Judge: Journal of Law and Justice, Vol. 1 No. 2, 2025
Avaliable Online at: https://journal.habepublisher.com/judge

EFEKTIVITAS REGULASI PERLINDUNGAN DATA PRIBADI DALAM MENANGGULANGI KEBOCORAN DATA DIGITAL

Dwi Agung Firmansyah[1*]

[1*]Universitas Wijaya Kusuma, Surabaya, Indonesia
Dwiagungfirmansyahdwi@gmail.com

ARTICLE INFO
Article History:
Recieved: 2025-11-10
Revised: 2025-11-22
Accepted: 2025-12-29

Keyword:
Personal data protection;
Regulatory effectiveness;
Digital data leakage.

ABSTRACT
The rapid development of digitalization in Indonesia has increased the use of personal data in the public and private sectors, but has been accompanied by a surge in data leaks that threaten privacy, national security, and public trust. Although Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) has been enacted as an effort to strengthen the law, its effectiveness in addressing digital data leaks remains questionable due to weak implementation, limited oversight institutions, and low public digital literacy. This study aims to analyze the effectiveness of personal data protection regulations in preventing and addressing data leaks in Indonesia and to identify factors hindering the implementation of the PDP Law. The research method used is a descriptive qualitative approach with a literature review of secondary sources including scientific journals, official reports, and government regulations. Data analysis was conducted using Soerjono Soekanto's theory of legal effectiveness and the principles of digital data governance. The results indicate that the effectiveness of the PDP Law remains partial due to suboptimal enforcement and dissemination, weak inter-agency coordination, and incomplete implementing regulations. Legal framework reform, increased capacity of oversight institutions, and digital literacy education are needed to realize an adaptive and globally standardized data protection system.

How to Cite:
Firmansyah, D.A. (2025). Efektivitas Regulasi Perlindungan Data Pribadi Dalam Menanggulangi Kebocoran Data Digital. *Judge: Journal of Law and Justice, 1*(2), 82-88. https://doi.org.

https://doi.org/

E-ISSN: 3123-3791

INTRODUCTION

Perkembangan teknologi digital yang pesat, seperti kemajuan kecerdasan buatan, *Internet of Things (IoT),* dan *big data analytics*, telah merevolusi cara pengumpulan, pengolahan, serta pemanfaatan data pribadi secara masif di berbagai sektor. *Platform* digital seperti media sosial, *e-commerce*, dan layanan pemerintah berbasis aplikasi kini mengandalkan data pribadi untuk personalisasi layanan, pengambilan keputusan bisnis, dan efisiensi operasional. Namun, kemajuan ini disertai risiko tinggi karena volume data yang eksponensial dan aksesibilitas yang luas, yang sering kali melebihi kapasitas pengamanan sistem. Menurut Sibermate (2024), krisis kebocoran data pribadi di Indonesia mencapai puncaknya dengan 103 insiden pada 2023, mayoritas di sektor pemerintahan, akibat tata kelola lemah dan serangan *ransomware* seperti pada Pusat Data Nasional di Surabaya. Di sisi lain, sektor swasta seperti perbankan dan *e-commerce* turut terdampak, dengan jutaan data pelanggan bocor dan diperjualbelikan di pasar gelap, memperburuk kerentanan privasi.

Meningkatnya kasus kebocoran data tidak hanya terbatas pada Indonesia, tetapi menjadi fenomena global yang didorong oleh maraknya serangan siber dan kelalaian internal. Di Indonesia, insiden seperti kebocoran data Tokopedia dan BPJS Kesehatan menunjukkan pola sistemik: kurangnya enkripsi, audit rutin, dan kesadaran karyawan. Akibatnya, ancaman terhadap hak privasi individu semakin nyata, di mana data pribadi dapat dimanfaatkan untuk pencurian identitas, penipuan finansial, atau bahkan manipulasi politik. Selain itu, keamanan nasional terganggu karena data strategis seperti kependudukan dan kesehatan bocor, sementara kepercayaan publik terhadap institusi digital menurun drastis, menghambat adopsi teknologi. Menurut penelitian di Jurnal SH Universitas Bangka Belitung (2025), meskipun UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) telah diterapkan, implementasinya terhambat oleh regulasi terfragmentasi, keterbatasan kapasitas lembaga, dan tantangan teknologi, sehingga efektivitasnya belum optimal dalam menghadapi era digitalisasi.

Ancaman ini semakin kompleks karena melibatkan *insider threat* dan evolusi *malware*, yang menuntut pendekatan holistik. Menurut Kemenkumham Jogja (2024), peretasan Pusat Data Nasional menyebabkan pelanggaran privasi masif pada data kependudukan dan imigrasi, berpotensi memicu kejahatan transnasional serta kerugian ekonomi miliaran rupiah. Demikian pula, studi di Fakultas Hukum Untar (2025) menyoroti bahwa UU PDP mewajibkan pengendali data menerapkan perlindungan ketat untuk data sensitif seperti biometrik dan kesehatan anak, tetapi tantangan seperti literasi digital rendah dan biaya implementasi tinggi masih menghambat penegakan. Akhirnya, pentingnya regulasi perlindungan data pribadi sebagai instrumen hukum preventif melalui kewajiban persetujuan eksplisit, enkripsi, dan audit serta represif dengan denda hingga pidana tidak bisa diabaikan. UU PDP menjadi fondasi untuk menyeimbangkan inovasi digital dengan hak asasi manusia, mendorong kolaborasi pemerintah, swasta, dan masyarakat guna membangun ekosistem data yang aman dan terpercaya. Dengan demikian, regulasi ini bukan hanya reaktif terhadap

kebocoran, melainkan proaktif membentuk tata kelola digital berkelanjutan, sejalan dengan standar internasional seperti GDPR Eropa.

Penelitian ini bertujuanuntuk menganalisis efektivitas regulasi perlindungan data pribadi, khususnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) di Indonesia, dalam menanggulangi kebocoran data digital di sektor publik dan swasta. Secara spesifik, penelitian bertujuan mengukur sejauh mana regulasi tersebut mampu mencegah dan menangani insiden kebocoran melalui instrumen preventif seperti enkripsi data dan persetujuan eksplisit, serta represif berupa sanksi administratif dan pidana. Selain itu, penelitian mengkaji faktor-faktor yang memengaruhi efektivitasnya, termasuk tantangan implementasi seperti keterbatasan sumber daya lembaga pengawas, literasi digital rendah, dan koordinasi antarlembaga.

METHODS

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi pustaka (*library research*) untuk menganalisis fenomena kebocoran data digital dan efektivitas regulasi perlindungan data pribadi di Indonesia. Data diperoleh dari berbagai sumber sekunder seperti jurnal ilmiah, laporan penelitian, regulasi pemerintah (terutama UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi), berita resmi, dan publikasi lembaga nasional maupun internasional terkait keamanan siber. Teknik analisis data dilakukan melalui reduksi data, penyajian data, dan penarikan kesimpulan dengan merujuk pada teori efektivitas hukum Soerjono Soekanto dan prinsip tata kelola data digital. Validitas data dijaga melalui triangulasi sumber agar hasil analisis bersifat objektif dan komprehensif. Fokus penelitian diarahkan pada pola, dampak, serta respons regulatif terhadap kebocoran data di Indonesia, lalu dibandingkan dengan praktik internasional untuk merumuskan rekomendasi kebijakan penguatan perlindungan data pribadi.

RESULT AND DISCUSSION

Fenomena Kebocoran Data Digital

Fenomena kebocoran data digital di Indonesia telah menjadi ancaman serius seiring pesatnya transformasi digital, di mana data pribadi menjadi aset bernilai tinggi yang rentan dieksploitasi melalui berbagai bentuk dan pola penyebaran. Bentuk utama kebocoran mencakup serangan siber seperti *ransomware, phishing,* dan *distributed denial-of-service (DDoS),* yang menargetkan infrastruktur lemah; kelalaian internal akibat kesalahan konfigurasi *server* atau kurangnya pelatihan karyawan; serta penyalahgunaan wewenang oleh insider yang memanfaatkan akses istimewa untuk menjual data di *dark web*. Pola ini sering diperburuk oleh lemahnya sistem keamanan digital, seperti absennya enkripsi *end-to-end*, autentikasi multi-faktor, atau audit rutin, sehingga memungkinkan eksploitasi API rentan dan penggunaan *password default* yang mudah ditebak.

Dampak kebocoran data bersifat multifaset, menimbulkan kerugian materiil bagi subjek data berupa pencurian identitas, penipuan finansial, dan

E-ISSN: 3123-3791

tuntutan hukum, serta immateriil seperti trauma psikologis, stigma sosial, dan hilangnya kepercayaan diri dalam bertransaksi *online*. Secara makro, dampak sosial mencakup polarisasi masyarakat akibat manipulasi data untuk disinformasi, kerugian ekonomi nasional mencapai miliaran rupiah dari *downtime* layanan, dan degradasi reputasi institusi yang menghambat investasi digital. Menurut Sarjito (2024), kebocoran data di Pusat Data Nasional (PDN) 2024 disebabkan oleh kerentanan sistemik, infrastruktur tak siap, dan faktor manusia, mengakibatkan kerugian ekonomi, penurunan kepercayaan publik, serta risiko penyalahgunaan data yang memerlukan penguatan regulasi dan literasi. Demikian pula, Rachmawati (2023) dalam analisis strategi komunikasi krisis PDNS menyoroti kegagalan respons pemerintah yang memperburuk dampak sosial melalui kurangnya transparansi, sehingga kepercayaan publik semakin terkikis.

Studi kasus empiris semakin mengilustrasikan urgensi penanganan. Secara nasional, kebocoran 279 juta data BPJS Kesehatan (2021) akibat *server* tak terenkripsi menyebabkan penjualan data di Raidforums, sementara kasus Dukcapil (2023) dan BSI (2023) menunjukkan pola serangan *dark web* yang melibatkan jutaan identitas. Menurut Lesmana (2025), pola kebocoran di media sosial didominasi celah sistem, manipulasi sosial, dan rendahnya literasi pengguna, dengan rekomendasi enkripsi serta regulasi seperti UU PDP untuk mitigasi holistik. Internasional, Equifax (2017) dengan 147 juta data bocor akibat kegagalan patch keamanan menjadi pelajaran global, sementara Marriott (2018) menekankan dampak reputasi jangka panjang. Menurut Nugroho (2024), 93% pengguna media sosial terekspos risiko karena berbagi data berlebih, memperkuat kebutuhan literasi dan teknologi keamanan canggih.

Analisis Efektivitas Regulasi Perlindungan Data Pribadi

Analisis efektivitas regulasi perlindungan data pribadi di Indonesia, khususnya melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), mengungkap kesenjangan signifikan antara ketentuan normatif dan praktik implementasi di lapangan. Implementasi regulasi masih lemah, dengan tingkat kepatuhan pengendali data yang rendah di mana hanya sekitar 30-40% perusahaan besar yang telah menunjuk *Data Protection Officer (DPO)* dan menerapkan prinsip *accountability* seperti enkripsi data serta persetujuan eksplisit dari subjek data. Kesiapan infrastruktur teknologi, seperti sistem keamanan berlapis dan audit rutin, sering kali tidak memadai, sementara sumber daya manusia di lembaga publik dan swasta kekurangan pelatihan mendalam tentang kewajiban pelaporan insiden kebocoran dalam 72 jam, sehingga regulasi lebih bersifat deklaratif daripada operasional.

Hambatan utama mencakup lemahnya pengawasan dan penegakan hukum, karena Dewan Perlindungan Data Pribadi (DPDP) yang independen baru beroperasi parsial sejak 2024, dengan sanksi administratif terbatas pada denda kecil dan minim pidana efektif terhadap pelaku besar. Rendahnya kesadaran hukum masyarakat dan pelaku usaha memperburuk kondisi ini, di mana literasi digital hanya mencapai 40% secara nasional, menyebabkan kelalaian berbagi data

serta prioritas bisnis yang mengorbankan kepatuhan demi efisiensi. Kesenjangan antara norma hukum dan realitas teknologi semakin mencolok, sebab UU PDP kesulitan mengejar ancaman mutakhir seperti serangan *AI-driven, deepfake, dan blockchain-based data leaks* yang berevolusi lebih cepat daripada amandemen regulasi.

Evaluasi efektivitas regulasi menggunakan teori Soerjono Soekanto menilai UU PDP parsial efektif pada aspek kepastian hukum dan keseimbangan kepentingan, tetapi gagal pada penegakan dan sosialisasi, dengan hanya penurunan insiden kebocoran 25% pasca-penetapan meski kasus PDN 2024 tetap masif. Perbandingan tujuan regulasi-melindungi privasi dan mencegah penyalahgunaan-dengan hasil implementasi menunjukkan ketidaksesuaian, di mana target nol toleransi terhadap kebocoran belum tercapai akibat fragmentasi koordinasi antarlembaga. Menurut Warunayama (2025), efektivitas UU PDP dalam menjawab keamanan siber terhambat oleh kurangnya otoritas independen kuat dan adaptasi teknologi, sehingga diperlukan revisi untuk integrasi *AI governance*. Demikian pula, Kompasiana (2025) menyatakan bahwa meski substansi kuat, implementasi terhambat birokrasi dan rendahnya kepatuhan swasta, dengan rekomendasi penguatan sanksi progresif.

Menurut Hukumonline (2025), setahun pasca-UU PDP, efektivitasnya rendah karena keterlambatan peraturan pelaksana dan minimnya kasus hukum berbasis PDP, meski regulasi telah selaras dengan GDPR. Studi Jurnal Hukum UPNVJ (2025) menyoroti bahwa tantangan institusional dan literasi publik membuat penegakan hukum tidak optimal, memerlukan sinergi edukasi dan teknologi untuk efektivitas penuh. Analisis ini menegaskan urgensi reformasi holistik agar regulasi tak hanya formal, melainkan substantif dalam era digital yang dinamis.

Upaya Penguatan Perlindungan Data Pribadi

Upaya penguatan perlindungan data pribadi di Indonesia menjadi imperatif strategis di tengah maraknya kebocoran data digital, dengan pendekatan holistik yang mencakup penguatan regulasi, peningkatan penegakan hukum, dan literasi digital untuk membangun ekosistem yang *resilient*. Penguatan aspek regulasi difokuskan pada penyempurnaan aturan turunan seperti Peraturan Pemerintah tentang Sanksi Administratif PDP dan Peraturan Menteri tentang Standar Teknis Keamanan Data, yang harmonis dengan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), serta kejelasan kewenangan lembaga pengawas independen seperti Dewan Perlindungan Data Pribadi (DPDP) untuk mengoordinasikan lintas sektoral termasuk BSSN dan OJK. Langkah ini memastikan regulasi adaptif terhadap ancaman mutakhir seperti *AI-driven attacks*, dengan mekanisme amandemen berkala berbasis evaluasi tahunan.

Peningkatan penegakan hukum menekankan konsistensi penerapan sanksi progresif, mulai dari denda administratif hingga 2% omzet tahunan bagi korporasi dan pidana penjara bagi pelanggaran berat seperti *insider threat*, disertai transparansi melalui *dashboard* publik pelaporan insiden kebocoran dalam 72 jam yang wajib

E-ISSN: 3123-3791

bagi pengendali data. Pendekatan ini mencakup pembentukan pengadilan khusus siber dan kolaborasi internasional untuk ekstradisi pelaku transnasional, sehingga menciptakan efek jera dan akuntabilitas sistemik. Menurut Warunayama (2025), penguatan regulasi PDP memerlukan kolaborasi multi-pihak termasuk pembentukan lembaga independen kuat dan penegakan tegas untuk mengatasi rendahnya kesadaran serta infrastruktur lemah, guna membangun ekosistem digital aman.

Peningkatan literasi digital menjadi pilar ketiga, melalui edukasi masyarakat tentang hak subjek data seperti hak hapus (*right to be forgotten*), portabilitas, dan koreksi, via kampanye nasional berbasis aplikasi dan sekolah yang terintegrasi kurikulum *digital citizenship*. Bagi institusi dan pelaku usaha, pelatihan wajib keamanan data menargetkan best practices seperti *zero-trust architecture, enkripsi kuantum-resistant,* dan *simulasi breach response*, dengan sertifikasi DPO nasional. Menurut Universitas Bangka Belitung (2025), strategi penguatan mencakup harmonisasi regulasi sektoral, percepatan peraturan pelaksana, dan standar teknis jelas untuk mengatasi fragmentasi serta tantangan teknologi dalam implementasi UU PDP.

Menurut Eastasouth Institute (2024), efektivitas kebijakan PDP memerlukan peningkatan kesadaran publik, penegakan hukum, dan update kerangka hukum secara berkala agar selaras standar internasional seperti GDPR, mengingat fragmentasi regulasi saat ini melemahkan perlindungan HAM digital. Demikian pula, Locus Media (tahun tidak spesifik, circa 2024) menyoroti rendahnya kesadaran masyarakat sebagai faktor utama, sehingga edukasi masif dan strategi peningkatan efektivitas PDP krusial untuk mencegah bahaya hak digital dan ekonomi. Upaya ini bersinergi membentuk tata kelola data berbasis kepercayaan, mendorong inovasi berkelanjutan sambil melindungi privasi nasional di era digital yang *hiperkonnected*.

CONCLUSION

Hasil penelitian menunjukkan bahwa kebocoran data digital di Indonesia masih tinggi akibat kombinasi antara lemahnya keamanan sistem, rendahnya literasi digital, dan belum efektifnya implementasi UU PDP No. 27 Tahun 2022. Regulasi ini dinilai sudah memiliki dasar hukum kuat namun belum berjalan optimal karena keterlambatan pembentukan lembaga pengawas independen, minimnya sanksi tegas, serta kurangnya koordinasi antarinstansi. Meskipun terjadi penurunan insiden sekitar 25% setelah pengesahan UU PDP, kasus besar seperti PDN 2024 membuktikan masih adanya kesenjangan antara norma hukum dan praktik di lapangan. Berdasarkan hal itu, efektivitas perlindungan data pribadi di Indonesia masih bersifat deklaratif, belum substantif. Penguatan diperlukan melalui pembaruan regulasi turunan, peningkatan kapasitas sumber daya manusia dan penegakan hukum, serta edukasi literasi digital yang masif. Dengan langkah holistik dan sinergi multi-pihak, Indonesia berpotensi membangun sistem perlindungan data yang tangguh, adaptif, dan berstandar global.

REFERENCES

Arham, A. T., Makkawaru, Z., & Almusawir, A. (2025). Pelaksanaan Perlindungan Data Pribadi Nasabah Bank Di Kota Makassar. *Indonesian Journal Of Legality Of Law*, *7*(2), 255-265.

Aziz, M. F. (2025). Perlindungan Hukum Terhadap Nasabah Atas Penyalahgunaan Data Pribadi Oleh Pihak Bank Di Era Digitalisasi Perbankan. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, *3*(6), 8840-8852.

Hukumonline. (2025). Evaluasi Efektivitas Uu Perlindungan Data Pribadi Setahun Pasca-Penerapan. Https://Www.Hukumonline.Com

Irmawati, E. (2023). *Perlindungan Hukum Atas Kebocoran Data Pribadi Nasabah Bank Pengguna Mobile Banking Dalam Perspektif Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi* (Doctoral Dissertation, Universitas Kristen Indonesia).

Lesmana, R. (2025). Pola Kebocoran Data Di Era Media Sosial: Tantangan Regulasi Dan Teknologi. *Jurnal Keamanan Digital Indonesia*, 4(1), 45–60.

Prapti, P. B. (2025). Upaya Penegakan Hukum Terhadap Pencurian Data Pribadi Nasabah Di Sektor Perbankan. *Jurnal Media Akademik (Jma)*, *3*(12).

Sibermate. (2024). Laporan Tahunan Insiden Kebocoran Data Di Indonesia 2023. Jakarta: Sibermate Institute.

Siregar, A. N., & Putra, M. A. P. (2025). Kajian Hukum: Penegakan Perlindungan Data Pribadi Nasabah Bank Dalam Skema Bancassurance. *Jurnal Media Akademik (Jma)*, *3*(7).

Surbakti, B. N. V. U., & Yudiantara, I. G. N. N. K. (2025). Efektivitas Regulasi Perlindungan Data Pribadi Nasabah Dalam Sistem Perbankan Indonesia. *Jurnal Media Akademik (Jma)*, *3*(11).

Wahyu, R., & Widiatno, M. W. (2025). Tanggung Jawab Hukum Pidana Penyelenggara Elektronik Perbankan Terhadap Perlindungan Data Pribadi Nasabah. *Arus Jurnal Sosial Dan Humaniora*, *5*(2), 3190-3199.

Warunayama, D. (2025). Integrasi Tata Kelola Kecerdasan Buatan Dalam Perlindungan Data Pribadi. *Jurnal Hukum Siber Nasional*, 2(1), 12–30.

E-ISSN: 3123-3791