasi, yang mengelola dan menyimpan data pribadi dalam skala besar. Data pribadi tersebut meliputi identitas diri, informasi kontak, data biometrik, data keuangan, hingga rekam medis. Keberadaan data pribadi di dalam sistem elektronik menimbulkan konsekuensi hukum yang signifikan, terutama terkait dengan perlindungan data pribadi dan pertanggungjawaban pihak-pihak yang terlibat dalam pengelolaannya [2].

Di Indonesia, digitalisasi pelayanan publik dan sektor swasta meningkat secara pesat dalam satu dekade terakhir. Layanan berbasis elektronik seperti perbankan digital, *e-commerce*, aplikasi transportasi, layanan kesehatan daring, serta sistem administrasi pemerintahan elektronik menjadi bagian tak terpisahkan dari kehidupan masyarakat [3].

Di balik berbagai kemudahan yang ditawarkan, meningkat pula risiko terjadinya pelanggaran keamanan data

[1] Astrid Faidlatul Habibah dan Irwansyah Irwansyah, "Era Masyarakat Informasi sebagai Dampak Media Baru," *Jurnal Teknologi Dan Sistem Informasi Bisnis* 3, no. 2 (2021): 350–63, https://doi.org/10.47233/jteksis.v3i2.255.

[2] Myrna Fitria dkk., "Perlindungan Dan Tanggung Jawab Hukum Kebocoran Informasi Data Pribadi Pada Penyelenggara Sistem Elektronik Berdasarkan Perspektif Rahasia Dagang," *Cerdika: Jurnal Ilmiah Indonesia* 5, no. 1 (2025): 1416–23, https://doi.org/10.59141/cerdika.v5i1.2408.

[3] Diana Diana dkk., "Public Service Innovation in the Era of Society 5.0: Data Protection, Governance, and Regulation in Indonesia," *DISCOURSE: Indonesian Journal of Social Studies and Education* 3, no. 1 (2025): 61–72, https://doi.org/10.69875/djosse.v3i1.315.

atau kebocoran data pribadi (*data Beach*). Kebocoran data pribadi merupakan peristiwa ketika data individu yang seharusnya bersifat rahasia diakses, diperoleh, diungkapkan, diubah, atau disalahgunakan oleh pihak yang tidak berwenang [4]. Peristiwa ini tidak hanya berdampak pada kerugian ekonomi, tetapi juga berpotensi menimbulkan kerugian immateriil seperti terganggunya rasa aman, reputasi, dan hak privasi individu sebagai subjek data.

Fenomena kebocoran data pribadi di Indonesia dalam beberapa tahun terakhir menunjukkan tren yang mengkhawatirkan. Insiden kebocoran data menimpa berbagai sektor strategis seperti keuangan, telekomunikasi, kesehatan, pendidikan, dan administrasi kependudukan [5]. Berbagai dugaan kebocoran data dalam skala besar mengemuka di ruang publik dan ramai diberitakan, mulai dari kasus kebocoran data pelanggan operator seluler, data nasabah perbankan, data peserta BPJS, hingga data penduduk dari sistem administrasi kependudukan. Banyak dari insiden tersebut diduga berasal dari lemahnya sistem keamanan elektronik, kelalaian pengelola sistem elektronik, atau penyalahgunaan akses oleh pihak internal maupun eksternal [6]. Kondisi ini menimbulkan pertanyaan mendasar mengenai sejauh mana penyelenggara sistem elektronik dapat dimintai pertanggungjawaban atas kebocoran data pribadi yang terjadi.

Data pribadi pada dasarnya merupakan perpanjangan dari identitas manusia yang melekat pada diri setiap individu. Dalam perspektif hak asasi manusia, data pribadi terkait erat dengan hak atas privasi, martabat manusia, dan perlindungan diri dari intervensi yang tidak sah. Oleh karena itu, perlindungan data pribadi memiliki kedudukan konstitusional, karena secara substansial berkaitan dengan pemenuhan hak warga negara sebagaimana diatur dalam konstitusi dan instrumen hak asasi manusia lainnya. Kebocoran data pribadi berarti terganggunya hak atas privasi, sehingga negara memiliki kewajiban untuk menjamin perlindungan hukum

[4] Irena Puspa Mega dan Albertus Sentot Sudarwanto, "PELANGGARAN HAK KONSUMEN ATAS KEBOCORAN DATA PRIBADI OLEH PT. TELKOMSEL," *Jurnal Privat Law* 13, no. 2 (2025): 224, https://doi.org/10.20961/privat.v13i2.53149.

[5] Muhamad Naufal Aulia Azmi dkk., "Analisa Kasus Kebocoran Data pada Bank Indonesia Dalam Sistem Perbankan: Indonesia," *JURNAL MULTIDISIPLIN ILMU AKADEMIK* 1, no. 6 (2024): 448–58, https://doi.org/10.61722/jmia.v1i6.3267.

[6] Annisa Ayu Handayani dkk., "Strategi Mengatasi Data Breaches di Era Industri 4.0: Kasus Data Breaches Bank Rakyat Indonesia," *JURNAL MANAJEMEN DAN BISNIS EKONOMI* 3, no. 2 (2025): 161–75, https://doi.org/10.54066/jmbe-itb.v3i2.3170.

yang memadai. Jaminan tersebut diwujudkan melalui regulasi, kelembagaan pengawas, serta mekanisme pertanggungjawaban bagi pihak yang melanggar [7].

Pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan tonggak penting dalam sistem hukum Indonesia. Undang-undang ini menghadirkan kerangka hukum komprehensif yang mengatur hak subjek data, kewajiban pengendali dan pemroses data, serta sanksi atas pelanggaran perlindungan data pribadi. UU PDP memberikan definisi yang tegas mengenai data pribadi, membedakan antara data pribadi umum dan data pribadi spesifik, serta mengatur prinsip-prinsip pemrosesan data seperti keabsahan tujuan, pembatasan tujuan, keakuratan, akuntabilitas, dan kerahasiaan. Dengan demikian, UU PDP memperkuat rezim perlindungan data pribadi yang sebelumnya hanya tersebar dalam berbagai aturan sektoral.

Salah satu isu krusial dalam UU PDP adalah mengenai pertanggungjawaban pidana atas kebocoran data pribadi yang dilakukan atau diakibatkan oleh penyelenggara sistem elektronik. Penyelenggara sistem elektronik merupakan pihak yang menyediakan, mengelola, dan mengoperasikan sistem elektronik untuk memproses data pribadi[8].

Dalam praktiknya, pengendali data, pemroses data, dan penyelenggara sistem elektronik sering kali memiliki peran yang tumpang tindih. Oleh karena itu, penting untuk memperjelas bagaimana bentuk pertanggungjawaban pidana dapat dikenakan kepada penyelenggara sistem elektronik dalam hal terjadi pelanggaran perlindungan data pribadi.

Pertanggungjawaban pidana dalam hukum pidana Indonesia pada umumnya berkaitan dengan adanya unsur perbuatan melawan hukum, kesalahan (*schuld*), kemampuan bertanggung jawab pelaku, serta hubungan antara perbuatan dan akibat yang ditimbulkan [9]. Dalam konteks kebocoran data pribadi, timbul persoalan apakah kebocoran tersebut hasil dari kesengajaan, kelalaian, atau kegagalan sistem yang seharusnya dapat diduga dan dicegah. Pertanyaan hukum

[7] Fitria dkk., "Perlindungan Dan Tanggung Jawab Hukum Kebocoran Informasi Data Pribadi Pada Penyelenggara Sistem Elektronik Berdasarkan Perspektif Rahasia Dagang."

[8] Fitria dkk., "Perlindungan Dan Tanggung Jawab Hukum Kebocoran Informasi Data Pribadi Pada Penyelenggara Sistem Elektronik Berdasarkan Perspektif Rahasia Dagang."

[9] Shulhan Iqbal Nasution, *MENS REA: FONDASI PERTANGGUNGJAWABAN PIDANA DALAM SISTEM PERADILAN PIDANA DI INDONESIA*, 7 (2025).

lain yang muncul adalah mengenai pembuktian unsur kesalahan pada korporasi atau badan hukum sebagai penyelenggara sistem elektronik. Hal ini menjadi semakin kompleks karena penyelenggara sistem elektronik dapat berbentuk badan hukum privat maupun instansi pemerintah.

UU PDP memperkenalkan pengaturan sanksi pidana yang cukup tegas terhadap pelanggaran tertentu, seperti pengumpulan dan penggunaan data pribadi secara melawan hukum, pengungkapan data tanpa persetujuan, atau pemalsuan data pribadi. Namun, dalam kasus kebocoran data akibat lemahnya sistem pengamanan atau kelalaian pengendali data, interpretasi bagaimana pertanggungjawaban pidana diterapkan masih memerlukan kajian mendalam. Pemidanaan terhadap korporasi, pembuktian pertanggung-jawaban pidana pengurus, serta batasan antara tanggung jawab perdata, administratif, dan pidana menjadi isu yang perlu dianalisis.

Selain itu, dalam praktiknya, kebocoran data pribadi sering kali melibatkan berbagai aktor. Data dapat bocor akibat serangan siber oleh pihak ketiga, kesalahan teknis, atau pengelolaan yang tidak sesuai standar perlindungan [10]. Dalam situasi demikian, penentuan pihak yang paling bertanggung jawab secara pidana menjadi persoalan yang tidak sederhana. Apakah pelaku utama adalah peretas yang secara aktif menyerang sistem, penyelenggara sistem elektronik yang lalai membangun keamanan, atau pihak internal yang menyalahgunakan akses? Pertanyaan ini berimplikasi langsung pada konstruksi pertanggungjawaban pidana.

Lebih lanjut, perkembangan kejahatan siber (*cybercrime*) menambah kompleksitas penegakan hukum terkait kebocoran data pribadi. Modus operandi kejahatan data semakin canggih, lintas batas negara, dan sering kali melibatkan jaringan terorganisasi. Penegakan hukum terkendala oleh masalah yurisdiksi, pembuktian digital, serta keterbatasan kapasitas aparat penegak hukum dalam melakukan forensik digital [11]. Namun demikian, keberadaan UU PDP memberikan dasar hukum yang lebih kuat untuk menindak pelanggaran, meskipun penerapannya masih menghadapi tantangan implementasi.

[10] Mega dan Sudarwanto, "PELANGGARAN HAK KONSUMEN ATAS KEBOCORAN DATA PRIBADI OLEH PT. TELKOMSEL."

[11] Satya Agung Hardiansyah dan Tata Sutabri, *Analisis Pelanggaran Etika Teknologi Informasi Di Indonesia: Studi Kasus Kebocoran Data*, 2026.

Di sisi lain, penyelenggara sistem elektronik memiliki tanggung jawab untuk memastikan keamanan data pribadi melalui penerapan standar teknis tertentu, manajemen risiko, dan tata kelola perlindungan data. UU PDP juga mewajibkan penerapan prinsip keamanan dan kerahasiaan data serta mitigasi apabila terjadi insiden kebocoran [12].

Kewajiban memberikan notifikasi kebocoran data kepada subjek data dan otoritas pengawas merupakan instrumen akuntabilitas yang penting. Namun, apabila kewajiban tersebut diabaikan atau data bocor akibat kelalaian berat, maka pertanggungjawaban pidana bisa menjadi konsekuensi yang wajar.

Dengan demikian, penelitian mengenai pertanggungjawaban pidana atas kebocoran data pribadi oleh penyelenggara sistem elektronik menjadi sangat relevan dan urgen. Pentingnya penelitian ini tidak hanya untuk memperkuat perlindungan hak atas privasi warga negara, tetapi juga untuk memberikan kepastian hukum bagi penyelenggara sistem elektronik dalam menjalankan kewajibannya. Selain itu, penelitian ini diharapkan mampu menjelaskan batasan-batasan pertanggungjawaban pidana, sehingga tidak semua insiden kebocoran data otomatis dikualifikasikan sebagai tindak pidana, tetapi dibedakan menurut unsur kesalahan dan tingkat pelanggaran yang terjadi.

Di ranah akademik, topik ini juga menarik karena menggabungkan beberapa bidang kajian, yaitu hukum pidana, hukum siber, dan hukum perlindungan data pribadi. Pendekatan interdisipliner diperlukan untuk memahami fenomena kebocoran data yang bukan hanya persoalan teknis, tetapi juga memiliki dimensi sosial, ekonomi, dan etika. Penelitian ini sekaligus menjawab kebutuhan pengembangan doktrin hukum terkait pertanggungjawaban pidana korporasi dalam ranah kejahatan siber. Penelitian ini akan memfokuskan analisis pada bagaimana konstruksi pertanggung-jawaban pidana diterapkan, unsur-unsur tindak pidana yang relevan, serta implikasi yuridisnya bagi perlindungan data pribadi di Indonesia.

Berdasarkan latar belakang di atas, maka untuk memperjelas fokus kajian penelitian ini perlu dirumuskan permasalahan yang akan diteliti, yaitu sebagai berikut: Bagaimana pengaturan

[12] Julienna Hartono dkk., *Failing to Protect Personal Data: Key Aspects of Electronic System Operators' Agreements*, 2023.

pertanggungjawaban pidana atas kebocoran data pribadi oleh penyelenggara sistem elektronik dalam perspektif Undang-Undang Perlindungan Data Pribadi? Bagaimana bentuk penerapan pertanggungjawaban pidana terhadap penyelenggara sistem elektronik yang menyebabkan terjadinya kebocoran data pribadi, serta faktor-faktor apa saja yang menjadi kendala dalam penegakannya?

A. Metode

Metode penelitian yang digunakan dalam penelitian ini adalah penelitian hukum normatif atau yuridis normatif, yaitu penelitian yang berfokus pada kajian norma hukum dalam peraturan perundang-undangan, asas hukum, doktrin, dan putusan pengadilan yang relevan. Penelitian ini bertujuan menganalisis konstruksi pertanggungjawaban pidana dalam sistem hukum Indonesia terhadap kebocoran data pribadi oleh penyelenggara sistem elektronik, termasuk subjek hukum yang dapat dimintai pertanggungjawaban serta unsur-unsur tindak pidana yang diatur dalam peraturan terkait perlindungan data pribadi dan sistem elektronik.

Penelitian ini menggunakan data kepustakaan sebagai sumber utama yang terdiri atas bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Perlindungan Data Pribadi, Undang-Undang Informasi dan Transaksi Elektronik beserta perubahannya, serta peraturan dan putusan pengadilan yang relevan. Bahan hukum sekunder berupa buku, jurnal ilmiah, hasil penelitian, dan pendapat ahli yang berkaitan dengan perlindungan data pribadi, hukum pidana, dan pertanggungjawaban penyelenggara sistem elektronik. Adapun bahan hukum tersier berupa kamus dan ensiklopedia hukum digunakan untuk mendukung pemahaman istilah dan konsep hukum.
Pengumpulan bahan hukum dilakukan melalui studi kepustakaan dengan menelaah berbagai peraturan perundang-undangan, literatur ilmiah, doktrin, artikel jurnal, dan putusan pengadilan yang relevan dengan topik penelitian.

Selanjutnya, bahan hukum dianalisis secara kualitatif dengan pendekatan yuridis normatif melalui penafsiran sistematis dan konseptual terhadap norma hukum yang berlaku serta dikaitkan dengan asas hukum dan pendapat para ahli. Analisis ini bertujuan untuk memahami ruang lingkup dan implikasi pertanggungjawaban pidana atas kebocoran data pribadi, sekaligus mengidentifikasi kemungkinan adanya

kekosongan norma, ketidaksesuaian, atau tumpang tindih pengaturan hukum. Hasil analisis kemudian disusun secara deskriptif-analitis guna menjawab rumusan masalah penelitian dan menarik kesimpulan secara logis serta argumentatif.

B. Pembahasan dan Diskusi

1. Pengaturan Pertanggungjawaban Pidana atas Kebocoran Data Pribadi oleh Penyelenggara Sistem Elektronik

Perkembangan teknologi informasi dan komunikasi dalam beberapa dekade terakhir telah mendorong terjadinya transformasi digital yang signifikan dalam berbagai aspek kehidupan masyarakat. Perubahan tersebut tidak hanya berdampak pada sektor ekonomi, tetapi juga meluas ke bidang pemerintahan, pendidikan, kesehatan, serta pola interaksi sosial masyarakat. Digitalisasi yang masif ini ditandai dengan meningkatnya aktivitas pengumpulan, pengolahan, penyimpanan, dan distribusi data pribadi melalui sistem elektronik [13]. Dalam konteks ini, data pribadi tidak lagi sekadar informasi individual, melainkan telah berkembang menjadi aset yang memiliki nilai ekonomi tinggi sekaligus mengandung potensi risiko yang besar apabila tidak dikelola secara tepat [14].

Dalam praktiknya, penyelenggara sistem elektronik, baik yang berada di sektor publik maupun privat, secara intensif mengelola data pribadi dalam skala besar [15]. Aktivitas tersebut mencakup layanan keuangan berbasis teknologi (*financial technology*), perdagangan elektronik (*e-commerce*), media sosial, hingga layanan administrasi publik berbasis digital. Kondisi ini memberikan berbagai kemudahan, seperti efisiensi pelayanan, peningkatan aksesibilitas, serta percepatan proses transaksi. Namun demikian, peningkatan volume dan kompleksitas pengelolaan data pribadi juga membuka peluang terjadinya pelanggaran, khususnya kebocoran data pribadi yang berpotensi merugikan subjek data baik secara material maupun immaterial [16].

---

[13] Johan Alfred Sarades Silalahi dkk., "Analisis Yuridis terhadap Mekanisme Perlindungan Data Pribadi dalam Sistem Informasi Elektronik Berdasarkan Perspektif Hukum Pidana di Indonesia," *Jurnal Minfo Polgan* 14, no. 1 (2025): 604–13, https://doi.org/10.33395/jmp.v14i1.14810.

[14] Fitria dkk., "Perlindungan Dan Tanggung Jawab Hukum Kebocoran Informasi Data Pribadi Pada Penyelenggara Sistem Elektronik Berdasarkan Perspektif Rahasia Dagang."

[15] Rista Maharani dan Andria Luhur Prakoso, "Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital," *JURNAL USM LAW REVIEW* 7, no. 1 (2024): 333–47, https://doi.org/10.26623/julr.v7i1.8705.

[16] Giuseppe D'Acquisto dkk., *Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics*, versi 1, 2015, https://doi.org/10.48550/ARXIV.1512.06000.

Kebocoran data pribadi tidak hanya berdampak pada kerugian ekonomi, tetapi juga dapat menimbulkan dampak psikologis dan sosial yang serius [17]. Penyalahgunaan data pribadi dapat mengarah pada berbagai bentuk kejahatan, seperti pencurian identitas, penipuan berbasis digital, peretasan akun, hingga pelanggaran privasi yang bersifat invasif. Oleh karena itu, perlindungan data pribadi tidak lagi dapat dipandang sebagai isu teknis semata, melainkan telah menjadi bagian integral dari sistem perlindungan hukum modern yang berkaitan erat dengan perlindungan hak asasi manusia [18].

Secara konseptual, perlindungan data pribadi berakar pada hak atas privasi yang telah diakui secara universal. Hak ini menegaskan bahwa setiap individu memiliki kontrol atas informasi mengenai dirinya, termasuk dalam hal bagaimana data tersebut dikumpulkan, digunakan, dan disebarluaskan. Dalam perspektif internasional, pengakuan terhadap hak privasi tercermin dalam Pasal 12 *Universal Declaration of Human Rights* (UDHR) yang menyatakan bahwa tidak seorang pun boleh mengalami gangguan sewenang-wenang terhadap kehidupan pribadinya, keluarga, tempat tinggal, maupun korespondensinya. Selain itu, konsep perlindungan privasi juga telah dikemukakan secara klasik oleh Warren dan Brandeis (1890) melalui gagasan *the right to be let alone*, yang menjadi landasan konseptual bagi perkembangan rezim perlindungan data pribadi di era modern [19].

Dalam konteks hukum nasional, Indonesia telah mengadopsi kerangka hukum yang lebih komprehensif melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Undang-undang ini merupakan tonggak penting dalam penguatan regulasi terkait pengelolaan data pribadi, yang mencakup seluruh tahapan pemrosesan data, mulai dari pengumpulan hingga penghapusan data.

Pasal 1 angka 1 UU PDP mendefinisikan data pribadi sebagai setiap data tentang seseorang yang teridentifikasi atau dapat diidentifikasi, baik secara langsung maupun tidak langsung, melalui sistem elektronik

[17] Cassandra Cross dan Thomas J. Holt, "Beyond Fraud and Identity Theft: Assessing the Impact of Data Breaches on Individual Victims," *Journal of Crime and Justice*, 17 Juli 2025, 1–24, https://doi.org/10.1080/0735648X.2025.2535007.

[18] Siti Rahmadani dan Rina Arum Prastyanti, "Human Rights and Cybersecurity: Reinforcing Legal Protections for Personal Data," *International Journal of Law Dynamics Review* 3, no. 1 (2025): 20–29, https://doi.org/10.62039/ijldr.v3i1.80.

[19] Volini, Anthony G, "The Right to Data Privacy: Revisiting Warren & Brandeis," *Journal of Technology and Intellectual Property* 21, no. 1 (2023).

maupun non-elektronik. Definisi ini menunjukkan bahwa cakupan perlindungan bersifat luas dan adaptif terhadap perkembangan teknologi informasi.

Lebih lanjut, UU PDP menegaskan bahwa penyelenggara sistem elektronik, khususnya dalam kapasitasnya sebagai pengendali data pribadi, memiliki kewajiban hukum untuk melindungi data pribadi yang dikelola. Pasal 35 UU PDP menyatakan bahwa pengendali data pribadi wajib melindungi dan memastikan keamanan data pribadi dari pemrosesan yang tidak sah. Ketentuan ini mencerminkan penerapan prinsip akuntabilitas (*accountability principle*), yang mengharuskan setiap pengendali data bertanggung jawab secara penuh terhadap seluruh proses pengelolaan data yang dilakukan [20].

Selain kewajiban normatif tersebut, UU PDP juga mengatur kewajiban teknis yang harus dipenuhi oleh penyelenggara sistem elektronik. Pasal 39 UU PDP mengatur bahwa pengendali data wajib melakukan langkah-langkah teknis dan operasional untuk melindungi data pribadi dari gangguan keamanan. Langkah-langkah ini meliputi penerapan sistem keamanan informasi, penggunaan teknologi enkripsi, pengendalian akses, serta pengelolaan risiko keamanan data [21]. Dengan demikian, perlindungan data pribadi tidak hanya bergantung pada norma hukum, tetapi juga pada implementasi teknologi yang memadai untuk menjamin keamanan data.

Dalam hal terjadinya kebocoran data pribadi, tanggung jawab hukum penyelenggara sistem elektronik menjadi aspek yang sangat krusial. Kebocoran data yang disebabkan oleh kelalaian dalam menjaga keamanan sistem dapat menjadi dasar untuk menuntut pertanggungjawaban hukum [22]. Dalam konteks ini, penting untuk membedakan antara kebocoran yang terjadi akibat faktor eksternal yang tidak dapat dihindari (*force majeure*) dengan kebocoran yang disebabkan oleh kegagalan internal dalam sistem pengamanan. Perbedaan ini memiliki implikasi langsung terhadap penentuan unsur kesalahan sebagai dasar pertanggungjawaban pidana.

---

[20] Ahmad Ardaful Abror Jauhari, "Perlindungan Hukum Terhadap Data Pribadi Pengguna Platform Digital Dalam Persfektif Kepastian Hukum," *Journal Equitable* 11, no. 1 (2026).

[21] Loso Judijanto dkk., "Analisis Keamanan Data dan Perlindungan Privasi dalam Pengelolaan Big Data: Tinjauan Teknologi Enkripsi dan Anonimisasi," *Jurnal Penelitian Inovatif* 5, no. 2 (2025): 1991–2000, https://doi.org/10.54082/jupin.1151.

[22] Annisa Fitria dan Diah Putri Hasian, "Pertanggung Jawaban Telkomsel Atas Kebocoran Rahasia Data Pribadi Pengguna Indihome," *Arus Jurnal Sosial dan Humaniora* 5, no. 2 (2025): 1812–21, https://doi.org/10.57250/ajsh.v5i2.1440.

Dari perspektif hukum pidana, UU PDP mengatur berbagai perbuatan yang dapat dikualifikasikan sebagai tindak pidana. Pasal 67 UU PDP mengatur bahwa setiap orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain dapat dikenakan sanksi pidana. Selain itu, Pasal 68 UU PDP mengatur bahwa setiap orang yang secara melawan hukum mengungkapkan data pribadi yang bukan miliknya juga dapat dipidana. Ketentuan ini menunjukkan bahwa pelanggaran terhadap perlindungan data pribadi diposisikan sebagai delik pidana yang serius.

Namun demikian, penerapan pertanggungjawaban pidana dalam kasus kebocoran data pribadi tidak selalu sederhana. Salah satu tantangan utama adalah pembuktian unsur kesalahan (*mens rea*), terutama dalam kasus yang melibatkan sistem elektronik yang kompleks. Dalam hukum pidana dikenal prinsip *geen straf zonder schuld*, yang menegaskan bahwa tidak ada pidana tanpa kesalahan [23]. Oleh karena itu, perlu dibuktikan adanya unsur kesengajaan (*dolus*) atau kelalaian (*culpa*) dalam terjadinya kebocoran data tersebut.

Selain pertanggungjawaban individu, hukum pidana modern juga mengakui adanya pertanggungjawaban pidana korporasi. Hal ini relevan mengingat sebagian besar penyelenggara sistem elektronik berbentuk badan hukum. Menurut Sjahdeini korporasi dapat dimintai pertanggungjawaban pidana apabila tindak pidana dilakukan dalam lingkup kegiatan usaha atau untuk kepentingan korporasi tersebut [24]. Konsep ini sejalan dengan doktrin *corporate criminal liability*, yang menyatakan bahwa tindakan pengurus atau pihak yang mewakili korporasi dapat diatribusikan sebagai tindakan korporasi itu sendiri [25].

Dalam konteks kebocoran data pribadi, pertanggungjawaban pidana korporasi dapat timbul apabila kebocoran tersebut disebabkan oleh kebijakan perusahaan yang lalai, lemahnya sistem pengendalian internal, atau kegagalan dalam menerapkan standar keamanan

[23] Rr. Dijan Widijowati, "A Comparative Study Of Principle Of Guilt In The Provision Of Indonesian And English Criminal Law," *KRTHA BHAYANGKARA* 18, no. 3 (2024): 559–68, https://doi.org/10.31599/krtha.v18i3.3302.

[24] Sutan Remy Sjahdeini, *Ajaran Pemidanaan: Tindak Pidana Korporasi Dan Seluk-Beluknya* (Kencana, 2017).

[25] Shinde Hema Pramod dan Narendra Kumar Singh, "A Study on Corporate Criminal Liability: Comparative Approach," *Journal of Advances and Scholarly Researches in Allied Education* 20, no. 4 (2023): 797–804, https://doi.org/10.29070/qpzqqg91.

yang memadai. Dengan demikian, korporasi tidak dapat menghindari tanggung jawab hanya dengan mengalihkan kesalahan kepada individu tertentu.

Pengaturan mengenai kewajiban penyelenggara sistem elektronik juga diperkuat melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016. Pasal 15 UU ITE menegaskan bahwa setiap penyelenggara sistem elektronik wajib menyelenggarakan sistem yang andal, aman, dan bertanggung jawab. Ketentuan ini memperkuat dasar hukum bagi penegakan tanggung jawab terhadap penyelenggara sistem elektronik dalam hal terjadi kegagalan sistem yang mengakibatkan kebocoran data.

Meskipun kerangka hukum yang ada telah relatif komprehensif, implementasinya masih menghadapi berbagai tantangan. Keterbatasan kapasitas aparat penegak hukum dalam memahami aspek teknis teknologi informasi, belum adanya standar keamanan yang seragam, serta rendahnya tingkat kepatuhan penyelenggara sistem elektronik menjadi kendala dalam penegakan hukum [26] . Selain itu, koordinasi antar lembaga juga menjadi faktor penting dalam memastikan efektivitas perlindungan data pribadi.

Oleh karena itu, diperlukan upaya yang berkelanjutan untuk memperkuat sistem perlindungan data pribadi di Indonesia. Upaya tersebut meliputi peningkatan kapasitas sumber daya manusia, pengembangan regulasi teknis yang lebih rinci, serta penguatan mekanisme pengawasan dan penegakan hukum. Di samping itu, penting untuk mendorong kesadaran hukum dan budaya kepatuhan di kalangan penyelenggara sistem elektronik agar perlindungan data pribadi tidak hanya dipandang sebagai kewajiban hukum, tetapi juga sebagai tanggung jawab etis.

Dengan demikian, pengaturan pertanggungjawaban pidana atas kebocoran data pribadi oleh penyelenggara sistem elektronik dalam sistem hukum Indonesia telah memiliki dasar normatif yang kuat. Namun, efektivitasnya sangat bergantung pada implementasi yang konsisten, penegakan hukum yang tegas, serta kesadaran semua pihak dalam menjaga keamanan dan kerahasiaan data pribadi. Dalam konteks ini, hukum pidana berfungsi sebagai

[26] Muhamad Adri Rinjani dan Ricky Firmansyah, "Hambatan Implementasi UU 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia," *Jurnal Analisis Hukum* 8, no. 1 (2025): 70–83, https://doi.org/10.38043/jah.v8i1.6793.

instrumen penting untuk menjamin perlindungan data pribadi sekaligus menjaga kepercayaan masyarakat terhadap sistem elektronik di era digital.

2. Pertanggungjawaban Pidana Penyelenggara Sistem Elektronik atas Kebocoran Data Pribadi dan Kendala Penegakannya

Penerapan pertanggungjawaban pidana terhadap penyelenggara sistem elektronik (PSE) yang menyebabkan terjadinya kebocoran data pribadi merupakan isu yang semakin krusial dalam perkembangan hukum di era digital. Fenomena ini tidak dapat dilepaskan dari meningkatnya intensitas pemanfaatan teknologi informasi dalam berbagai sektor kehidupan, baik sektor publik maupun privat, yang secara langsung berdampak pada meningkatnya volume dan kompleksitas pengelolaan data pribadi. Dalam beberapa tahun terakhir, berbagai kasus kebocoran data yang melibatkan institusi pemerintah maupun korporasi swasta menunjukkan bahwa risiko pelanggaran data pribadi tidak lagi bersifat hipotetis, melainkan telah menjadi realitas yang nyata dan memerlukan respons hukum yang tidak hanya tegas, tetapi juga efektif serta adaptif terhadap perkembangan teknologi [27].

Dalam konteks tersebut, hukum pidana diharapkan mampu menjalankan dua fungsi sekaligus, yaitu fungsi represif dan preventif. Fungsi represif diwujudkan melalui penjatuhan sanksi terhadap pelaku pelanggaran, sedangkan fungsi preventif bertujuan untuk mencegah terjadinya pelanggaran melalui efek jera serta peningkatan kepatuhan hukum. Dengan demikian, keberadaan hukum pidana dalam perlindungan data pribadi tidak hanya berorientasi pada penghukuman semata, tetapi juga diarahkan pada pembentukan kesadaran hukum dan perilaku yang lebih bertanggung jawab dalam pengelolaan data pribadi oleh para penyelenggara sistem elektronik .

Secara normatif, penerapan pertanggungjawaban pidana terhadap PSE di Indonesia dapat dianalisis melalui kerangka Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi serta Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016. UU PDP secara khusus mengatur berbagai bentuk perbuatan

[27] Tanti Kirana Utami dkk., "Personal Data Breach Cases In Indonesia : Perspective Of Personal Data Protection Law," *Journal Customary Law* 2, no. 2 (2025): 21, https://doi.org/10.47134/jcl.v2i2.3742.

yang dapat dikualifikasikan sebagai tindak pidana, antara lain perolehan, pengungkapan, dan penggunaan data pribadi secara melawan hukum. Namun demikian, dalam praktiknya, tidak semua peristiwa kebocoran data pribadi dapat secara otomatis dikategorikan sebagai tindak pidana. Hal ini disebabkan oleh adanya prinsip dasar dalam hukum pidana yang mensyaratkan adanya unsur kesalahan (*mens rea*), baik dalam bentuk kesengajaan (*dolus*) maupun kelalaian (*culpa*) sebagai dasar untuk menjatuhkan pidana [28].

Dalam praktiknya, penerapan pertanggungjawaban pidana terhadap PSE dapat diklasifikasikan ke dalam dua bentuk utama, yaitu pertanggungjawaban pidana individu dan pertanggungjawaban pidana korporasi. Pertanggungjawaban pidana individu umumnya dikenakan kepada pihak-pihak yang secara langsung melakukan perbuatan melawan hukum, seperti individu yang secara ilegal memperoleh, mengakses, atau menyebarluaskan data pribadi tanpa hak. Dalam hal ini, ketentuan Pasal 67 dan Pasal 68 UU PDP menjadi dasar hukum utama dalam menjerat pelaku yang secara sengaja melakukan pelanggaran terhadap data pribadi.

Namun demikian, dalam banyak kasus kebocoran data, pelanggaran tidak selalu disebabkan oleh tindakan aktif individu yang bersifat langsung. Tidak jarang kebocoran data justru terjadi akibat kelemahan sistem keamanan, kesalahan konfigurasi sistem, atau bahkan kelalaian dalam pengelolaan data yang dilakukan secara sistemik. Dalam kondisi seperti ini, pertanggungjawaban pidana dapat diarahkan kepada PSE sebagai entitas korporasi. Konsep ini dikenal sebagai pertanggungjawaban pidana korporasi, yang dalam perkembangan hukum pidana modern telah diakui sebagai bagian dari perluasan subjek hukum pidana [29].

Pertanggungjawaban pidana korporasi didasarkan pada asumsi bahwa korporasi sebagai subjek hukum memiliki kemampuan untuk bertindak melalui organ-organ yang mewakilinya, seperti direksi, komisaris, maupun karyawan. Oleh karena itu, tindakan yang dilakukan oleh individu dalam lingkup pekerjaannya dapat diatribusikan sebagai tindakan korporasi. Dengan demikian, apabila kebocoran data terjadi akibat

[28] Sjahdeini, *Ajaran Pemidanaan: Tindak Pidana Korporasi Dan Seluk-Beluknya*.
[29] Muhammad Wahyu Alfakar dkk., "Evalution of Corporate Criminal Liability Model and Theories under Indonesia New Criminal Code," *Indonesian Journal of Criminal Law Studies* 8, no. 2 (2023).

kebijakan perusahaan yang tidak memadai, lemahnya sistem pengendalian internal, atau kegagalan dalam menerapkan standar keamanan yang layak, maka korporasi dapat dimintai pertanggungjawaban pidana [30].

Dalam konteks teoritis, terdapat beberapa pendekatan yang dapat digunakan untuk menentukan pertanggungjawaban pidana korporasi. Pertama, *identification theory*, yang menempatkan tindakan pejabat tinggi sebagai representasi langsung dari tindakan korporasi. Kedua, *vicarious liability*, yang memungkinkan korporasi bertanggung jawab atas perbuatan karyawan selama perbuatan tersebut dilakukan dalam lingkup pekerjaan. Ketiga, *strict liability*, yang memungkinkan penjatuhan sanksi tanpa harus membuktikan unsur kesalahan secara subjektif, sepanjang telah terjadi pelanggaran terhadap kewajiban hukum tertentu [31]. Ketiga pendekatan ini pada dasarnya memberikan dasar teoritis yang cukup kuat untuk menjerat korporasi dalam kasus kebocoran data pribadi.

Meskipun demikian, dalam praktik penegakan hukum di Indonesia, penerapan pertanggungjawaban pidana terhadap PSE masih menghadapi berbagai kendala yang tidak sederhana. Salah satu kendala utama adalah kesulitan dalam membuktikan hubungan kausal (*causal link*) antara tindakan atau kelalaian PSE dengan terjadinya kebocoran data pribadi. Hal ini menjadi kompleks karena sistem elektronik yang digunakan biasanya melibatkan berbagai komponen teknologi, termasuk pihak ketiga seperti vendor atau penyedia layanan cloud, sehingga sulit untuk menentukan secara pasti sumber kebocoran dan pihak yang paling bertanggung jawab.

Selain itu, kendala lain yang cukup signifikan adalah keterbatasan kapasitas aparat penegak hukum dalam memahami aspek teknis teknologi informasi. Penanganan kasus kebocoran data tidak hanya membutuhkan pemahaman hukum, tetapi juga memerlukan keahlian khusus di bidang keamanan siber, forensik digital, dan analisis sistem informasi. Tanpa dukungan keahlian tersebut, proses pembuktian dalam perkara pidana menjadi kurang optimal dan berpotensi menghambat penegakan hukum secara efektif [32].

---

[30] Sjahdeini, *Ajaran Pemidanaan: Tindak Pidana Korporasi Dan Seluk-Beluknya*.
[31] Pramod dan Singh, "A Study on Corporate Criminal Liability."
[32] Meenakshi Tyagi dkk., "Digital Evidence and Local Law Enforcement: Challenges in Cybercrime Prosecution," *Advances in Consumer Research* 2, no. 5 (2025).

Kendala berikutnya berkaitan dengan belum adanya standar teknis yang seragam dalam pengamanan data pribadi. Meskipun UU PDP telah mengatur kewajiban penerapan langkah-langkah teknis dan operasional, implementasinya di lapangan masih sangat bergantung pada kebijakan masing-masing PSE. Hal ini menyebabkan adanya variasi dalam tingkat keamanan sistem yang diterapkan, sehingga menyulitkan dalam menentukan apakah suatu tindakan dapat dikategorikan sebagai kelalaian atau tidak.

Di samping itu, persoalan yurisdiksi juga menjadi tantangan yang cukup serius, terutama dalam kasus yang melibatkan PSE lintas negara. Dalam era digital yang bersifat global, data pribadi sering kali disimpan atau diproses di server yang berada di luar wilayah hukum Indonesia. Kondisi ini menimbulkan kesulitan dalam menentukan kewenangan hukum serta memerlukan kerja sama internasional yang efektif dalam proses penegakan hukum [33].

Faktor lain yang tidak kalah penting adalah rendahnya tingkat kesadaran dan kepatuhan PSE terhadap pentingnya perlindungan data pribadi. Dalam praktiknya, masih banyak penyelenggara sistem elektronik yang memandang perlindungan data sebagai beban tambahan, bukan sebagai bagian dari tata kelola perusahaan yang baik. Akibatnya, investasi dalam sistem keamanan data sering kali tidak menjadi prioritas, sehingga meningkatkan potensi terjadinya kebocoran data.

Selain faktor-faktor tersebut, kendala juga muncul dari aspek regulasi. Meskipun UU PDP telah memberikan dasar hukum yang cukup komprehensif, namun masih diperlukan peraturan pelaksana yang lebih rinci untuk mengatur aspek teknis dan prosedural dalam penegakan hukum. Tanpa adanya regulasi turunan yang jelas, implementasi ketentuan pidana dalam UU PDP berpotensi menimbulkan perbedaan interpretasi di antara aparat penegak hukum.

Dalam menghadapi berbagai kendala tersebut, diperlukan pendekatan yang lebih komprehensif dalam penerapan pertanggungjawaban pidana terhadap PSE. Pendekatan ini tidak hanya mengandalkan penegakan hukum secara represif, tetapi juga perlu didukung oleh upaya preventif yang sistematis. Upaya preventif tersebut antara lain meliputi peningkatan standar keamanan data,

[33] Tazkiya An Nafisa dkk., "Analisis Pengaturan Pengalihan Data Pribadi Lintas Negara Pasca Akuisisi Dalam Undang-Undang Perlindungan Data Pribadi," *Jurnal Dialektika Hukum* 7, no. 1 (2025): 97–135, https://doi.org/10.36859/jdh.v7i1.3548.

penguatan regulasi teknis, serta edukasi kepada pelaku usaha dan masyarakat.

Selain itu, sinergi antara pemerintah, sektor swasta, dan masyarakat juga menjadi faktor penting dalam menciptakan sistem perlindungan data pribadi yang efektif. Pemerintah perlu memperkuat kapasitas lembaga pengawas dan aparat penegak hukum, sementara sektor swasta harus meningkatkan kepatuhan terhadap standar perlindungan data. Di sisi lain, masyarakat juga perlu diberikan edukasi agar lebih memahami hak-haknya sebagai subjek data.

Dengan demikian, dapat disimpulkan bahwa bentuk penerapan pertanggungjawaban pidana terhadap penyelenggara sistem elektronik dalam kasus kebocoran data pribadi mencakup dua aspek utama, yaitu pertanggungjawaban pidana individu dan pertanggungjawaban pidana korporasi.

Adapun dalam penegakannya, terdapat berbagai kendala yang meliputi aspek pembuktian, keterbatasan kapasitas aparat penegak hukum, kompleksitas teknologi, permasalahan yurisdiksi, serta belum optimalnya regulasi dan tingkat kepatuhan PSE. Oleh karena itu, efektivitas penerapan pertanggungjawaban pidana sangat bergantung pada penguatan aspek regulasi, teknis, dan kelembagaan secara berkelanjutan.

C. Penutup

1. Kesimpulan

Berdasarkan hasil penelitian, dapat disimpulkan bahwa pengaturan pertanggungjawaban pidana atas kebocoran data pribadi oleh penyelenggara sistem elektronik dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah memberikan dasar hukum yang cukup jelas dalam melindungi data pribadi masyarakat. Undang-undang tersebut mengatur hak subjek data, kewajiban penyelenggara sistem elektronik, serta sanksi pidana terhadap perbuatan yang menyebabkan kebocoran data pribadi, baik karena kesengajaan maupun kelalaian. Pertanggungjawaban pidana dalam kasus kebocoran data pribadi dapat dikenakan kepada individu maupun korporasi. Individu bertanggung jawab atas perbuatan melawan hukum yang dilakukan secara langsung, sedangkan korporasi dapat dimintai pertanggungjawaban apabila kebocoran data terjadi akibat lemahnya sistem keamanan, kebijakan internal yang tidak memadai, atau kelalaian dalam pengelolaan data pribadi. Namun, penerapan sanksi pidana tetap harus didasarkan pada pembuktian unsur-unsur

pidana sesuai ketentuan hukum yang berlaku. Dalam praktiknya, penegakan hukum masih menghadapi berbagai kendala, seperti kesulitan pembuktian, keterbatasan kemampuan aparat dalam bidang forensik digital, kompleksitas teknologi informasi, serta persoalan yurisdiksi lintas negara. Selain itu, rendahnya kesadaran dan kepatuhan penyelenggara sistem elektronik terhadap standar keamanan data juga mempengaruhi efektivitas perlindungan data pribadi.

Dengan demikian, efektivitas pertanggungjawaban pidana. terhadap kebocoran data pribadi tidak hanya bergantung pada keberadaan aturan hukum, tetapi juga pada penguatan implementasi, peningkatan kapasitas aparat penegak hukum, serta penerapan standar keamanan data yang lebih baik guna mewujudkan perlindungan data pribadi yang efektif di era digital. serta harmonisasi hukum nasional dengan rezim hukum lingkungan dan instrumen internasional. Dengan demikian, hukum pidana perikanan dapat berperan secara efektif sebagai instrumen pengendalian dan perlindungan sumber daya perikanan yang berkelanjutan.

2. Saran

Untuk meningkatkan efektivitas perlindungan data pribadi di Indonesia, pemerintah perlu menyusun regulasi teknis yang lebih rinci mengenai standar keamanan data pribadi yang wajib diterapkan oleh penyelenggara sistem elektronik. Regulasi tersebut penting agar terdapat pedoman yang jelas terkait tata kelola, penyimpanan, dan pengamanan data pribadi guna meminimalisir terjadinya kebocoran data. Selain itu, peningkatan kapasitas aparat penegak hukum juga perlu dilakukan, khususnya dalam bidang forensik digital dan penanganan kejahatan siber.

Hal ini penting untuk mendukung proses pembuktian dalam kasus kebocoran data pribadi yang semakin kompleks seiring perkembangan teknologi informasi. Di sisi lain, penyelenggara sistem elektronik perlu meningkatkan kepatuhan terhadap ketentuan perlindungan data pribadi dengan memperkuat sistem keamanan, melakukan audit keamanan secara berkala, serta menerapkan manajemen risiko yang baik dalam pengelolaan data pengguna. Upaya tersebut diperlukan untuk mencegah terjadinya kelalaian yang dapat menimbulkan kerugian bagi masyarakat. Selanjutnya, diperlukan

peningkatan kesadaran hukum masyarakat mengenai pentingnya perlindungan data pribadi melalui edukasi dan sosialisasi secara berkelanjutan. Dengan meningkatnya kesadaran masyarakat, diharapkan penggunaan layanan digital dapat dilakukan secara lebih aman dan bertanggung jawab. Terakhir, pemerintah perlu memperkuat kerja sama lintas negara dalam penanganan tindak pidana kebocoran data pribadi, terutama pada kasus yang melibatkan sistem elektronik internasional. Kerja sama tersebut penting untuk mendukung efektivitas penegakan hukum dan perlindungan data pribadi di era digital yang bersifat global

DAFTAR PUSTAKA

Alfakar, Muhammad Wahyu, Ali Masyhar, Cahya Wulandari, dan Ngboawaji Daniel Nte. "Evalution of Corporate Criminal Liability Model and Theories under Indonesia New Criminal Code." *Indonesian Journal of Criminal Law Studies* 8, no. 2 (2023).

An Nafisa, Tazkiya, Moch. Zairul Alam, dan Diah Pawestri Maharani. "Analisis Pengaturan Pengalihan Data Pribadi Lintas Negara Pasca Akuisisi Dalam Undang-Undang Perlindungan Data Pribadi." *Jurnal Dialektika Hukum* 7, no. 1 (2025): 97–135. https://doi.org/10.36859/jdh.v7i1.3548.

Annisa Ayu Handayani, Balqis Naura Izzati, Diana Nur'azzah, dan Khoirunnisa Khoirunnisa. "Strategi Mengatasi Data Breaches di Era Industri 4.0: Kasus Data Breaches Bank Rakyat Indonesia." *JURNAL MANAJEMEN DAN BISNIS EKONOMI* 3, no. 2 (2025): 161–75. https://doi.org/10.54066/jmbe-itb.v3i2.3170.

Cross, Cassandra, dan Thomas J. Holt. "Beyond Fraud and Identity Theft: Assessing the Impact of Data Breaches on Individual Victims." *Journal of Crime and Justice*, 17 Juli 2025, 1–24. https://doi.org/10.1080/0735648X.2025.2535007.

D'Acquisto, Giuseppe, Josep Domingo-Ferrer, Panayiotis Kikiras, Vicenç Torra, Yves-Alexandre de Montjoye, dan Athena Bourka. *Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics*. Versi 1. 2015. https://doi.org/10.48550/ARXIV.1512.06000.

Diana, Diana, Salasaiah Salasaiah, dan Rungarun Boonsayan. "Public Service Innovation in the Era of Society 5.0: Data Protection, Governance, and Regulation in Indonesia." *DISCOURSE: Indonesian Journal of Social Studies and Education* 3, no. 1 (2025): 61–72. https://doi.org/10.69875/djosse.v3i1.315.

Faidlatul Habibah, Astrid, dan Irwansyah Irwansyah. "Era Masyarakat Informasi sebagai Dampak Media Baru." *Jurnal Teknologi Dan Sistem Informasi Bisnis* 3, no. 2 (2021): 350–63. https://doi.org/10.47233/jteksis.v3i2.255.

Fitria, Annisa, dan Diah Putri Hasian. "Pertanggung Jawaban Telkomsel Atas Kebocoran Rahasia Data Pribadi Pengguna Indihome." *Arus Jurnal Sosial dan Humaniora* 5, no. 2 (2025): 1812–21. https://doi.org/10.57250/ajsh.v5i2.1440.

Fitria, Myrna, Dewi Iryani, dan Puguh Aji Hari Setiawan. "Perlindungan Dan Tanggung Jawab Hukum Kebocoran Informasi Data Pribadi Pada Penyelenggara Sistem Elektronik Berdasarkan Perspektif Rahasia Dagang." *Cerdika: Jurnal Ilmiah Indonesia* 5, no. 1 (2025): 1416–23. https://doi.org/10.59141/cerdika.v5i1.2408.

Hardiansyah, Satya Agung, dan Tata Sutabri. *Analisis Pelanggaran Etika Teknologi Informasi Di Indonesia: Studi Kasus Kebocoran Data*. 2026.

Hartono, Julienna, Angelica Milano, Xavier Nugraha, dan Stefania Arshanty. *Failing to Protect Personal Data: Key Aspects of Electronic System Operators' Agreements*. 2023.

Jauhari, Ahmad Ardaful Abror. "Perlindungan Hukum Terhadap Data Pribadi Pengguna Platform Digital Dalam Persfektif Kepastian Hukum." *Journal Equitable* 11, no. 1 (2026).

Judijanto, Loso, Pratama Dahlian Persadha, Indah Susilowati, Heru Kreshna Reza, dan Melly Susanti. "Analisis Keamanan Data dan Perlindungan Privasi dalam Pengelolaan Big Data: Tinjauan Teknologi Enkripsi dan Anonimisasi." *Jurnal Penelitian Inovatif* 5, no. 2 (2025): 1991–2000. https://doi.org/10.54082/jupin.1151.

Maharani, Rista, dan Andria Luhur Prakoso. "Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital." *JURNAL USM LAW REVIEW* 7, no. 1 (2024): 333–47. https://doi.org/10.26623/julr.v7i1.8705.

Mega, Irena Puspa, dan Albertus Sentot Sudarwanto. "PELANGGARAN HAK KONSUMEN ATAS KEBOCORAN DATA PRIBADI OLEH PT.

TELKOMSEL." *Jurnal Privat Law* 13, no. 2 (2025): 224. https://doi.org/10.20961/privat.v13i2.53149.

Muhamad Naufal Aulia Azmi, Habib Saifudin, Cristine T Purba, Asri Suryaningtyas, dan Urfani Syamuria Situmorang. "Analisa Kasus Kebocoran Data pada Bank Indonesia Dalam Sistem Perbankan: Indonesia." *JURNAL MULTIDISIPLIN ILMU AKADEMIK* 1, no. 6 (2024): 448–58. https://doi.org/10.61722/jmia.v1i6.3267.

Nasution, Shulhan Iqbal. *MENS REA: FONDASI PERTANGGUNGJAWABAN PIDANA DALAM SISTEM PERADILAN PIDANA DI INDONESIA*. 7 (2025).

Pramod, Shinde Hema, dan Narendra Kumar Singh. "A Study on Corporate Criminal Liability: Comparative Approach." *Journal of Advances and Scholarly Researches in Allied Education* 20, no. 4 (2023): 797–804. https://doi.org/10.29070/qpzqqg91.

Rahmadani, Siti, dan Rina Arum Prastyanti. "Human Rights and Cybersecurity: Reinforcing Legal Protections for Personal Data." *International Journal of Law Dynamics Review* 3, no. 1 (2025): 20–29. https://doi.org/10.62039/ijldr.v3i1.80.

Rinjani, Muhamad Adri, dan Ricky Firmansyah. "Hambatan Implementasi UU 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia." *Jurnal Analisis Hukum* 8, no. 1 (2025): 70–83. https://doi.org/10.38043/jah.v8i1.6793.

Rr. Dijan Widijowati. "A Comparative Study Of Principle Of Guilt In The Provision Of Indonesian And English Criminal Law." *KRTHA BHAYANGKARA* 18, no. 3 (2024): 559–68. https://doi.org/10.31599/krtha.v18i3.3302.

Silalahi, Johan Alfred Sarades, Yuspika Yuliana Purba, dan Muhammad Fadly Nasution. "Analisis Yuridis terhadap Mekanisme Perlindungan Data Pribadi dalam Sistem Informasi Elektronik Berdasarkan Perspektif Hukum Pidana di Indonesia." *Jurnal Minfo Polgan* 14, no. 1 (2025): 604–13. https://doi.org/10.33395/jmp.v14i1.14810.

Sjahdeini, Sutan Remy. *Ajaran Pemidanaan: Tindak Pidana Korporasi Dan Seluk-Beluknya*. Kencana, 2017.

Tanti Kirana Utami, Kayla Andini Putri, Salsa Octaviani Suryanto, dan Fina Asriani. "Personal Data Breach Cases In Indonesia : Perspective Of Personal Data Protection Law." *Journal Customary Law* 2, no. 2 (2025): 21. https://doi.org/10.47134/jcl.v2i2.3742.

Tyagi, Meenakshi, TNVR Swamy, Amit Chawla, dan Punam Ahlawat. "Digital Evidence and Local Law Enforcement: Challenges in Cybercrime Prosecution." *Advances in Consumer Research* 2, no. 5 (2025).

Volini, Anthony G. "The Right to Data Privacy: Revisiting Warren & Brandeis." *Journal of Technology and Intellectual Property* 21, no. 1 (2023).