HUNILA: Jurnal Ilmu Hukum dan Integrasi Peradilan
Volume 4, Nomor 2, Desember 2025
e-ISSN : 2963-0487
DOI: 10.53491/hunila.v4i2.2077

TINJAUAN EFEKTIFITAS HUKUM UNDANG-UNDANG PERLINDUNGAN DATA PRIBADI DALAM KASUS KEBOCORAN DATA DI INDONESIA

[Rizqy Dimas Monica][1], [Exanti Tira Permatasari][2]
Universitas Terbuka[1], Universitas Langlangbuana[2]
045384803@ecampus.ut.ac.id[2], Exantitira@gmail.com[2]

Abstract

This study aims to analyze the effectiveness of the implementation of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) in addressing and preventing cases of data breaches in Indonesia. This research employs a normative juridical method using statutory and conceptual approaches through the examination of laws and regulations, academic literature, scientific journals, and previous studies relevant to personal data protection. The findings indicate that although the PDP Law has adopted various data protection principles aligned with the European Union's General Data Protection Regulation (GDPR), its implementation effectiveness in Indonesia still faces several challenges. These obstacles include suboptimal law enforcement mechanisms, the absence of a fully functional and independent supervisory authority, and the low level of compliance among public and private sectors with personal data protection obligations. In addition, limitations in cybersecurity infrastructure and low levels of digital literacy and public awareness also affect the effectiveness of the implementation of the PDP Law. Therefore, strengthening implementing regulations, enhancing institutional capacity, and harmonizing data protection standards are necessary to ensure effective protection of citizens' privacy rights.

Keywords: *Legal Effectiveness Review*; *Personal Data Protection Law*; *Data Breach Prevention.*

Abstrak

Penelitian ini bertujuan untuk menganalisis efektivitas penerapan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dalam menanggulangi dan mencegah terjadinya kasus kebocoran data di Indonesia. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan dan pendekatan konseptual melalui penelaahan terhadap peraturan perundang-undangan, literatur akademik, jurnal ilmiah, serta hasil penelitian terdahulu yang relevan dengan perlindungan data pribadi. Hasil penelitian menunjukkan bahwa meskipun UU PDP telah mengadopsi berbagai prinsip perlindungan data yang sejalan dengan General Data Protection Regulation (GDPR) Uni Eropa, efektivitas implementasinya di Indonesia masih menghadapi berbagai kendala. Hambatan tersebut meliputi belum optimalnya mekanisme

penegakan hukum, belum terbentuk dan berfungsinya lembaga pengawas yang independen secara maksimal, serta rendahnya tingkat kepatuhan sektor publik dan swasta terhadap kewajiban perlindungan data pribadi. Selain itu, keterbatasan infrastruktur keamanan siber dan rendahnya literasi serta kesadaran digital masyarakat turut memengaruhi efektivitas pelaksanaan UU PDP. Oleh karena itu, diperlukan penguatan regulasi turunan, peningkatan kapasitas kelembagaan, serta harmonisasi standar perlindungan data guna menjamin perlindungan hak privasi warga negara secara efektif.

***Kata Kunci**: Tinjauan Efektivitas Hukum*; *Undang-undang Perlindungan Data Pribadi*; *Kasus Kebocoran Data*

A. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi pada era digital telah mengubah secara signifikan pola interaksi sosial, aktivitas ekonomi, serta sistem pemerintahan modern. Digitalisasi tidak hanya menghadirkan kemudahan dalam akses informasi dan layanan publik, tetapi juga meningkatkan ketergantungan terhadap pengelolaan data, khususnya data pribadi. Dalam konteks Indonesia, data pribadi kini menjadi aset strategis yang memiliki nilai ekonomi tinggi, namun sekaligus rentan terhadap berbagai bentuk penyalahgunaan, seperti pencurian identitas, penipuan digital, hingga perdagangan data ilegal. Seiring dengan pesatnya pertumbuhan ekonomi digital dan layanan berbasis daring, risiko terhadap keamanan data pribadi juga semakin meningkat.

Menurut Algamar menyatakan bahwa kewajiban pemberitahuan kebocoran data (data breach notification) di Indonesia masih belum seragam dan menimbulkan ketidakpastian hukum di berbagai sektor (Algamar, 2024). Kondisi ini menunjukkan bahwa sebelum hadirnya regulasi yang komprehensif, pengaturan mengenai perlindungan data pribadi di Indonesia masih bersifat sektoral dan belum terintegrasi secara nasional. Akibatnya, terdapat perbedaan standar dan mekanisme perlindungan data di berbagai sektor, seperti perbankan, telekomunikasi, dan layanan digital lainnya. Ketidakseragaman ini tidak hanya menimbulkan kebingungan bagi pelaku usaha, tetapi juga mengurangi tingkat perlindungan hukum bagi masyarakat sebagai subjek data (Algamar, 2024).

Sebagai respons terhadap kebutuhan tersebut, pemerintah Indonesia mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Regulasi ini merupakan tonggak penting dalam sistem hukum nasional karena untuk pertama kalinya Indonesia memiliki kerangka hukum yang secara khusus mengatur perlindungan data pribadi secara komprehensif. UU PDP mengatur berbagai aspek, mulai dari definisi dan klasifikasi data pribadi, hak subjek data, kewajiban pengendali dan pemroses data, hingga mekanisme sanksi administratif dan pidana. Kehadiran UU PDP diharapkan mampu memberikan kepastian hukum, meningkatkan kepercayaan publik, serta memperkuat tata kelola keamanan data di Indonesia.

Namun demikian, sebagaimana dikemukakan oleh Sari, efektivitas UU PDP belum optimal karena masih terdapat

enforcement gap, yaitu kesenjangan antara norma hukum yang tertuang dalam peraturan perundang-undangan dengan praktik implementasinya di lapangan. Dalam perspektif hukum positif, efektivitas suatu peraturan tidak hanya diukur dari keberadaannya secara formal, tetapi juga dari sejauh mana peraturan tersebut dipatuhi, diawasi, dan ditegakkan secara konsisten (Sari, 2024).

Lebih lanjut, Utami dkk. menjelaskan bahwa sebagian besar insiden kebocoran data di Indonesia disebabkan oleh lemahnya kontrol akses serta kesalahan konfigurasi sistem (Utami et al., 2025). Hal ini menunjukkan bahwa permasalahan perlindungan data pribadi tidak semata-mata berkaitan dengan aspek hukum, tetapi juga sangat dipengaruhi oleh faktor teknis dalam pengelolaan sistem informasi. Dalam konteks tersebut, Simbolon menegaskan pentingnya pedoman teknis yang terintegrasi dengan regulasi hukum agar prinsip-prinsip perlindungan data dapat diterapkan secara konsisten (Simbolon, 2022).

Selain aspek regulatif dan teknis, faktor kelembagaan juga memegang peranan penting dalam menentukan efektivitas UU PDP. Keberadaan lembaga pengawas yang independen dan profesional menjadi elemen krusial dalam memastikan pengawasan dan penegakan hukum berjalan secara optimal. Tanpa dukungan kelembagaan yang kuat, pelaksanaan UU PDP berpotensi mengalami hambatan, terutama dalam hal koordinasi antarinstansi dan konsistensi penegakan sanksi.

Di sisi lain, pendekatan hukum internasional seperti General Data Protection Regulation (GDPR) di Uni Eropa dapat dijadikan sebagai tolok ukur dalam meningkatkan kualitas regulasi dan praktik perlindungan data di Indonesia. GDPR dikenal sebagai salah satu regulasi perlindungan data paling komprehensif di dunia, dengan penekanan pada prinsip accountability, transparency, dan perlindungan hak subjek data. Menurut Danrivanto (2024), penerapan prinsip-prinsip accountability, transparency, dan perlindungan hak subjek data sebagaimana diatur dalam GDPR perlu diadopsi dalam praktik kelembagaan di Indonesia guna memperkuat kepercayaan publik terhadap sistem perlindungan data.

Sebagai ilustrasi, dalam GDPR, setiap pengendali data diwajibkan untuk dapat membuktikan kepatuhan terhadap prinsip perlindungan data melalui dokumentasi dan audit yang sistematis. Pendekatan ini tidak hanya menekankan kepatuhan formal, tetapi juga mendorong terciptanya budaya perlindungan data dalam organisasi. Jika dibandingkan dengan Indonesia, pendekatan semacam ini masih perlu diperkuat, baik dari sisi regulasi turunan maupun implementasinya di lapangan.

Dengan demikian, efektivitas UU PDP perlu dilihat secara komprehensif dengan mempertimbangkan berbagai aspek, yaitu regulatif, kelembagaan, teknis, dan kultural. Keempat aspek tersebut saling berkaitan dan tidak dapat dipisahkan dalam mewujudkan sistem perlindungan data yang optimal. Tanpa dukungan dari seluruh elemen tersebut, tujuan UU PDP untuk melindungi hak privasi individu serta meningkatkan keamanan data nasional akan sulit tercapai secara maksimal.

Berdasarkan latar belakang tersebut,

penelitian ini bertujuan untuk menganalisis tingkat efektivitas penerapan UU PDP di Indonesia, mengidentifikasi faktor-faktor yang memengaruhi pelaksanaannya, serta melakukan perbandingan dengan prinsip-prinsip perlindungan data dalam GDPR Uni Eropa. Melalui pendekatan tersebut, diharapkan dapat diperoleh pemahaman yang lebih komprehensif mengenai standar perlindungan data yang ideal serta rekomendasi kebijakan yang relevan bagi penguatan sistem perlindungan data pribadi di Indonesia.

Pemilihan judul *"Tinjauan Efektivitas Hukum Undang-Undang Perlindungan Data Pribadi dalam Kasus Kebocoran Data di Indonesia"* didasarkan pada meningkatnya kasus kebocoran data pribadi yang menimbulkan ancaman terhadap hak privasi, keamanan informasi, serta kepercayaan masyarakat terhadap sistem digital di Indonesia. Kehadiran Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menjadi langkah penting dalam memberikan kepastian hukum dan perlindungan bagi pemilik data melalui pengaturan hak subjek data, kewajiban pengendali data, serta mekanisme pertanggungjawaban atas pelanggaran. Namun, keberadaan regulasi tersebut belum secara otomatis menjamin berkurangnya insiden kebocoran data apabila implementasi dan penegakan hukumnya belum berjalan optimal. Oleh karena itu, penting dilakukan kajian terhadap efektivitas hukum UU Perlindungan Data Pribadi untuk menilai sejauh mana norma hukum yang telah dibentuk mampu diterapkan secara nyata dalam mencegah, menangani, dan memberikan perlindungan hukum terhadap kasus kebocoran data di Indonesia.

B. METODE PENELITIAN

Penelitian ini menggunakan pendekatan yuridis normatif, yaitu metode yang menelaah dan menganalisis hukum berdasarkan norma-norma tertulis yang terdapat dalam peraturan perundang-undangan serta literatur hukum yang relevan. Pendekatan ini dipilih karena penelitian berfokus pada kajian terhadap efektivitas peraturan hukum yang berlaku. Menurut Soerjono Soekanto (2017), pendekatan yuridis normatif adalah penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder yang meliputi asas-asas hukum, doktrin, dan peraturan perundang-undangan. Jenis data yang digunakan dalam penelitian ini adalah data sekunder yang terdiri dari bahan hukum primer berupa peraturan perundang-undangan terkait seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, serta Peraturan Pemerintah tentang Penyelenggaraan Sistem Elektronik; bahan hukum sekunder berupa buku, jurnal ilmiah, artikel penelitian, dan pendapat para ahli yang mendukung analisis; serta bahan hukum tersier seperti kamus hukum, ensiklopedia hukum, dan sumber daring akademik yang relevan.

Metode analisis dan pengolahan data dalam penelitian berjudul *"Tinjauan Efektivitas Hukum Undang-Undang Perlindungan Data Pribadi dalam Kasus Kebocoran Data di Indonesia"* menggunakan metode analisis kualitatif dengan pendekatan yuridis normative (Fajrul Mmtaz, 2025). Data yang digunakan berupa data sekunder yang diperoleh melalui studi kepustakaan,

meliputi bahan hukum primer seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan peraturan terkait, bahan hukum sekunder berupa buku, jurnal ilmiah, hasil penelitian terdahulu, serta bahan hukum tersier yang mendukung kajian. Pengolahan data dilakukan melalui tahapan inventarisasi, klasifikasi, dan sistematisasi bahan hukum untuk mengidentifikasi konsep, norma, serta mekanisme perlindungan data pribadi yang berlaku (Heru Suherman, 2025) Selanjutnya, data dianalisis secara deskriptif-analitis dengan menafsirkan ketentuan hukum yang ada dan menghubungkannya dengan fenomena kasus kebocoran data di Indonesia guna menilai tingkat efektivitas penerapan hukum dalam memberikan perlindungan terhadap hak privasi masyarakat.

C. HASIL DAN PEMBAHASAN

A. Efektivitas Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dalam Menangani Kebocoran Data di Indonesia

A. Efektivitas Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dalam Menangani Kebocoran Data di Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) lahir sebagai respons atas meningkatnya ancaman penyalahgunaan dan kebocoran data pribadi di era digital. Kehadiran UU PDP diharapkan dapat memberikan kepastian hukum, meningkatkan akuntabilitas pengendali data, serta menjamin perlindungan hak privasi masyarakat sebagai bagian dari hak asasi manusia (ELSAM, 2019). Secara normatif, UU PDP telah mengatur prinsip-prinsip dasar perlindungan data pribadi yang mengadopsi standar internasional, seperti prinsip legalitas pemrosesan data, persetujuan pemilik data, pembatasan tujuan penggunaan data, keamanan data, serta hak subjek data untuk mengakses, memperbaiki, dan menghapus data pribadinya (Republik Indonesia, 2022). Namun demikian, keberadaan norma hukum tidak secara otomatis menjamin efektivitas perlindungan data apabila tidak didukung oleh sistem penegakan hukum yang memadai.

Menurut teori efektivitas hukum Soerjono Soekanto, keberhasilan suatu peraturan perundang-undangan ditentukan oleh lima faktor utama, yaitu faktor hukum, faktor penegak hukum, faktor sarana atau fasilitas, faktor masyarakat, dan faktor budaya hukum (Soekanto, 2008). Dengan menggunakan kerangka teori tersebut, efektivitas UU PDP dapat dianalisis secara lebih komprehensif. Pendekatan ini memungkinkan identifikasi berbagai kendala yang tidak hanya bersifat normatif, tetapi juga struktural dan kultural dalam implementasi perlindungan data pribadi di Indonesia (Prasetyo & Karo-Karo, 2021).

Dari aspek hukum (legal substance), UU PDP sebenarnya telah memberikan dasar hukum yang relatif lengkap dibandingkan dengan regulasi sebelumnya yang masih tersebar dalam berbagai peraturan sektoral. UU ini mengintegrasikan berbagai prinsip perlindungan data dalam satu kerangka hukum yang sistematis, sehingga secara teoritis mampu mengatasi fragmentasi regulasi yang sebelumnya terjadi. Namun demikian, hingga beberapa tahun setelah pengesahannya, sejumlah peraturan pelaksana masih belum sepenuhnya tersedia. Ketiadaan regulasi turunan ini

menimbulkan ketidakpastian dalam implementasi teknis, seperti standar keamanan data, mekanisme audit, serta prosedur pelaporan kebocoran data (Republik Indonesia, 2022).

Selanjutnya, dari aspek penegak hukum (law enforcement), efektivitas UU PDP masih menghadapi berbagai tantangan. Meskipun undang-undang ini telah mengatur sanksi administratif dan pidana, implementasinya di lapangan belum berjalan secara optimal. Kasus kebocoran data yang terjadi dalam beberapa tahun terakhir menunjukkan bahwa penegakan hukum terhadap pelanggaran perlindungan data masih terbatas. Hal ini antara lain disebabkan oleh belum optimalnya koordinasi antarinstansi, keterbatasan kapasitas aparat penegak hukum dalam menangani kasus berbasis teknologi informasi, serta belum terbentuknya lembaga pengawas independen yang memiliki kewenangan kuat. Akibatnya, efek jera terhadap pelanggar masih relatif rendah.

Dari aspek sarana atau fasilitas, kesiapan infrastruktur teknologi dan keamanan siber juga menjadi faktor penting dalam menentukan efektivitas UU PDP. Banyak organisasi, baik di sektor publik maupun swasta, masih memiliki keterbatasan dalam hal sistem keamanan informasi, seperti penggunaan enkripsi, pengelolaan akses, serta sistem deteksi dan respons terhadap insiden. Keterbatasan ini menyebabkan tingginya kerentanan terhadap kebocoran data, yang pada akhirnya menghambat implementasi prinsip-prinsip perlindungan data sebagaimana diatur dalam UU PDP.

Sementara itu, dari aspek masyarakat, tingkat literasi digital dan kesadaran terhadap pentingnya perlindungan data pribadi masih relatif rendah. Banyak masyarakat yang belum memahami hak-haknya sebagai subjek data, termasuk hak untuk memberikan persetujuan, mengakses data, atau menuntut pertanggungjawaban atas penyalahgunaan data. Rendahnya kesadaran ini menyebabkan masyarakat cenderung pasif dan tidak kritis dalam menghadapi potensi pelanggaran data pribadi.

Terakhir, dari aspek budaya hukum (legal culture), masih terdapat kecenderungan rendahnya kepatuhan terhadap regulasi perlindungan data, baik di kalangan masyarakat maupun pelaku usaha. Budaya hukum yang belum terbentuk secara kuat ini berdampak pada kurangnya komitmen dalam menerapkan prinsip-prinsip perlindungan data secara konsisten. Dalam banyak kasus, perlindungan data masih dianggap sebagai beban administratif, bukan sebagai kewajiban hukum yang harus dipatuhi secara serius.

Selain itu, terdapat kesenjangan antara norma hukum dan praktik di lapangan. Meskipun UU PDP mengatur kewajiban pengendali data untuk menjaga kerahasiaan dan keamanan data pribadi, berbagai kasus kebocoran data berskala besar masih terus terjadi. Hal ini menunjukkan bahwa efektivitas UU PDP tidak dapat diukur hanya dari keberadaan norma, melainkan harus dilihat dari tingkat kepatuhan para penyelenggara sistem elektronik terhadap kewajiban yang diatur dalam undang-undang tersebut.

Sebagai ilustrasi, sejumlah insiden kebocoran data yang melibatkan jutaan data pengguna layanan digital

menunjukkan bahwa banyak organisasi belum menerapkan standar keamanan yang memadai. Dalam beberapa kasus, kebocoran terjadi akibat kesalahan konfigurasi sistem atau lemahnya kontrol akses, yang sebenarnya dapat dicegah melalui penerapan praktik keamanan informasi yang baik. Kondisi ini menegaskan bahwa tantangan utama dalam implementasi UU PDP tidak hanya terletak pada aspek regulasi, tetapi juga pada kesiapan teknis dan komitmen institusional.

Dengan demikian, efektivitas UU PDP dalam menangani kebocoran data di Indonesia masih menghadapi berbagai tantangan multidimensional. Upaya peningkatan efektivitas perlu dilakukan secara menyeluruh, meliputi penyempurnaan regulasi turunan, penguatan kelembagaan, peningkatan kapasitas penegak hukum, pengembangan infrastruktur keamanan siber, serta peningkatan kesadaran dan budaya hukum masyarakat. Tanpa langkah-langkah tersebut, tujuan UU PDP untuk memberikan perlindungan yang optimal terhadap data pribadi akan sulit tercapai secara maksimal.

B. Analisis Kasus Kebocoran Data Pribadi di Indonesia

1. Kasus Kebocoran Data BPJS Kesehatan

Kasus kebocoran data BPJS Kesehatan pada tahun 2021 merupakan salah satu insiden terbesar dalam sejarah keamanan siber Indonesia. Sebanyak sekitar 279 juta data penduduk Indonesia diduga diperjualbelikan melalui forum daring internasional (Tempo, 2021). Data yang bocor mencakup Nomor Induk Kependudukan (NIK), nomor telepon, alamat, hingga informasi kesehatan peserta. Apabila dianalisis menggunakan UU PDP, kasus tersebut menunjukkan adanya kegagalan dalam penerapan prinsip keamanan data (security principle). Pengendali data seharusnya menerapkan langkah teknis dan organisatoris yang memadai untuk melindungi data pribadi dari akses yang tidak sah. Fakta bahwa data dalam jumlah besar dapat diakses dan diperjualbelikan menunjukkan adanya kelemahan sistem pengamanan maupun tata kelola data. Dari perspektif teori Friedman, masalah utama dalam kasus ini bukan terletak pada substansi hukum, melainkan pada struktur hukum (legal structure) yang belum mampu melakukan pengawasan dan penegakan hukum secara efektif (Friedman, 1975). Ketiadaan lembaga pengawas independen menyebabkan proses investigasi dan pemberian sanksi berjalan lambat sehingga tidak menimbulkan efek jera yang signifikan.

2. Kasus Kebocoran Data Tokopedia

Kasus Tokopedia pada tahun 2020 yang melibatkan kebocoran data sekitar 91 juta pengguna dan 7 juta merchant menunjukkan bahwa sektor swasta juga menghadapi risiko serius dalam pengelolaan data pribadi (CNN Indonesia, 2020). Meskipun perusahaan menyatakan bahwa kata sandi pengguna telah dienkripsi, kebocoran data tetap berpotensi menimbulkan berbagai bentuk kejahatan siber seperti phishing, pencurian identitas, dan penipuan digital. Dalam perspektif UU PDP, perusahaan sebagai pengendali data memiliki tanggung jawab hukum untuk

memastikan keamanan data yang dikelolanya. Kebocoran data dalam jumlah besar menunjukkan bahwa penerapan prinsip akuntabilitas (accountability principle) belum berjalan optimal. Di samping itu, kasus Tokopedia memperlihatkan bahwa investasi keamanan siber di sektor swasta masih sering dipandang sebagai biaya operasional semata, bukan sebagai bagian dari kewajiban hukum yang harus dipenuhi. Dari sudut pandang efektivitas hukum, kasus ini mengindikasikan bahwa ancaman sanksi yang tersedia belum cukup mendorong kepatuhan maksimal dari para pelaku usaha digital. Dengan kata lain, fungsi preventif hukum masih belum berjalan secara efektif.

3. Kasus Kebocoran Data Dukcapil

Kebocoran data yang berkaitan dengan NIK dan Kartu Keluarga yang beredar di media sosial menunjukkan bahwa lembaga publik juga menghadapi tantangan besar dalam menjaga keamanan data warga negara (Kementerian Komunikasi dan Informatika Republik Indonesia, 2023). Padahal data kependudukan merupakan kategori data strategis yang memiliki tingkat sensitivitas tinggi. Kasus ini memperlihatkan adanya persoalan koordinasi antarlembaga dan lemahnya pengawasan terhadap akses data. Dalam perspektif efektivitas hukum, keberadaan regulasi yang baik tidak akan memberikan perlindungan optimal apabila tidak didukung oleh infrastruktur teknologi yang kuat dan mekanisme pengawasan yang berkelanjutan. Berikut penjelasan menurut European Unioan mengenai Perbandingan UU PDP Indonesia dan GDPR Uni Eropa ((European Union, 2016; Republik Indonesia, 2022).

Tabel 1. Perbandingan UU PDP Indonesia dan GDPR Uni Eropa

Persetujuan Subjek Data	Wajib, dapat ditarik kapan saja	Wajib, berbasis "explicit consent"	Belum ada sistem standar pencabutan izin data
Hak Subjek Data	Akses, koreksi, hapus, dan keberatan	Akses, koreksi, hapus ("right to be forgotten"), portabilitas data	Fasilitas masih terbatas di lembaga publik
Kewajiban Pengendali Data	Melindungi dan melaporkan kebocoran data	Melaporkan insiden dalam 72 jam	Di Indonesia belum ada batas waktu tegas pelaporan insiden
Cakupan Wilayah	Nasional, berlaku untuk entitas di Indonesia	Ekstrateritorial, mencakup semua pengolah data warga UE	UU PDP belum menjangkau entitas lintas negara secara penuh

Sumber: Diolah dari *UU No. 27 Tahun 2022* dan *GDPR 2016/679*.

Tabel di atas menunjukkan bahwa UU PDP Indonesia sudah mengadopsi sebagian prinsip GDPR, namun implementasinya masih lemah, terutama dalam aspek penegakan dan kesiapan infrastruktur.

C. Analisis Penegakan Hukum dan Kelembagaan

Salah satu indikator utama efektivitas hukum adalah kemampuan negara dalam menegakkan aturan melalui institusi yang memiliki kewenangan jelas dan legitimasi yang kuat. Dalam konteks Undang-Undang Perlindungan Data Pribadi (UU PDP), negara telah menyediakan kerangka normatif yang cukup komprehensif, termasuk pengaturan mengenai sanksi administratif dan pidana terhadap pelanggaran perlindungan data pribadi. UU PDP menetapkan ancaman pidana penjara hingga enam tahun serta denda maksimal Rp6 miliar terhadap pelanggaran perlindungan data pribadi

(Republik Indonesia, 2022). Secara teoritis, ketentuan tersebut diharapkan mampu memberikan efek jera (deterrent effect) bagi pelaku pelanggaran serta mendorong kepatuhan dari para pengendali dan pemroses data pribadi.

Namun demikian, dalam praktiknya efektivitas ancaman sanksi tersebut masih menjadi tanda tanya. Hingga saat ini, jumlah kasus kebocoran data pribadi yang benar-benar diproses hingga tahap penjatuhan sanksi pidana masih sangat terbatas. Banyak kasus kebocoran data yang hanya berhenti pada tahap klarifikasi atau penanganan administratif tanpa adanya tindak lanjut hukum yang tegas. Kondisi ini mencerminkan adanya kesenjangan antara law in books dan law in action, di mana hukum telah tersedia secara normatif tetapi belum diimplementasikan secara optimal dalam praktik. Kesenjangan ini tidak hanya berdampak pada rendahnya efek jera, tetapi juga berpotensi menurunkan tingkat kepercayaan masyarakat terhadap komitmen negara dalam melindungi data pribadi.

Salah satu faktor utama yang menyebabkan lemahnya penegakan hukum tersebut adalah belum optimalnya pembentukan lembaga pengawas independen sebagaimana diamanatkan dalam Pasal 58 UU PDP. Lembaga ini seharusnya berperan sebagai otoritas sentral yang memiliki kewenangan untuk melakukan pengawasan, penindakan, serta penjatuhan sanksi terhadap pelanggaran perlindungan data pribadi. Namun, keterlambatan dalam pembentukan dan operasionalisasi lembaga tersebut mengakibatkan terjadinya kekosongan otoritas yang berdampak langsung pada efektivitas penegakan hukum.

Akibat dari belum terbentuknya lembaga pengawas yang independen, fungsi pengawasan dan penegakan hukum saat ini masih tersebar pada berbagai institusi, seperti Kementerian Komunikasi dan Digital, Kepolisian, serta sejumlah lembaga sektoral lainnya. Fragmentasi kewenangan antarinstansi berpotensi menimbulkan berbagai permasalahan, antara lain tumpang tindih fungsi, ketidakjelasan koordinasi, serta lambatnya proses penanganan kasus (Kementerian Komunikasi dan Informatika Republik Indonesia, 2023). Selain itu, perbedaan standar operasional antarinstansi juga dapat menyebabkan inkonsistensi dalam penanganan kasus yang serupa.

Dalam perspektif teori sistem hukum yang dikemukakan oleh Lawrence M. Friedman, keberhasilan suatu sistem hukum sangat dipengaruhi oleh tiga unsur utama, yaitu legal structure, legal substance, dan legal culture (Friedman, 1975). Dalam konteks UU PDP, substansi hukum dapat dikatakan sudah relatif memadai karena telah mengatur secara rinci mengenai hak dan kewajiban serta sanksi bagi pelanggar. Namun, dari sisi struktur hukum, masih terdapat kelemahan yang signifikan, terutama terkait dengan belum optimalnya kelembagaan pengawas. Tanpa struktur kelembagaan yang kuat, substansi hukum yang baik tidak akan dapat diimplementasikan secara efektif.

Lebih lanjut, kelemahan dalam struktur hukum ini juga berimplikasi pada aspek budaya hukum masyarakat dan aparat penegak hukum. Ketika penegakan hukum tidak berjalan secara konsisten, maka akan terbentuk persepsi bahwa pelanggaran terhadap perlindungan data pribadi bukanlah pelanggaran yang serius.

Hal ini dapat menurunkan tingkat kepatuhan para pelaku usaha maupun institusi pemerintah dalam mengelola data pribadi. Selain itu, masyarakat sebagai subjek data juga menjadi kurang percaya terhadap mekanisme perlindungan hukum yang tersedia, sehingga enggan untuk melaporkan pelanggaran yang dialami.

Untuk mengatasi permasalahan tersebut, diperlukan langkah strategis yang berfokus pada penguatan aspek kelembagaan dan penegakan hukum.

1. Pemerintah harus segera merealisasikan pembentukan lembaga pengawas data pribadi yang independen, profesional, dan memiliki kewenangan yang jelas. Lembaga ini perlu dilengkapi dengan sumber daya manusia yang kompeten, infrastruktur yang memadai, serta mekanisme kerja yang transparan dan akuntabel.
2. Perlu dilakukan harmonisasi dan penguatan koordinasi antarinstansi yang terlibat dalam penegakan hukum perlindungan data pribadi. Pembagian kewenangan yang jelas serta mekanisme koordinasi yang efektif akan mengurangi potensi tumpang tindih dan meningkatkan efisiensi penanganan kasus. Ketiga, penegakan hukum harus dilakukan secara konsisten dan tegas untuk menciptakan efek jera serta meningkatkan kepatuhan.

Dengan demikian, dapat disimpulkan bahwa efektivitas penegakan hukum dalam UU PDP sangat bergantung pada kesiapan struktur kelembagaan yang mendukung. Tanpa adanya lembaga pengawas yang independen dan sistem penegakan hukum yang terintegrasi, maka ketentuan hukum yang telah disusun secara normatif tidak akan mampu memberikan perlindungan yang optimal terhadap data pribadi masyarakat.

D. Analisis Perbandingan UU PDP Indonesia dengan GDPR Uni Eropa

Jika dibandingkan dengan General Data Protection Regulation (GDPR) Uni Eropa, terdapat sejumlah perbedaan mendasar yang berimplikasi langsung terhadap tingkat efektivitas perlindungan data pribadi. GDPR sering dijadikan sebagai standar global dalam tata kelola perlindungan data karena tidak hanya kuat secara normatif, tetapi juga didukung oleh mekanisme implementasi dan pengawasan yang konsisten.

Dari aspek kelembagaan, GDPR didukung oleh keberadaan Data Protection Authority (DPA) di setiap negara anggota Uni Eropa yang berfungsi sebagai otoritas independen dalam mengawasi pelaksanaan perlindungan data. DPA memiliki kewenangan luas, mulai dari melakukan investigasi, memberikan sanksi administratif, hingga mengeluarkan pedoman teknis bagi pengendali data. Independensi lembaga ini menjadi faktor kunci dalam menjamin objektivitas dan konsistensi penegakan hukum. Sebaliknya, Indonesia hingga saat ini masih berada dalam tahap penguatan kelembagaan pengawas data pribadi sebagaimana diamanatkan dalam UU PDP (Republik Indonesia, 2022). Ketiadaan lembaga pengawas yang sepenuhnya independen menyebabkan fungsi pengawasan belum berjalan secara optimal dan masih tersebar di berbagai instansi, yang berpotensi menimbulkan tumpang tindih

kewenangan.

Dari sisi mekanisme respons terhadap insiden kebocoran data, GDPR menetapkan kewajiban pelaporan maksimal 72 jam sejak insiden diketahui. Ketentuan ini mendorong pengendali data untuk memiliki sistem deteksi dan respons insiden yang cepat dan terstruktur. Selain itu, kewajiban tersebut juga memberikan perlindungan yang lebih baik bagi subjek data karena memungkinkan tindakan mitigasi dilakukan sesegera mungkin, seperti pemberitahuan kepada pihak terdampak dan langkah pengamanan lanjutan. Sebaliknya, UU PDP di Indonesia belum mengatur batas waktu pelaporan yang seketat GDPR (European Union, 2016; Republik Indonesia, 2022). Akibatnya, dalam praktiknya, banyak kasus kebocoran data yang dilaporkan secara terlambat atau bahkan tidak dilaporkan secara transparan kepada publik, sehingga meningkatkan risiko kerugian bagi pemilik data.

Perbedaan signifikan juga terlihat pada aspek sanksi. GDPR menerapkan sanksi yang sangat tegas dan berskala besar, yakni dapat mencapai €20 juta atau sebesar 4% dari total pendapatan tahunan global perusahaan, tergantung mana yang lebih besar. Pendekatan ini menciptakan tekanan yang kuat bagi perusahaan, terutama korporasi multinasional, untuk mematuhi ketentuan perlindungan data. Dalam praktiknya, sejumlah perusahaan teknologi besar telah dikenakan denda dalam jumlah signifikan, yang menunjukkan bahwa penegakan hukum GDPR tidak hanya bersifat simbolis, tetapi benar-benar diterapkan secara konsisten. Sebaliknya, sanksi dalam UU PDP meskipun telah mengatur pidana dan denda, masih relatif terbatas jika dibandingkan dengan skala ekonomi perusahaan besar. Hal ini berpotensi mengurangi daya paksa hukum terhadap korporasi, terutama yang memiliki sumber daya finansial besar.

Selain tiga aspek tersebut, perbedaan lain juga dapat dilihat dari tingkat kematangan ekosistem perlindungan data. Uni Eropa telah memiliki budaya kepatuhan (compliance culture) yang lebih mapan, didukung oleh regulasi turunan yang rinci, pedoman teknis, serta praktik terbaik yang terus diperbarui. Sementara itu, Indonesia masih berada dalam tahap awal pembentukan ekosistem tersebut, sehingga membutuhkan waktu dan upaya berkelanjutan untuk mencapai tingkat kematangan yang serupa.

Sebagai ilustrasi, dalam kasus pelanggaran data di Uni Eropa, perusahaan diwajibkan tidak hanya melaporkan insiden dalam waktu 72 jam, tetapi juga menunjukkan langkah-langkah mitigasi yang telah dilakukan serta rencana perbaikan ke depan. Jika kewajiban ini tidak dipenuhi, DPA dapat langsung menjatuhkan sanksi administratif yang signifikan. Sebaliknya, dalam konteks Indonesia, mekanisme seperti ini belum sepenuhnya berjalan secara sistematis, sehingga respons terhadap pelanggaran sering kali bersifat reaktif dan kurang terkoordinasi.

Berdasarkan analisis perbandingan tersebut, dapat disimpulkan bahwa tantangan utama Indonesia dalam implementasi UU PDP bukan terletak pada kekurangan norma hukum, melainkan pada aspek implementasi, pengawasan, dan penegakan hukum. Oleh karena itu, langkah ke depan yang perlu dilakukan

adalah memperkuat kelembagaan pengawas yang independen, menetapkan standar operasional yang lebih tegas, serta meningkatkan kapasitas institusi dalam merespons dan menangani pelanggaran data secara cepat dan efektif. Dengan demikian, efektivitas perlindungan data pribadi di Indonesia dapat ditingkatkan secara signifikan dan mampu mendekati standar internasional seperti GDPR.

E. Tantangan dan Upaya Peningkatan Efektivitas UU PDP

Berdasarkan hasil analisis, terdapat empat tantangan utama dalam implementasi Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia.

1. Rendahnya kesiapan infrastruktur keamanan siber di berbagai lembaga, baik pemerintah maupun swasta. Banyak institusi masih belum memiliki sistem keamanan yang memadai, seperti enkripsi data yang kuat, sistem deteksi intrusi, serta prosedur manajemen risiko yang terstandarisasi. Kondisi ini meningkatkan kerentanan terhadap kebocoran dan penyalahgunaan data pribadi.
2. Rendahnya tingkat literasi digital masyarakat terkait hak-hak atas data pribadi. Sebagian besar masyarakat belum sepenuhnya memahami pentingnya perlindungan data pribadi, termasuk bagaimana data mereka dikumpulkan, digunakan, dan dilindungi. Minimnya kesadaran ini menyebabkan masyarakat cenderung tidak kritis dalam memberikan data pribadi kepada berbagai platform digital, sehingga meningkatkan risiko eksploitasi data.
3. Belum optimalnya kelembagaan pengawas data pribadi. Meskipun UU PDP telah mengamanatkan pembentukan lembaga pengawas yang independen, hingga saat ini efektivitas kelembagaan tersebut masih menghadapi berbagai kendala, seperti keterbatasan sumber daya manusia, kewenangan yang belum sepenuhnya terimplementasi, serta koordinasi yang belum solid dengan lembaga lain. Hal ini berdampak pada lemahnya fungsi pengawasan dan penegakan regulasi.
4. Lemahnya konsistensi penegakan hukum terhadap pelanggaran perlindungan data pribadi. Penegakan hukum yang belum tegas dan konsisten menyebabkan efek jera bagi pelanggar menjadi rendah. Selain itu, proses penanganan kasus kebocoran data sering kali berjalan lambat dan kurang transparan, sehingga menurunkan kepercayaan publik terhadap sistem perlindungan data yang ada.

Untuk meningkatkan efektivitas UU PDP, diperlukan sejumlah langkah strategis yang bersifat komprehensif dan berkelanjutan.

1. Pemerintah perlu mempercepat pembentukan serta operasionalisasi lembaga pengawas data pribadi yang benar-benar independen dan profesional. Lembaga ini harus memiliki kewenangan yang jelas, sumber daya yang memadai, serta mampu menjalankan fungsi pengawasan dan penegakan hukum

secara efektif.

2. Peningkatan standar keamanan siber nasional harus menjadi prioritas. Hal ini dapat dilakukan melalui penerapan kewajiban audit keamanan data secara berkala, sertifikasi sistem keamanan informasi, serta penerapan standar internasional seperti ISO/IEC 27001. Dengan demikian, setiap organisasi memiliki baseline keamanan yang jelas dan terukur.
3. Diperlukan penguatan koordinasi antarinstansi penegak hukum, seperti kepolisian, kejaksaan, dan lembaga pengawas. Sinergi ini penting untuk memastikan penanganan kasus pelanggaran data dapat dilakukan secara cepat, tepat, dan terintegrasi.
4. Peningkatan literasi digital masyarakat harus dilakukan melalui program edukasi yang sistematis dan berkelanjutan. Pemerintah, lembaga pendidikan, serta sektor swasta perlu berkolaborasi dalam memberikan pemahaman kepada masyarakat mengenai pentingnya perlindungan data pribadi dan cara menjaga keamanan data.
5. Penerapan mekanisme pelaporan insiden kebocoran data yang cepat, transparan, dan akuntabel juga sangat penting. Setiap organisasi wajib melaporkan insiden kebocoran dalam jangka waktu tertentu, serta memberikan informasi yang jelas kepada pihak yang terdampak.

D. Simpulan

Secara normatif UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah membentuk kerangka hukum yang relatif komprehensif dan mengadopsi sejumlah prinsip utama perlindungan data internasional, namun efektivitasnya dalam menangani kebocoran data di Indonesia masih rendah karena terhambat oleh kekosongan dan kelemahan aturan pelaksana, belum optimalnya pembentukan dan kinerja lembaga pengawas independen, keterbatasan infrastruktur keamanan siber, serta rendahnya literasi dan budaya hukum masyarakat terkait perlindungan data pribadi. Melalui analisis teori efektivitas hukum Soerjono Soekanto dan kerangka sistem hukum Lawrence M. Friedman, tampak jelas bahwa persoalan utama bukan lagi pada substansi UU PDP, melainkan pada aspek struktur hukum, sarana pendukung, dan budaya hukum yang belum memadai, sehingga diperlukan langkah penguatan kelembagaan, pengetatan mekanisme penegakan dan sanksi, peningkatan standar keamanan siber, serta edukasi publik yang berkelanjutan agar tujuan perlindungan hak privasi dan pencegahan kebocoran data dapat tercapai secara lebih efektif.

DAFTAR PUSTAKA

Algamar, M. D. (2024). Managing Indonesian data breach notification. JCLI.

CNN Indonesia. (2020, 3 Mei). Kebocoran data Tokopedia. CNN Indonesia.

Danrivanto, B. (2024). Hukum pelindungan data pribadi dan data nasional. ResearchGate.

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons

with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation/GDPR). Official Journal of the European Union.

ELSAM. (2019). Perlindungan data pribadi: Konsep, instrumen, dan prinsipnya. ELSAM.

ELSAM. (2024). Riset perlindungan data pribadi di Indonesia. ELSAM.

Friedman, L. M. (1975). The legal system: A social science perspective. Russell Sage Foundation.

Kementerian Komunikasi dan Informatika Republik Indonesia. (2023). Laporan insiden keamanan data nasional. Kementerian Komunikasi dan Informatika Republik Indonesia.

Mumtaz, fajrul. (2025). Kekuatan Pembuktian Perjanjian Elektronik Dalam Sengketa Utang Piutang Di Era Digitalisasi. *HUNILA : Jurnal Ilmu Hukum Dan Integrasi Peradilan*, *4*(1), 14–28. https://doi.org/10.53491/hunila.v4i1.1873

Prasetyo, T., & Karo-Karo, R. P. P. (2021). Pengaturan perlindungan data pribadi di Indonesia: Perspektif teori keadilan bermartabat. Bintang Pusnas.

Republik Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 208.

Sari, H. P. (2024). Efektivitas hukum perlindungan data pribadi. Jurnal Media Akademik.

Simbolon, V. A. (2022). Comparative review: Gap analysis of data protection regulations. Semantic Scholar.

Soekanto, S. (2008). Faktor-faktor yang mempengaruhi penegakan hukum. RajaGrafindo Persada.

Suherman, H. A. (2025). Relevansi Teori Hukum Pembangunan Dan Teori Hukum Progresif Dalam Pembentukan Teori Hukum Pancasila. *HUNILA : Jurnal Ilmu Hukum Dan Integrasi Peradilan*, *4*(1), 1–13. https://doi.org/10.53491/hunila.v4i1.1703

Tempo. (2021, 21 Mei). Kasus kebocoran data BPJS Kesehatan. Tempo.

Utami, T. K., dkk. (2025). Personal data breach cases in Indonesia: Perspective of personal data protection law. PubMedia Journal Series.