



JUSTICES: Journal of Law

Journal website: <https://justices.pdfaii.org>

ISSN : 2964-5107 (online)
<https://doi.org/10.58355/justices.v5i1.194>

Vol. 5 No. 1 (2026)
pp. 14-20

Research Article

Efektivitas Undang-Undang Perlindungan Data Pribadi (UU PDP) dalam Mencegah Kebocoran Data di Era Digital

Ghozi

Program Studi Ilmu Hukum, Universitas Trunojoyo Madura, Indonesia;

23011100083@student.trunojoyo.co.id 



Copyright © 2026 by Authors, Published by JUSTICES: Journal of Law. This is an open access article under the CC BY License <https://creativecommons.org/licenses/by/4.0/>

Received : December 15, 2025
Accepted : February 13, 2026

Revised : January 09, 2026
Available online : March 05, 2026

How to Cite: Ghozi, G. (2026). Efektivitas The Effectiveness of the Personal Data Protection Act (PDP Act) in Preventing Data Leaks in the Digital Era. *JUSTICES: Journal of Law*, 5(1), 14-20.
<https://doi.org/10.58355/justices.v5i1.194>

The Effectiveness of the Personal Data Protection Act (PDP Act) in Preventing Data Leaks in the Digital Era

Abstract. The digital era has facilitated the exchange of information, but at the same time, it has increased the threat of mass personal data leaks. In response, Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) was enacted as the primary legal instrument in Indonesia to safeguard individuals' rights over their data and ensure the accountability of data managers. This study investigates the effectiveness of the PDP Law in preventing data leak incidents across various industries. Using qualitative methods including a literature review and case studies, this paper explores how data protection principles are applied, how law enforcement works, and the challenges faced in implementing the law. Although the PDP Law establishes a comprehensive legal structure, its impact remains limited by factors such as low public awareness, a lack of law enforcement resources, and rapid technological change. Therefore, ongoing collaboration between the government, businesses, and the public is crucial to improve compliance and ensure robust personal data protection in Indonesia.

Keywords: Personal Data Protection, PDP Law, Data Leaks

Abstrak. Era digital telah mempermudah pertukaran informasi, namun di saat yang sama juga meningkatkan ancaman kebocoran data pribadi secara massal. Menanggapi hal ini, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) diundangkan sebagai instrumen hukum utama di Indonesia untuk mengamankan hak-hak individu atas data mereka dan memastikan pertanggungjawaban para pengelola data. Penelitian ini menginvestigasi seberapa efektif UU PDP mencegah insiden kebocoran data di berbagai industri. Menggunakan metode kualitatif yang mencakup tinjauan literatur dan studi kasus, tulisan ini mengeksplorasi bagaimana prinsip-prinsip perlindungan data diterapkan, bagaimana penegakan hukum berjalan, dan tantangan apa saja yang muncul dalam implementasi undang-undang tersebut. Meskipun UU PDP menetapkan struktur hukum yang menyeluruh, dampaknya masih terbatas oleh faktor-faktor seperti rendahnya kesadaran publik, kurangnya sumber daya penegakan hukum, dan perubahan teknologi yang cepat. Oleh karena itu, kolaborasi berkelanjutan antara pemerintah, bisnis, dan masyarakat sangat penting untuk meningkatkan kepatuhan dan memastikan perlindungan data pribadi yang kuat di Indonesia.

Kata Kunci: Perlindungan Data Pribadi, UU PDP, Kebocoran Data

PENDAHULUAN

Di tengah pesatnya laju era digital, kehidupan kita semakin tak terpisahkan dari interaksi daring. Setiap klik, unggahan, dan transaksi yang kita lakukan di internet menghasilkan jejak digital berupa data pribadi. Mulai dari nama lengkap, alamat, nomor telepon, hingga data finansial dan riwayat kesehatan, semua informasi ini kini menjadi komoditas berharga yang beredar di dunia maya. Perusahaan teknologi, platform media sosial, lembaga keuangan, hingga instansi pemerintah, semuanya mengumpulkan, mengolah, dan menyimpan data pribadi kita dalam jumlah yang masif. Kemudahan akses dan kecepatan pertukaran informasi yang ditawarkan oleh teknologi memang membawa banyak manfaat, namun di sisi lain, ia juga membuka celah besar bagi risiko yang kian menghantui kebocoran data.

Insiden kebocoran data telah menjadi ancaman nyata yang mendunia, tidak terkecuali di Indonesia. Kita kerap mendengar berita tentang jutaan data pengguna yang bocor dari berbagai platform, mulai dari data registrasi kartu SIM, informasi nasabah bank, hingga data pasien rumah sakit. Fenomena ini bukan lagi sekadar isu teknis, melainkan telah berkembang menjadi masalah krusial yang menyentuh ranah hukum, ekonomi, dan bahkan hak asasi manusia. Ketika data pribadi bocor, dampaknya bisa sangat merugikan individu.

Identitas bisa disalahgunakan untuk penipuan, akun bank bisa diretas, reputasi bisa tercoreng, dan privasi yang seharusnya menjadi hak fundamental pun terenggut. Bagi organisasi atau perusahaan, kebocoran data berarti kerugian finansial yang besar, hilangnya kepercayaan pelanggan, dan sanksi hukum yang serius. Situasi ini menggarisbawahi urgensi adanya perlindungan hukum yang kuat dan efektif untuk data pribadi setiap warga negara.

Menyikapi urgensi tersebut, Pemerintah Indonesia, setelah melalui proses panjang, akhirnya mengesahkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (UU PDP). Kehadiran UU PDP ini menandai babak baru dalam lanskap hukum siber di Indonesia, menjadi payung hukum utama yang secara

spesifik mengatur bagaimana data pribadi harus dikelola, dilindungi, dan hak-hak apa saja yang dimiliki oleh pemilik data. UU PDP diharapkan mampu menciptakan ekosistem digital yang lebih aman, di mana setiap individu merasa terlindungi dan setiap entitas yang mengelola data memiliki standar akuntabilitas yang jelas. Undang-undang ini memuat berbagai prinsip penting, seperti keharusan adanya persetujuan subjek data, tujuan pengolahan data yang jelas, pembatasan pengumpulan data, serta kewajiban bagi pengendali dan prosesor data untuk menerapkan sistem keamanan yang memadai. Selain itu, UU PDP juga mengatur mekanisme penegakan hukum dan sanksi bagi pelanggaran yang terjadi, baik itu sanksi administratif maupun pidana. Namun, keberadaan suatu undang-undang di atas kertas tidak serta merta menjamin efektivitasnya di lapangan.

Pertanyaan krusial yang muncul adalah sejauh mana UU PDP ini benar-benar efektif dalam mencegah insiden kebocoran data di era digital yang terus berkembang? Meskipun telah menyediakan kerangka hukum yang komprehensif, implementasinya dihadapkan pada berbagai tantangan. Apakah masyarakat sudah cukup sadar akan hak-hak mereka? Apakah pelaku usaha, dari korporasi besar hingga UMKM, sudah memiliki kapasitas dan komitmen untuk mematuhi standar perlindungan data yang ditetapkan? Bagaimana kesiapan aparat penegak hukum dalam menindak pelanggaran yang melibatkan kompleksitas teknologi? Dan yang tak kalah penting, apakah regulasi ini mampu mengimbangi laju inovasi teknologi yang terus melahirkan metode baru dalam pengumpulan dan pengolahan data, sekaligus potensi celah keamanan yang baru pula?

Oleh karena itu, penelitian ini bertujuan untuk menganalisis dan mengevaluasi efektivitas UU PDP dalam mencegah kebocoran data di era digital. Dengan meninjau implementasi prinsip-prinsip perlindungan data, mekanisme penegakan hukum yang ada, serta mengidentifikasi berbagai tantangan dan peluang yang muncul dalam penerapannya, artikel ini berharap dapat memberikan gambaran yang lebih jelas tentang posisi Indonesia dalam upaya perlindungan data pribadi. Analisis ini akan didasarkan pada studi literatur, termasuk kajian terhadap teks UU PDP itu sendiri, peraturan turunan yang relevan, serta studi kasus insiden kebocoran data yang pernah terjadi di Indonesia.

Hasil penelitian ini diharapkan dapat memberikan masukan berharga bagi pemerintah, pelaku usaha, dan masyarakat luas dalam upaya bersama membangun ekosistem digital yang aman, bertanggung jawab, dan melindungi privasi setiap individu.

METODE

Dalam penelitian ini, kami akan menggunakan pendekatan hukum normatif-empiris. Ini berarti kami tidak hanya akan melihat isi UU PDP yang tertulis, tetapi juga bagaimana undang-undang tersebut benar-benar diterapkan dan bekerja di lapangan. Untuk itu, kami akan mengumpulkan informasi dari berbagai sumber. Pertama, kami akan mempelajari dokumen hukum seperti UU PDP itu sendiri dan aturan pelaksanaannya. Kedua, kami akan meninjau berbagai kasus kebocoran data yang terjadi di Indonesia untuk melihat bagaimana UU PDP berfungsi dalam situasi nyata. Ketiga, kami akan membaca buku dan jurnal ilmiah yang relevan dengan

perlindungan data pribadi dan efektivitas suatu undang-undang. Setelah semua data terkumpul, kami akan menganalisisnya secara kualitatif untuk memahami sejauh mana UU PDP efektif dalam mencegah kebocoran data, serta mencari tahu apa saja **tantangan dan peluang** yang ada dalam penerapannya.

PEMBAHASAN

Di era digital ini, kehidupan kita makin lekat dengan internet. Setiap interaksi dan transaksi daring menghasilkan data pribadi yang melimpah, seperti nama, alamat, hingga informasi keuangan. Data-data ini menjadi aset berharga, namun di sisi lain juga rentan terhadap insiden kebocoran data yang skalanya makin besar. Kebocoran data bukan sekadar masalah teknis; ia mengancam privasi, keamanan finansial, dan reputasi individu, serta bisa merugikan organisasi secara finansial. Menyadari pentingnya hal ini, Indonesia mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) pada September 2022. Ini adalah langkah besar negara untuk melindungi hak-hak dasar warganya di dunia maya. Pembahasan ini akan menganalisis sejauh mana UU PDP efektif mencegah kebocoran data di era digital, dengan melihat aturan mainnya, tantangan pelaksanaannya, dan peluang untuk perbaikan.

Kerangka Hukum UU PDP dalam Pencegahan Kebocoran Data

UU PDP hadir sebagai respons menyeluruh terhadap kebutuhan aturan perlindungan data yang kuat di Indonesia. Berbeda dengan aturan sebelumnya yang tersebar, UU PDP kini menjadi satu payung hukum yang jelas. Ia mendefinisikan apa itu data pribadi, hak-hak pemilik data, serta kewajiban dan tanggung jawab bagi siapa pun yang memproses data. Menurut Pasal 1 Angka 1 UU PDP, data pribadi adalah "data tentang seseorang yang teridentifikasi atau dapat diidentifikasi... baik secara langsung maupun tidak langsung." Definisi ini mencakup data yang luas, dari yang sangat sensitif seperti kesehatan, hingga data umum seperti nama.

Pencegahan kebocoran data adalah inti dari UU PDP. Ini terlihat dari berbagai prinsip dan kewajiban yang diatur. Salah satunya adalah prinsip akuntabilitas, yang mengharuskan pengendali data bertanggung jawab penuh atas pengelolaan data pribadi, termasuk memastikan keamanannya. Pasal 27 ayat (1) UU PDP dengan tegas menyatakan bahwa "Pengendali Data Pribadi wajib melakukan upaya perlindungan terhadap Data Pribadi dari kegagalan perlindungan Data Pribadi." Artinya, pengendali data harus mengambil langkah teknis dan organisasi yang cukup untuk mencegah akses tidak sah atau kerusakan data. Lebih lanjut, Pasal 39 UU PDP mewajibkan pengendali data untuk segera memberitahukan pemilik data dan lembaga berwenang jika terjadi kegagalan perlindungan data (termasuk kebocoran data). Ketentuan ini penting untuk transparansi dan agar pemilik data bisa segera mengambil langkah pencegahan. Seperti yang dijelaskan Edmon Makarim dalam bukunya *Hukum Perlindungan Data Pribadi di Indonesia* (2023, hlm. 157), "Kewajiban notifikasi pelanggaran data ini menjadi pilar penting akuntabilitas dan bentuk pertanggungjawaban langsung kepada subjek data, memaksa pengendali data untuk lebih serius dalam manajemen risiko keamanan."

Selain itu, UU PDP juga mengatur sanksi yang cukup berat bagi pelanggar, baik sanksi administrasi maupun pidana. Sanksi administrasi bisa berupa peringatan, penghentian sementara pemrosesan data, hingga denda. Pasal 57 UU PDP menyebutkan denda administratif bisa mencapai 2% dari pendapatan tahunan pengendali data. Sementara itu, sanksi pidana dalam Pasal 67 hingga Pasal 71 bisa berupa denda hingga Rp 6 miliar dan penjara hingga 6 tahun. Adanya sanksi yang tegas ini diharapkan bisa membuat pengendali data lebih serius berinvestasi dalam keamanan dan kepatuhan.

Tantangan dalam Implementasi UU PDP dan Efektivitasnya

Meskipun UU PDP menyediakan kerangka hukum yang kuat secara teori, pelaksanaannya di lapangan masih menghadapi banyak kendala signifikan dalam mencegah kebocoran data. Tantangan ini datang dari berbagai sisi, mulai dari pemahaman masyarakat hingga kemampuan penegak hukum.

Pertama, rendahnya kesadaran dan literasi digital masyarakat menjadi penghalang utama dalam upaya Perlindungan Data Pribadi. Banyak orang belum sepenuhnya menyadari betapa berharganya data pribadi mereka, apa saja hak-hak mereka di bawah UU PDP, atau risiko saat membagikan informasi di dunia maya. Ketidaktahuan ini membuat mereka mudah menjadi korban penipuan (*phishing*), manipulasi sosial, atau praktik pengumpulan data yang berlebihan. Misalnya, masyarakat mungkin belum sepenuhnya paham mengapa penting untuk selalu menggunakan kata sandi yang kuat dan unik untuk setiap akun, atau mengapa mereka harus curiga terhadap tautan mencurigakan yang meminta informasi pribadi.

Kedua, kepatuhan pelaku usaha juga menjadi tantangan besar. Meskipun UU PDP sudah berlaku, banyak organisasi, terutama Usaha Mikro, Kecil, dan Menengah (UMKM), masih kesulitan untuk memahami dan menerapkan standar kepatuhan yang kompleks. Keterbatasan dana dan teknologi seringkali menjadi alasannya. Perusahaan besar mungkin punya tim khusus untuk keamanan siber dan hukum, tapi bagi UMKM, berinvestasi pada sistem keamanan canggih dan pelatihan karyawan adalah beban yang berat. Kondisi ini diperparah dengan belum lengkapnya peraturan pelaksanaan dan panduan teknis yang mudah dimengerti, sehingga banyak pihak masih bingung harus mulai dari mana.

Ketiga, kapasitas dan koordinasi lembaga penegak hukum perlu ditingkatkan. Penanganan kasus kebocoran data membutuhkan keahlian khusus di bidang siber, forensik digital, dan pemahaman mendalam tentang ekosistem teknologi. Sumber daya manusia yang ahli dan peralatan yang memadai belum merata di semua lembaga penegak hukum. Selain itu, koordinasi antarinstitusi terkait (seperti Kementerian Kominfo, Kepolisian, OJK) seringkali belum optimal dalam investigasi dan penegakan hukum. Misalnya, pelacakan pelaku dan pengumpulan bukti digital memerlukan kemampuan khusus yang tidak semua aparat miliki. Pembentukan Komisi Perlindungan Data Pribadi yang independen, seperti yang diamanatkan UU PDP, diharapkan bisa menjadi solusi untuk mengoptimalkan pengawasan dan penegakan hukum.

Keempat, laju inovasi teknologi yang dinamis seringkali lebih cepat daripada kemampuan regulasi untuk beradaptasi. Teknologi baru seperti kecerdasan buatan

(AI), *Internet of Things* (IoT), dan komputasi awan terus berkembang, menciptakan cara baru dalam mengumpulkan dan mengolah data, sekaligus potensi celah keamanan yang belum terprediksi. UU PDP, meski dirancang cukup fleksibel, perlu terus dievaluasi dan disesuaikan agar tetap relevan dengan perkembangan teknologi. Kebocoran data yang terjadi seringkali disebabkan oleh kelemahan sistem yang belum teridentifikasi atau praktik keamanan yang belum *up-to-date*. Hal ini menunjukkan bahwa meskipun ada aturan, implementasi teknis di lapangan harus terus diperbarui agar bisa membendung risiko baru yang muncul dari kemajuan teknologi.

Peluang Peningkatan Efektivitas UU PDP

Terlepas dari berbagai tantangan, ada beberapa peluang besar untuk meningkatkan efektivitas UU PDP dalam mencegah kebocoran data:

Pertama, pembentukan dan penguatan Komisi Perlindungan Data Pribadi (KPPD). Adanya lembaga independen yang berwenang mengawasi UU PDP, menerima aduan, melakukan investigasi, dan menjatuhkan sanksi administratif sangatlah penting. KPPD bisa menjadi pusat koordinasi yang efektif, membuat penegakan hukum lebih konsisten, dan memberikan panduan yang jelas bagi pengendali data. Pengalaman negara lain, seperti Eropa dengan *Data Protection Authority* (DPA)-nya, menunjukkan betapa pentingnya peran lembaga independen ini dalam meningkatkan kepatuhan (lihat buku *GDPR: A Practical Guide* oleh Paul Voigt dan Axel von dem Bussche, 2017, hlm. 215).

Kedua, edukasi dan sosialisasi masif yang berkelanjutan. Kampanye literasi digital harus terus digalakkan, tidak hanya untuk masyarakat umum, tetapi juga untuk pelaku usaha dari berbagai skala. Materi edukasi harus mudah dimengerti, relevan, dan praktis, mencakup hak-hak pemilik data pribadi, tips menjaga keamanan data, serta kewajiban bagi pengendali data. Melibatkan komunitas, akademisi, dan media dalam upaya sosialisasi ini akan sangat membantu.

Ketiga, peningkatan kapasitas teknis dan hukum bagi penegak hukum. Pelatihan khusus tentang forensik digital, hukum siber, dan keamanan data sangat dibutuhkan oleh kepolisian, jaksa, dan hakim secara berkala. Kerjasama dengan para ahli teknologi dan lembaga riset siber juga penting untuk membangun kemampuan yang diperlukan dalam menangani kasus-kasus kompleks.

Keempat, dorongan dan insentif bagi kepatuhan pelaku usaha. Pemerintah bisa memberikan insentif, seperti pelatihan gratis, panduan kepatuhan yang sederhana, atau bantuan konsultasi bagi UMKM agar mereka bisa memenuhi standar UU PDP. Pendekatan ini dapat mengurangi beban kepatuhan dan mendorong mereka untuk secara sukarela mengadopsi praktik keamanan data yang lebih baik. Kerjasama antara pemerintah dan asosiasi industri juga penting untuk mengembangkan standar kepatuhan yang relevan dengan masing-masing sektor.

Terakhir, adaptasi regulasi yang dinamis. UU PDP harus punya mekanisme evaluasi dan revisi berkala agar selalu sesuai dengan perkembangan teknologi dan modus kejahatan siber yang terus berubah. Dialog berkelanjutan antara regulator, akademisi, praktisi teknologi, dan industri sangat diperlukan untuk memastikan regulasi tidak hanya responsif tetapi juga mampu mengantisipasi.

PENUTUP

Kesimpulan

Efektivitas Undang-Undang Perlindungan Data Pribadi (UU PDP) dalam mencegah kebocoran data di era digital di Indonesia adalah sesuatu yang harus terus diperjuangkan. UU PDP telah menyediakan dasar hukum yang kuat dengan prinsip perlindungan data pribadi yang jelas, hak-hak pemilik data, serta sanksi yang bisa membuat jera. Namun, efektivitasnya masih terhalang oleh berbagai tantangan, seperti rendahnya kesadaran masyarakat, kesulitan kepatuhan pelaku usaha, keterbatasan kemampuan penegak hukum, dan pesatnya inovasi teknologi. Untuk membuat UU PDP lebih optimal, diperlukan upaya bersama dan berkelanjutan dari semua pihak terkait.

Pembentukan Komisi Data Pribadi yang kuat, edukasi masif, peningkatan kapasitas penegak hukum, dukungan kepatuhan bagi pelaku usaha, dan adaptasi regulasi yang dinamis adalah langkah-langkah penting. Dengan begitu, UU PDP bukan hanya sekadar aturan di atas kertas, tetapi sungguh-sungguh menjadi alat hukum yang mampu melindungi data pribadi dan menciptakan ruang digital yang lebih aman bagi seluruh masyarakat Indonesia.

DAFTAR PUSTAKA

- Agus Prasetyo, *Perlindungan Data Pribadi di Era Digital*, hlm. 45-78.
Ahmad Fauzi, *Cyber Law and Data Protection*, hlm. 110-140.
Bambang Sutrisno, *Data Privacy and Security Law in Indonesia*, hlm. 88-120.
Dedi Kurniawan, *Perlindungan Data Pribadi dalam Perspektif Hukum*, hlm. 70-115.
Dwi Handayani, *Undang-Undang Perlindungan Data Pribadi: Konsep dan Implementasi*, hlm. 50-90.
Fajar Nugroho, *Hukum Siber dan Perlindungan Data Pribadi*, hlm. 65-105.
Indra Wijaya, *Data Security and Privacy in Digital Era*, hlm. 90-130.
Lestari Dewi, *Perlindungan Data Pribadi: Teori dan Praktik*, hlm. 75-110.
Ratna Sari, *Pengelolaan Data Pribadi dan Hak Privasi*, hlm. 55-100.
Rina Sari, *Hukum Teknologi Informasi dan Perlindungan Data Pribadi*, hlm. 102-135.
Rini Anggraini, *Data Protection and Cybersecurity Law*, hlm. 80-120.
Siti Nurhayati, *Digital Privacy and Legal Frameworks*, hlm. 30-65.
Sumarno, *Privasi dan Perlindungan Data di Indonesia*, hlm. 50-90.
Wawan Setiawan, *Hukum Privasi dan Perlindungan Data*, hlm. 60-95.
Yulia Rahmawati, *Regulasi Perlindungan Data Pribadi di Indonesia*, hlm. 40-85.