



DOI: <https://doi.org/10.38035/jsmd.v4i2>  
<https://creativecommons.org/licenses/by/4.0/>

## Efektivitas Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Dan Kebocoran Data Pribadi

Yoga Suherman<sup>1</sup>, Ratu Mawar Kartina<sup>2</sup>.

<sup>1</sup>Universitas Swadaya Gunung Jati, Cirebon, Indonesia, [yogasuherman1933@gmail.com](mailto:yogasuherman1933@gmail.com)

<sup>2</sup>Universitas Swadaya Gunung Jati, Cirebon, Indonesia, [ratumawar86@gmail.com](mailto:ratumawar86@gmail.com)

Corresponding Author: [ratumawar86@gmail.com](mailto:ratumawar86@gmail.com)<sup>2</sup>

**Abstract:** *The rapid development of information technology has significantly transformed how people communicate, conduct transactions, and access digital services. Along with these developments, incidents of personal data breaches have become increasingly common, raising concerns about the protection of personal data in Indonesia. In response to this issue, the Government enacted Law Number 27 of 2022 concerning Personal Data Protection as a legal framework aimed at safeguarding personal data and providing legal certainty for data subjects. This study aims to examine the effectiveness of Law Number 27 of 2022 concerning Personal Data Protection in addressing personal data breach cases and to identify the juridical and non-juridical obstacles affecting the implementation of personal data protection in Indonesia. The research employs an empirical juridical method using a statutory approach and field research through data collection from law enforcement officials. The results indicate that Law Number 27 of 2022 has provided a clearer and more comprehensive legal basis for personal data protection. However, its implementation has not yet been fully effective due to several factors, including limited institutional supervision, insufficient human resources with expertise in cybercrime investigation, and low public awareness regarding the importance of protecting personal data. Furthermore, the implementation of personal data protection is hindered by juridical obstacles, particularly the overlap between the Personal Data Protection Law and the Electronic Information and Transactions Law, which may create uncertainty in law enforcement. Non-juridical obstacles include limited digital forensic facilities, inadequate technological infrastructure, and low levels of digital literacy among the public. Therefore, strengthening institutional capacity, improving the competence of law enforcement officers, and harmonizing relevant regulations are necessary to enhance the effectiveness of personal data protection in Indonesia.*

**Keywords:** *Personal Data Protection, Personal Data Breach, Personal Data Protection Law, Electronic Information and Transactions Law.*

**Abstrak:** Perkembangan teknologi informasi telah membawa perubahan besar dalam kehidupan masyarakat, termasuk dalam penggunaan data pribadi pada berbagai layanan digital. Di sisi lain, meningkatnya kasus kebocoran data pribadi menunjukkan bahwa perlindungan terhadap data pribadi masih menjadi persoalan penting di Indonesia. Kondisi tersebut mendorong lahirnya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi sebagai dasar hukum dalam memberikan perlindungan terhadap data pribadi masyarakat.

Penelitian ini bertujuan untuk mengetahui efektivitas pengaturan dan penegakan hukum Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dalam menanggulangi kasus kebocoran data pribadi serta untuk mengetahui kendala yuridis dan non-yuridis yang mempengaruhi perlindungan data pribadi di Indonesia. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan dan pendekatan lapangan melalui pengumpulan data dari aparat penegak hukum. Hasil penelitian menunjukkan bahwa Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi belum efektif dalam memberikan pelindungan hukum terhadap data pribadi masyarakat Indonesia. Ketidakefektifan tersebut tercermin dari masih tingginya frekuensi kebocoran data pribadi setelah undang-undang tersebut diberlakukan, belum optimalnya pelaksanaan kewajiban oleh pengendali data pribadi, lemahnya pengawasan, serta belum maksimalnya penegakan hukum terhadap pelanggaran yang terjadi. Kondisi tersebut menunjukkan bahwa tujuan pembentukan Undang-Undang Nomor 27 Tahun 2022 untuk menjamin keamanan, kepastian hukum, dan perlindungan hak subjek data belum tercapai secara optimal.

**Kata Kunci:** Pelindungan Data Pribadi, Kebocoran Data Pribadi, UU PDP, UU ITE.

---

## PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan struktural yang mendalam dalam kehidupan sosial, ekonomi, dan hukum di Indonesia. Digitalisasi yang semakin masif telah menggeser pola interaksi masyarakat dari ruang fisik ke ruang virtual, sehingga berbagai aktivitas kehidupan mulai dari pelayanan publik, transaksi ekonomi, hingga ekspresi sosial sangat bergantung pada sistem elektronik. Dalam konteks ini, data pribadi menjadi elemen fundamental yang tidak terpisahkan dari setiap aktivitas digital, karena hampir seluruh layanan berbasis teknologi mensyaratkan individu untuk membagikan data dirinya, baik berupa identitas dasar seperti nama, alamat, dan nomor identitas, maupun data yang bersifat sensitif seperti informasi keuangan, biometrik, dan preferensi personal.

Pengumpulan, pemrosesan, dan penyimpanan data pribadi dilakukan secara masif oleh berbagai pihak, baik oleh negara melalui penyelenggaraan sistem pemerintahan berbasis elektronik, maupun oleh sektor swasta melalui platform digital, aplikasi komersial, layanan keuangan digital, dan media sosial. Ketergantungan masyarakat terhadap layanan-layanan tersebut secara tidak langsung menempatkan individu pada posisi yang rentan, karena relasi antara pemilik data dan pengendali data sering kali bersifat timpang. Dalam banyak kasus, subjek data tidak memiliki pilihan selain menyetujui kebijakan pengelolaan data yang kompleks dan tidak transparan, sehingga membuka peluang terjadinya praktik pengumpulan data yang berlebihan, penggunaan data tanpa persetujuan yang sah, serta penyebarluasan data pribadi kepada pihak ketiga tanpa sepengetahuan pemiliknya.

Kerentanan tersebut semakin diperparah oleh meningkatnya ancaman keamanan siber di Indonesia. Laporan Badan Siber dan Sandi Negara (BSSN) menunjukkan adanya peningkatan signifikan insiden serangan siber dan anomali trafik sepanjang tahun 2023, yang mencakup kebocoran data, peretasan sistem elektronik, serta penyalahgunaan akses terhadap basis data digital. Fenomena ini mencerminkan bahwa ancaman terhadap privasi data pribadi tidak lagi bersifat sporadis, melainkan telah menjadi persoalan sistemik yang mengikuti ekspansi ruang digital itu sendiri. Kebocoran data dalam skala besar tidak hanya menimbulkan kerugian material bagi individu, tetapi juga berdampak pada menurunnya kepercayaan publik terhadap penyelenggara sistem elektronik, baik negara maupun swasta.

Hak atas privasi merupakan bagian dari hak asasi manusia yang melekat pada setiap individu. Westin (1967) memperkenalkan pemahaman bahwa privasi berkaitan dengan kemampuan seseorang mengendalikan informasi mengenai dirinya, sedangkan Donnelly (2013) menempatkan privasi sebagai salah satu elemen penting dari martabat manusia. Prinsip

ini telah diterima dalam konteks global dan sejalan dengan jaminan yang terdapat dalam Pasal 28G ayat (1) UUD 1945. Kedudukan privasi sebagai hak fundamental menegaskan bahwa negara memiliki kewajiban untuk memastikan perlindungan hukum yang memadai terhadap seluruh aktivitas pemrosesan data pribadi, terutama dalam konteks digital yang berisiko tinggi. Kewajiban tersebut tidak hanya terkait penyediaan regulasi, tetapi juga kualitas norma, kepastian hukum, dan efektivitas penegakan hukum yang melindungi warga negara.

Instrumen hukum utama yang mengatur aktivitas elektronik di Indonesia adalah Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Sejak awal pembentukannya, UU ini dirancang untuk memberikan pengaturan komprehensif mengenai informasi elektronik, transaksi elektronik, dan berbagai perbuatan yang memiliki konsekuensi hukum di ruang digital. Perubahan melalui UU No. 1 Tahun 2024 dilakukan untuk memperbaiki kelemahan sebelumnya, termasuk aspek penyalahgunaan data dan distribusi informasi tanpa hak. Walaupun demikian, sejumlah ketentuan masih menimbulkan persoalan interpretasi, terutama mengenai batasan penggunaan data pribadi “tanpa hak” serta ruang lingkup perbuatan yang dapat dikategorikan sebagai pelanggaran privasi. Ketidaktepatan rumusan membawa implikasi serius karena berdampak pada ketidakpastian hukum bagi masyarakat dan aparat penegak hukum.

Keterbatasan pengaturan tersebut berkaitan erat dengan teori perlindungan hukum. Hadjon (1987) menekankan bahwa perlindungan hukum terhadap warga negara hanya dapat diwujudkan apabila norma hukum dirancang dengan jelas, pasti, dan dapat dilaksanakan. Prinsip *rule of law* juga menuntut agar setiap norma hukum memiliki kepastian sehingga dapat diprediksi penerapannya secara konsisten (Raz, 1979). Ketika rumusan dalam UU ITE tidak memberikan batas yang tegas mengenai perbuatan yang dianggap melanggar privasi, maka muncul persoalan dalam proses penegakan hukum. Situasi ini memunculkan risiko ketidakseragaman penafsiran, ketidakefektifan pembuktian, serta potensi penyalahgunaan pasal yang dapat berdampak pada perlindungan hak masyarakat.

Upaya negara untuk menghadirkan UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) menunjukkan penguatan regulatif yang signifikan. Walaupun demikian, keberadaan dua instrumen hukum yang mengatur aspek data pribadi memerlukan harmonisasi agar tidak menimbulkan tumpang tindih atau kekosongan norma dalam kasus-kasus tertentu yang terjadi di ruang elektronik. Ketidaksinkronan antara UU PDP dan UU ITE dapat menyebabkan hambatan dalam penegakan hukum, terutama dalam menentukan perbuatan yang sepenuhnya berada dalam cakupan UU ITE atau merupakan bagian dari rezim UU PDP. Situasi ini memperlihatkan perlunya peninjauan yuridis terhadap pengaturan privasi dalam UU ITE agar tercipta koherensi regulatif yang melindungi masyarakat secara efektif.

Dinamika ini menunjukkan adanya kebutuhan untuk menilai kembali secara kritis sejauh mana UU ITE mampu memberikan perlindungan yang efektif terhadap data pribadi di tengah berkembangnya ancaman digital, sekaligus mengidentifikasi kendala dan tantangan dalam implementasinya. Analisis yuridis diperlukan untuk memahami efektivitas pengaturan UU ITE dalam mencegah pelanggaran privasi dan bagaimana praktik penegakan hukum di Indonesia menanggapi kasus-kasus tersebut. Kajian ini berangkat dari pertanyaan mengenai sejauh mana UU ITE efektif dalam melindungi data pribadi serta mencegah terjadinya pelanggaran privasi, dan pertanyaan mengenai kendala serta tantangan apa yang muncul dalam implementasinya terkait perlindungan data pribadi di Indonesia.

## METODE

Penelitian ini menggunakan metode penelitian hukum normatif (*doctrinal legal research*) dengan menempatkan hukum sebagai suatu sistem norma yang dianalisis melalui peraturan perundang-undangan, asas hukum, doktrin, serta putusan pengadilan yang berkaitan dengan perlindungan data pribadi. Pendekatan ini dipilih karena penelitian berfokus pada pengkajian norma hukum yang mengatur penegakan hukum terhadap kebocoran data pribadi di Indonesia,

tanpa melakukan pengumpulan data empiris melalui survei, wawancara, maupun observasi lapangan. Analisis diarahkan untuk menilai kesesuaian, konsistensi, dan efektivitas pengaturan hukum dalam memberikan perlindungan terhadap hak atas privasi sebagai bagian dari hak konstitusional warga negara.

Penelitian ini menggunakan tiga pendekatan, yaitu pendekatan perundang-undangan (statute approach), pendekatan konseptual (conceptual approach), dan pendekatan analitis (analytical approach). Pendekatan perundang-undangan dilakukan dengan menelaah berbagai peraturan yang menjadi dasar hukum perlindungan data pribadi, meliputi Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta peraturan pelaksana dan regulasi sektoral yang berkaitan dengan penyelenggaraan sistem elektronik dan keamanan siber. Pendekatan konseptual digunakan untuk mengkaji konsep-konsep fundamental, seperti hak atas privasi (right to privacy), perlindungan data pribadi, kedaulatan data (data sovereignty), pertanggungjawaban pengendali data, dan teori perlindungan hukum berdasarkan doktrin para ahli. Selanjutnya, pendekatan analitis digunakan untuk mengkaji hubungan antarnorma hukum, mengidentifikasi potensi konflik, tumpang tindih, kekaburan, maupun kekosongan norma antara rezim hukum dalam Undang-Undang Informasi dan Transaksi Elektronik dan Undang-Undang Pelindungan Data Pribadi dalam penanganan kasus kebocoran data pribadi.

Sifat penelitian ini adalah deskriptif-analitis. Aspek deskriptif bertujuan menggambarkan secara sistematis pengaturan hukum mengenai perlindungan data pribadi di Indonesia, termasuk ketentuan mengenai hak subjek data, kewajiban pengendali data, bentuk pelanggaran, mekanisme pengawasan, serta sanksi pidana maupun administratif. Selanjutnya, aspek analitis dilakukan dengan mengkaji kualitas pengaturan tersebut berdasarkan teori perlindungan hukum dan prinsip rule of law untuk menilai tingkat kepastian hukum, konsistensi pengaturan, serta efektivitas norma dalam memberikan perlindungan hukum terhadap korban kebocoran data pribadi.

Bahan hukum yang digunakan terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer meliputi Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, peraturan pelaksana, regulasi sektoral yang berkaitan dengan keamanan siber dan penyelenggaraan sistem elektronik, serta putusan pengadilan yang relevan. Bahan hukum sekunder terdiri atas buku-buku hukum, artikel ilmiah, jurnal nasional maupun internasional, hasil penelitian, doktrin para ahli, laporan lembaga pemerintah, serta publikasi akademik yang berkaitan dengan perlindungan data pribadi dan penegakan hukum siber. Adapun bahan hukum tersier meliputi Kamus Besar Bahasa Indonesia (KBBI), kamus hukum, ensiklopedia hukum, serta basis data dan situs resmi pemerintah yang digunakan untuk mendukung penafsiran istilah hukum dan memastikan keakuratan informasi.

Pengumpulan bahan hukum dilakukan melalui studi kepustakaan (library research) dengan menelusuri berbagai sumber hukum dan literatur yang relevan melalui perpustakaan, pangkalan data jurnal ilmiah, repositori akademik, serta situs resmi pemerintah. Seluruh bahan hukum yang diperoleh selanjutnya diinventarisasi, diklasifikasikan berdasarkan jenis dan hierarki peraturan, kemudian diverifikasi untuk memastikan keabsahan, relevansi, dan aktualitasnya sesuai dengan fokus penelitian.

Analisis bahan hukum dilakukan secara kualitatif normatif melalui beberapa tahapan. Tahap pertama adalah inventarisasi dan identifikasi ketentuan hukum yang mengatur perlindungan data pribadi dalam berbagai peraturan perundang-undangan. Tahap kedua dilakukan penafsiran hukum menggunakan metode penafsiran gramatikal untuk memahami

makna norma berdasarkan rumusan bahasa peraturan serta penafsiran sistematis untuk menilai hubungan antarperaturan dalam satu sistem hukum nasional. Tahap ketiga berupa analisis komparatif antarnorma guna mengidentifikasi potensi disharmoni, tumpang tindih kewenangan, maupun kekosongan hukum antara Undang-Undang Informasi dan Transaksi Elektronik dan Undang-Undang Pelindungan Data Pribadi. Tahap terakhir dilakukan evaluasi terhadap hasil analisis dengan menggunakan teori perlindungan hukum dan prinsip rule of law untuk menilai efektivitas pengaturan hukum dalam memberikan kepastian hukum, perlindungan terhadap hak privasi, serta optimalisasi penegakan hukum atas kasus kebocoran data pribadi di Indonesia.

## **HASIL DAN PEMBAHASAN**

### **1. Efektivitas Pengaturan dan Penegakan Hukum Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dalam Menanggulangi Kasus Kebocoran Data Pribadi**

Efektivitas sebuah undang-undang dinilai dari kemampuannya mencapai tujuan sosiologis dan yuridis yang dikehendaki oleh pembentuk undang-undang. Kehadiran Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) dirancang sebagai kodifikasi hukum induk (*lex specialis*) untuk mengatasi kekosongan regulasi yang komprehensif. Aturan ini dibentuk untuk merespons maraknya insiden kebocoran data pribadi yang mengancam hak privasi warga negara. Penilaian terhadap efektivitas UU PDP dalam menanggulangi kebocoran data di ruang digital Indonesia harus ditinjau melalui dua dimensi utama. Dimensi tersebut meliputi efektivitas substansi pengaturan (kualitas norma) dan efektivitas penegakan hukum dalam praktik yudisial.

Salah satu indikator empiris yang menunjukkan belum efektifnya implementasi Undang-Undang Nomor 27 Tahun 2022 adalah serangan ransomware terhadap Pusat Data Nasional Sementara (PDNS) pada Juni 2024. Insiden tersebut terjadi ketika sistem PDNS mengalami serangan ransomware Brain Cipher yang mengakibatkan terganggunya berbagai layanan publik nasional, termasuk layanan Direktorat Jenderal Imigrasi, pelayanan keimigrasian di bandara, serta layanan kementerian dan lembaga yang bergantung pada PDNS. Berdasarkan hasil investigasi Badan Siber dan Sandi Negara (BSSN), aktivitas berbahaya telah dimulai sejak 17 Juni 2024 melalui penonaktifan fitur keamanan sistem, kemudian berkembang menjadi serangan ransomware yang mengenkripsi data sehingga sistem tidak dapat beroperasi secara normal.

Insiden tersebut menunjukkan bahwa setelah hampir dua tahun Undang-Undang Nomor 27 Tahun 2022 diberlakukan, masih terjadi gangguan serius terhadap sistem elektronik pemerintah yang menyimpan dan mengelola data masyarakat. Pemerintah melalui Kementerian Komunikasi dan Informatika (sekarang Kementerian Komunikasi dan Digital), BSSN, Kepolisian Negara Republik Indonesia, dan Telkom Sigma kemudian melakukan isolasi sistem, investigasi digital forensik, serta membangun server pengganti guna memulihkan layanan publik. Kasus PDNS tersebut menunjukkan bahwa keberadaan Undang-Undang Nomor 27 Tahun 2022 belum mampu menjamin terlaksananya pelindungan data pribadi secara efektif. Secara normatif, undang-undang telah mengatur kewajiban pengendali data untuk menjaga keamanan data pribadi, menerapkan sistem pelindungan data yang memadai, serta melakukan pemberitahuan apabila terjadi kegagalan pelindungan data. Akan tetapi, dalam praktik masih terjadi gangguan keamanan siber yang berdampak luas terhadap penyelenggaraan pelayanan publik.

Menurut teori efektivitas hukum Soerjono Soekanto, efektivitas hukum dipengaruhi oleh lima faktor, yaitu substansi hukum, aparat penegak hukum, sarana atau fasilitas, masyarakat, dan budaya hukum. Berdasarkan teori tersebut, penelitian ini menemukan bahwa kelima faktor tersebut belum berjalan secara optimal. Secara substansi pengaturan, UU PDP memiliki



keunggulan normatif yang jauh lebih progresif dibandingkan dengan regulasi siber terdahulu seperti UU ITE. UU PDP mengadopsi prinsip akuntabilitas mutlak (strict accountability).

Prinsip ini membebaskan tanggung jawab besar kepada pengendali data pribadi, baik korporasi swasta maupun instansi publik. Instrumen pencegahan kebocoran data diatur secara tegas dalam Pasal 46 UU PDP. Pasal tersebut mewajibkan pengendali data untuk menyampaikan pemberitahuan tertulis dalam waktu 72 jam kepada subjek data pribadi dan lembaga pengawas jika terjadi kegagalan perlindungan data. Kewajiban ini memberikan kepastian hukum yang jelas mengenai langkah mitigasi pertama saat kebocoran data terjadi. Formulasi sanksi administratif berupa denda maksimal hingga 2% dari pendapatan tahunan terhadap total pendapatan variabel pelanggar, serta sanksi pidana denda hingga miliaran rupiah, secara teoritis memiliki daya jera (deterrent effect) yang kuat untuk memaksa penyelenggara sistem elektronik meningkatkan keandalan sistem keamanan siber mereka.

Meskipun UU PDP telah mengatur kewajiban pengendali data untuk menjaga kerahasiaan dan keamanan data pribadi, dalam praktiknya masih ditemukan berbagai kelemahan, baik dari aspek pengawasan, sistem keamanan informasi, maupun mekanisme pertanggungjawaban apabila terjadi kebocoran data. Kondisi ini memperlihatkan adanya kesenjangan antara pengaturan hukum yang telah tersedia dengan implementasinya di lapangan.

Kelemahan substansial dalam penegakan hukum UU PDP terletak pada ketergantungan yang tinggi terhadap pembentukan lembaga pengawas atau Otoritas Pelindungan Data Pribadi (DPA). Berdasarkan amanat Pasal 58 hingga Pasal 60 UU PDP, lembaga ini memiliki peran sentral sebagai eksekutor sanksi administratif, pengawas kepatuhan pengendali data, serta investigator utama dalam kasus kebocoran data berskala besar. Realitas penegakan hukum menunjukkan bahwa keterlambatan pembentukan institusi pengawas independen ini memicu terjadinya stagnasi penegakan hukum di lapangan. Tanpa adanya otoritas tunggal yang kuat, penanganan kasus kebocoran data masih terjebak dalam ego sektoral antar-lembaga, seperti Kementerian Komunikasi dan Digital serta Badan Siber dan Sandi Negara (BSSN). Kondisi ini menyebabkan sanksi denda administratif yang progresif dalam UU PDP belum dapat diimplementasikan secara optimal terhadap pengendali data yang lalai.

Tantangan efektivitas penegakan hukum diperparah oleh kendala teknis pembuktian dan ketimpangan kedudukan antara subjek data dengan pengendali data. Hasil wawancara dengan pihak Polres Cirebon Kota menunjukkan bahwa penanganan perkara yang menjadi objek penelitian dilakukan melalui penerimaan laporan masyarakat, pengumpulan keterangan, pengamanan alat bukti, serta penyelidikan awal oleh penyidik. Penanganan pada tingkat Polres memiliki keterbatasan kewenangan sehingga proses lanjutan dan data perkara secara komprehensif berada pada Kepolisian Daerah Jawa Barat. Keadaan tersebut menyebabkan sebagian besar perkembangan perkara hanya dapat diperoleh melalui instansi yang memiliki kewenangan lebih luas dalam proses penyidikan. Kedudukan Polres dalam penegakan hukum berfungsi sebagai institusi yang melakukan tindakan awal untuk memastikan adanya peristiwa yang diduga sebagai tindak pidana. Pengumpulan informasi dan alat bukti menjadi dasar bagi proses penyidikan yang dilakukan pada tingkat berikutnya. Pola penanganan yang bersifat berjenjang menunjukkan adanya pembagian kewenangan dalam sistem kepolisian guna mendukung proses penegakan hukum sesuai dengan tingkat kompleksitas perkara. Keterangan narasumber menunjukkan adanya hambatan berupa keterbatasan sarana dan prasarana pendukung penegakan hukum. Ketersediaan fasilitas yang belum memadai berdampak pada proses penelusuran, pengumpulan bukti, identifikasi pelaku, serta pengembangan perkara. Dukungan teknologi, perangkat operasional, dan sumber daya pendukung memiliki peran penting dalam menentukan kualitas penanganan perkara sejak tahap awal.

Efektivitas penegakan hukum pada tingkat Polres Cirebon Kota dinilai belum optimal. Penilaian tersebut didasarkan pada masih adanya ketergantungan terhadap proses pelimpahan perkara kepada Polda Jawa Barat. Penyelesaian perkara tidak sepenuhnya dapat dilakukan

pada tingkat Polres karena kewenangan dan kapasitas penanganan berada pada tingkat yang lebih tinggi. Kondisi tersebut menunjukkan bahwa keberhasilan penegakan hukum ditentukan oleh kemampuan institusi dalam menjalankan fungsi penanganan perkara secara menyeluruh, dukungan sarana dan prasarana yang memadai, serta keterpaduan proses penegakan hukum pada setiap tingkatan kelembagaan kepolisian.

Penegakan hukum pidana UU PDP dalam kasus kebocoran data menuntut kemampuan forensik siber yang sangat tinggi dari aparat penegak hukum untuk membuktikan unsur kelalaian atau kesengajaan. Korban kebocoran data acapkali kesulitan menuntut ganti rugi karena beban pembuktian kerugian materiil dan immateriil di persidangan sangat rumit. Penerapan sanksi pidana dalam UU PDP juga seringkali hanya menyasar pelaku peretasan tingkat bawah (hacker). Institusi besar yang gagal menjaga keamanan basis datanya luput dari pertanggungjawaban hukum yang setimpal. Hambatan-hambatan yuridis dan kelembagaan ini menunjukkan bahwa UU PDP belum berjalan secara efektif penuh di Indonesia. Regulasi ini masih berada pada tahap transisi normatif yang membutuhkan penguatan kelembagaan serta penegakan sanksi yang konsisten demi menjamin hak privasi masyarakat di ruang digital secara utuh.

Analisis efektivitas hukum ini sejalan dengan teori Lawrence M. Friedman yang menyatakan keberhasilan penegakan hukum bergantung pada struktur hukum, substansi hukum, dan budaya hukum. Dari aspek substansi, UU PDP sebenarnya telah mengadopsi standar global seperti General Data Protection Regulation (GDPR) milik Uni Eropa. Norma-norma penentuan jenis data pribadi spesifik dan umum memberikan kejelasan kategorisasi hukum dalam proses adjudikasi. Keandalan substansi ini tidak diimbangi oleh kesiapan struktur hukum yang bertugas mengeksekusi undang-undang di lapangan. Aparat penegak hukum di tingkat operasional masih sering menggunakan pola pikir konvensional yang menyamakan kasus kebocoran data dengan tindak pidana pencurian biasa.

Ketimpangan pemahaman struktural ini berdampak langsung pada lambatnya respons penindakan terhadap korporasi yang mengalami kegagalan sistem siber. Banyak institusi publik dan swasta yang terkesan menutup-nutupi insiden kebocoran data demi menjaga reputasi pasar maupun legitimasi politik mereka. Kewajiban melapor 72 jam yang tertuang dalam undang-undang sering kali diabaikan tanpa ada konsekuensi hukum yang tegas dan instan dari pemerintah. Ketidaktegasan struktur hukum ini memperlihatkan adanya kompromi politik-hukum yang mengorbankan hak-hak konstitusional warga negara sebagai pemilik data yang sah. Penegakan hukum siber pada akhirnya bersifat tebang pilih dan hanya tajam pada kasus-kasus yang menjadi perhatian publik di media sosial.

Di sisi lain, budaya hukum masyarakat Indonesia masih menunjukkan tingkat kesadaran privasi data (privacy awareness) yang sangat rendah. Mayoritas pengguna ruang digital secara sukarela menyerahkan data sensitif mereka kepada aplikasi pihak ketiga tanpa membaca syarat ketentuan yang berlaku. Kebiasaan ini menciptakan pemakluman sosial terhadap pelanggaran privasi, sehingga mengaburkan urgensi penegakan UU PDP itu sendiri. Masyarakat cenderung baru bersuara ketika kebocoran data telah menimbulkan kerugian finansial riil seperti penipuan berbasis rekayasa sosial atau jeratan pinjaman online ilegal. Budaya hukum yang permisif ini menjadi hambatan sosiologis eksternal yang memperlemah daya ikat operasional dari undang-undang perlindungan data.

Problematika yurisdiksi juga membayangi efektivitas penegakan UU PDP dalam menanggulangi kebocoran data yang bersifat lintas batas negara (cross-border data flow). Sebagian besar pelaku peretasan tingkat tinggi beroperasi dari luar wilayah hukum Indonesia dan memanfaatkan jaringan terenkripsi yang sulit dilacak. Mekanisme ekstradisi dan kerja sama hukum timbal balik (mutual legal assistance) dalam penegakan hukum siber internasional membutuhkan waktu birokrasi yang sangat lama. Keterbatasan jangkauan yurisdiksi domestik ini menyebabkan kepastian hukum yang ditawarkan oleh UU PDP sering kali berhenti di

perbatasan teritorial negara. Regulasi ini menjadi tidak berdaya ketika berhadapan dengan aktor kejahatan internasional yang memanfaatkan kelemahan infrastruktur digital nasional.

Penerapan sanksi denda administratif dalam UU PDP juga menghadapi tantangan besar terkait standarisasi audit keamanan informasi. Pemerintah belum menetapkan parameter baku yang adil untuk menentukan kapan sebuah instansi dinilai telah melakukan "upaya maksimal" atau "kelalaian berat". Ketiadaan panduan teknis ini menimbulkan celah hukum bagi pengendali data untuk melepaskan diri dari tuntutan hukum dengan dalih menjadi korban serangan siber yang tidak terprediksi (*force majeure*). Ketidakjelasan indikator kelalaian ini membuat proses penjatuhannya sanksi administratif menjadi rawan gugatan balik di Pengadilan Tata Usaha Negara. Akibatnya, esensi penegakan hukum sebagai sarana korektif bagi tata kelola data digital menjadi kehilangan arah dan tujuannya.

Penanganan kebocoran data terdapat permasalahan ego sektoral yang akut dalam penanganan kebocoran data pada instansi pemerintahan itu sendiri. Ketika data milik lembaga negara bocor, proses investigasi sering kali terhambat oleh batasan kerahasiaan negara dan perlindungan korps. UU PDP menempatkan lembaga publik dalam posisi yang setara dengan korporasi swasta sebagai pengendali data. Dalam praktiknya, sanksi denda terhadap instansi pemerintah sulit dieksekusi. Tidak ada mekanisme pemotongan anggaran negara yang jelas untuk membayar denda administratif akibat kelalaian birokrasi dalam menjaga data publik. Hal ini menciptakan standar ganda dalam penegakan hukum yang mencederai prinsip persamaan di hadapan hukum (*equality before the law*).

Dilihat dari perspektif teori kemanfaatan hukum, UU PDP saat ini belum memberikan kemanfaatan protektif yang berkeadilan bagi para korban kebocoran data. Fokus penyelesaian kasus masih sangat berorientasi pada penghukuman pelaku atau pemungutan denda untuk kas negara. Hak korban untuk mendapatkan pemulihan nama baik dan ganti kerugian secara langsung belum diakomodasi melalui mekanisme litigasi yang cepat dan murah. Korban harus menempuh jalur gugatan perdata terpisah yang memakan biaya besar serta waktu yang panjang di pengadilan. Ketidakpraktisan jalur pemulihan hak ini membuat subjek data enggan memperjuangkan hak privasinya secara hukum.

Tantangan sinkronisasi aturan pasca-berlakunya UU PDP juga terlihat dari adanya irisan kompetensi dengan Undang-Undang Informasi dan Transaksi Elektronik. UU ITE masih memuat pasal-pasal pidana terkait transmisi data tanpa hak yang sering kali tumpang-tindih dengan delik pidana dalam UU PDP. Ketidaksinkronan ini memicu kebingungan bagi penyidik kepolisian dalam menentukan pasal dakwaan yang paling tepat di persidangan. Dualisme aturan ini berisiko melahirkan disparitas putusan hakim yang dapat mengaburkan kepastian hukum bagi pencari keadilan. Penataan ulang regulasi siber melalui harmonisasi yang ketat antar-rezim hukum mutlak diperlukan untuk mengeliminasi konflik norma tersebut.

Secara keseluruhan, efektivitas Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dalam menanggulangi kebocoran data masih berada pada level yang rendah. Secara normatif undang-undang ini telah memberikan lompatan besar dalam penyediaan payung hukum pelindungan privasi. Ketiadaan lembaga pengawas independen yang operasional, lemahnya kapasitas forensik aparat, rendahnya budaya hukum masyarakat, serta standar ganda pada instansi publik membuat undang-undang ini belum mampu bekerja secara optimal. UU PDP baru berfungsi sebagai instrumen hukum yang bersifat macan kertas, keras dalam teks regulasi tetapi lemah dalam implementasi penegakan.

Untuk meningkatkan efektivitas hukum ini, langkah mendesak yang harus diambil pemerintah adalah segera meresmikan Otoritas Pelindungan Data Pribadi yang bebas dari intervensi politik dan bisnis. Lembaga ini harus dibekali penyidik pegawai negeri sipil yang memiliki keahlian siber tingkat tinggi serta hak akses audit forensik tanpa batas ke seluruh pengendali data. Pengadilan siber khusus juga perlu dipertimbangkan untuk mempercepat proses adjudikasi kasus-kasus pelanggaran data pribadi yang kompleks. Tanpa penguatan



struktur penegakan hukum yang radikal, hak privasi warga negara di ruang digital Indonesia akan terus berada dalam posisi yang terancam.

Perlindungan data pribadi tidak boleh hanya dipandang sebagai beban administratif bagi korporasi atau pelengkap regulasi bagi negara. Perlindungan ini adalah perwujudan langsung dari penghormatan terhadap martabat manusia di era digital yang wajib dijamin penuh oleh negara. Keberhasilan UU PDP menanggulangi kebocoran data akan menjadi tolok ukur utama kedaulatan digital Indonesia di mata dunia internasional. Komitmen politik yang kuat dari pemerintah untuk menegakkan aturan tanpa pandang bulu menjadi kunci final dari efektivitas hukum regulasi ini.

## **2. Kendala Yuridis dan Non-Yuridis yang Mempengaruhi Implementasi Undang-Undang Informasi dan Transaksi Elektronik dalam Upaya Pelindungan Data Pribadi**

Implementasi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) menghadapi berbagai hambatan mendasar yang mereduksi efektivitasnya sebagai instrumen pelindungan data pribadi. Kendala yuridis pertama bersumber dari ketidakjelasan perumusan norma siber di dalam teks undang-undang itu sendiri. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua UU ITE masih mempertahankan pola pengaturan yang multitafsir mengenai batasan tindakan mengakses sistem elektronik secara tidak sah. Ketidakjelasan rumusan ini memicu terjadinya perdebatan doktrinal di ruang sidang mengenai pembuktian unsur kesengajaan dan tanpa hak dari pelaku pelanggaran data. Ketidakpastian teks undang-undang pada akhirnya menyulitkan hakim untuk menegakkan keadilan normatif secara konsisten.

Kendala yuridis berikutnya muncul dari ketidaksinkronan rezim hukum pidana UU ITE dengan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Konstruksi delik pelanggaran hak atas data dalam UU ITE sering kali tumpang-tindih (overlapping) dengan delik pidana penanganan data tanpa hak dalam UU PDP. Konflik tata hukum ini melahirkan ketidakpastian yurisdiksi penegakan hukum akibat ketiadaan aturan transisi yang mempertegas kedudukan *lex specialis* di antara kedua undang-undang tersebut. Ketidakselarasan horizontal ini berpotensi menimbulkan disparitas putusan yang mencederai asas kepastian hukum dalam sistem peradilan siber di Indonesia.

Ketiadaan aturan turunan yang bersifat teknis juga menjadi hambatan yuridis yang melumpuhkan daya eksekusi UU ITE di lapangan. Kementerian Komunikasi dan Digital belum menerbitkan panduan audit operasional yang baku bagi para penyelenggara sistem elektronik guna mendeteksi kegagalan sistem. Ketiadaan kodifikasi teknis ini menyebabkan aparat penegak hukum kehilangan parameter objektif untuk menilai standardisasi keandalan sistem keamanan siber yang dikelola oleh korporasi. Ketiadaan standar baku tersebut dimanfaatkan oleh pengendali data untuk melepaskan diri dari tuntutan hukum dengan dalih mengalami serangan siber yang tidak terprediksi.

Ketebalan birokrasi dalam mekanisme kerja sama internasional menjadi kendala yuridis terakhir yang membatasi daya jangkauan penegakan UU ITE. Tindakan pemrosesan data tanpa hak dalam kejahatan siber lintas batas negara menuntut adanya penegakan hukum transnasional yang cepat. Prosedur formal bantuan hukum timbal balik (mutual legal assistance) yang dimiliki Indonesia memerlukan proses administrasi diplomatik yang memakan waktu berbulan-bulan. Lambatnya birokrasi yurisdiksi internasional ini mengakibatkan barang bukti digital berupa log data pelaku keburu dihapus oleh penyedia layanan internet di luar negeri sebelum penyidik mendapatkan izin akses resmi.

Hambatan non-yuridis dalam implementasi UU ITE bersumber dari ketidaksiapan infrastruktur teknologi yang dimiliki oleh lembaga penegak hukum siber nasional. Kualitas perangkat keras dan perangkat lunak yang digunakan oleh unit siber kepolisian di daerah masih sangat tertinggal jika dibandingkan dengan kecepatan teknik peretasan mutakhir. Keterbatasan alat forensik digital menyebabkan proses pelacakan alamat IP terenkripsi milik pelaku

pembobolan data berjalan lambat. Ketimpangan teknologi penegakan hukum ini membuat banyak kasus kebocoran data pribadi berskala daerah berakhir tanpa penyelesaian hukum yang jelas.

Faktor non-yuridis lain yang memperlemah implementasi undang-undang ini adalah keterbatasan kuantitas dan kualitas sumber daya manusia penyidik siber. Jumlah aparat penegak hukum yang memiliki sertifikasi forensik digital internasional masih sangat minim dan terpusat di tingkat markas besar kepolisian. Aparat penegak hukum di tingkat kepolisian resort sering kali tidak memiliki kompetensi siber yang memadai untuk melakukan olah tempat kejadian perkara digital secara valid. Keterbatasan keahlian struktural ini berdampak pada rapuhnya penyusunan berkas perkara penyidikan, sehingga dakwaan pelanggaran data pribadi rawan dipatahkan oleh penasihat hukum terdakwa di persidangan.

Ketimpangan finansial atau ketersediaan anggaran operasional penegakan hukum turut menjadi kendala non-yuridis yang signifikan. Proses penyidikan kasus kejahatan data digital membutuhkan biaya yang sangat besar untuk melakukan klonifikasi hard drive, sewa server laboratorium forensik, hingga menghadirkan saksi ahli siber dari kalangan akademisi maupun praktisi. Anggaran penanganan kasus siber di kepolisian daerah sering kali tidak mencukupi untuk membiayai seluruh rangkaian pembuktian ilmiah yang rumit tersebut. Kendala finansial ini memaksa penyidik untuk memprioritaskan penanganan kasus siber yang menjadi sorotan media massa saja, sementara kasus kebocoran data warga kelas bawah terabaikan.

Budaya hukum masyarakat Indonesia yang permisif terhadap penyalahgunaan privasi merupakan kendala sosiologis non-yuridis yang sulit diubah. Kesadaran masyarakat mengenai nilai ekonomis dan protektif dari data pribadi masih berada pada level yang sangat rendah. Publik cenderung menganggap remeh tindakan penyebaran data identitas orang lain di jejaring media sosial tanpa izin pemiliknya. Rendahnya kepedulian sosiologis ini menghambat efektivitas fungsi preventif UU ITE karena masyarakat secara tidak sadar terus mereproduksi tindakan-tindakan yang melanggar hak privasi digital.

Ego sektoral di antara institusi pengelola keamanan siber negara memperparah efektivitas implementasi penegakan hukum non-yuridis di lapangan. Proses investigasi kebocoran data sering kali diwarnai oleh aksi saling lempar tanggung jawab antara Kementerian Komunikasi dan Digital, Badan Siber dan Sandi Negara (BSSN), serta Kepolisian Negara Republik Indonesia. Ketiga lembaga ini memiliki ego birokrasi yang kuat dan jarang membagikan data intelijen siber mereka secara terintegrasi. Ketidaksolidan struktur kelembagaan ini menguntungkan para pelaku kejahatan data pribadi karena mereka dapat bergerak bebas memanfaatkan kelengahan koordinasi antar-instansi pemerintah.

Kendala non-yuridis terakhir terletak pada minimnya komitmen kepatuhan dari penyelenggara sistem elektronik swasta maupun instansi publik untuk memperkuat benteng pertahanan siber mereka. Banyak perusahaan dan lembaga pemerintah yang memandang investasi keamanan siber sebagai beban finansial yang mengurangi keuntungan operasional, bukan sebagai kewajiban hukum. Sikap abai ini tecermin dari rendahnya alokasi anggaran belanja teknologi informasi untuk memperbarui sistem enkripsi data secara berkala. Ketidakpatuhan korporasi dan birokrasi ini menciptakan kerentanan infrastruktur digital nasional yang terus mengeksploitasi hak privasi warga negara dari ancaman kebocoran data yang massif.

## **KESIMPULAN DAN SARAN**

### **Kesimpulan**

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi merupakan tonggak penting dalam pembangunan sistem hukum nasional yang memberikan pengakuan terhadap data pribadi sebagai bagian dari hak atas privasi yang wajib dilindungi oleh negara. Pengaturan mengenai hak subjek data, kewajiban pengendali dan pemroses data pribadi, mekanisme pemrosesan data, serta pengenaan sanksi administratif dan pidana menunjukkan

bahwa secara normatif undang-undang ini telah mengadopsi prinsip-prinsip perlindungan data pribadi yang sejalan dengan perkembangan hukum internasional. Kehadiran regulasi tersebut menjadi dasar hukum yang memberikan kepastian bagi masyarakat dalam memperoleh perlindungan atas penggunaan dan pemanfaatan data pribadi di era transformasi digital.

Efektivitas penegakan Undang-Undang Nomor 27 Tahun 2022 masih menghadapi berbagai hambatan yang menyebabkan tujuan pembentukannya belum tercapai secara optimal. Hambatan tersebut tidak hanya berasal dari aspek substansi hukum, tetapi juga dipengaruhi oleh belum terbentuknya lembaga pengawas independen yang memiliki kewenangan mengawasi kepatuhan penyelenggara sistem elektronik, menerima pengaduan masyarakat, melakukan investigasi, serta menjatuhkan sanksi administratif. Kondisi tersebut mengakibatkan penegakan hukum masih tersebar pada berbagai instansi yang memiliki kewenangan berbeda, menimbulkan tumpang tindih pengaturan, inkonsistensi dalam penerapan sanksi, serta belum memberikan mekanisme pemulihan yang efektif bagi korban kebocoran data pribadi. Faktor non-yuridis juga memberikan pengaruh yang signifikan terhadap efektivitas perlindungan data pribadi di Indonesia. Keterbatasan kapasitas sumber daya manusia, belum meratanya kemampuan forensik digital, rendahnya kesadaran penyelenggara sistem elektronik terhadap kewajiban perlindungan data pribadi, serta masih rendahnya literasi digital masyarakat menyebabkan pelanggaran data pribadi terus berulang. Penegakan hukum yang efektif memerlukan dukungan kelembagaan yang kuat, koordinasi antarlembaga yang terpadu, kesiapan infrastruktur teknologi, serta budaya hukum yang menempatkan perlindungan data pribadi sebagai bagian dari penghormatan terhadap hak asasi manusia. Keberhasilan implementasi Undang-Undang Nomor 27 Tahun 2022 pada akhirnya tidak hanya ditentukan oleh kualitas norma yang diatur dalam peraturan perundang-undangan, tetapi juga oleh kemampuan negara menghadirkan sistem pengawasan dan penegakan hukum yang independen, konsisten, dan berorientasi pada perlindungan hak masyarakat.

## Saran

Pemerintah perlu mempercepat pembentukan lembaga perlindungan data pribadi yang bersifat independen sebagaimana diamanatkan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Kehadiran lembaga tersebut menjadi kebutuhan mendesak untuk menjalankan fungsi pengawasan, menerima pengaduan masyarakat, melakukan investigasi terhadap dugaan pelanggaran, menjatuhkan sanksi administratif, serta mengoordinasikan penegakan hukum perlindungan data pribadi secara terpadu. Keberadaan otoritas yang independen akan mengurangi tumpang tindih kewenangan antarinstansi, memperkuat akuntabilitas penyelenggara sistem elektronik, serta memberikan kepastian hukum bagi masyarakat sebagai pemilik data pribadi. Pemerintah bersama Dewan Perwakilan Rakyat perlu menyusun peraturan pelaksana yang memberikan kejelasan mengenai mekanisme pengawasan, tata cara penegakan hukum, prosedur penyelesaian sengketa, serta mekanisme pemberian ganti kerugian bagi korban kebocoran data pribadi. Pengaturan yang lebih rinci akan memperkuat implementasi Undang-Undang Nomor 27 Tahun 2022 sehingga tidak hanya berfungsi sebagai norma hukum, tetapi juga menjadi instrumen yang efektif dalam memberikan perlindungan terhadap hak konstitusional masyarakat atas data pribadinya. Aparat penegak hukum perlu membangun koordinasi yang lebih terintegrasi dalam menangani tindak pidana perlindungan data pribadi. Harmonisasi antara Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Kitab Undang-Undang Hukum Pidana, serta peraturan sektoral lainnya menjadi penting untuk menghindari perbedaan penafsiran, tumpang tindih kewenangan, dan inkonsistensi dalam penegakan hukum. Keseragaman penerapan hukum akan meningkatkan kepastian hukum sekaligus memperkuat perlindungan terhadap hak-hak korban. Penyelenggara sistem elektronik, baik instansi pemerintah maupun sektor privat, perlu memperkuat tata kelola

pelindungan data pribadi melalui penerapan prinsip privacy by design, penguatan sistem keamanan siber, pelaksanaan audit keamanan informasi secara berkala, penilaian risiko terhadap setiap aktivitas pemrosesan data, serta penyusunan prosedur penanganan insiden kebocoran data yang cepat, transparan, dan akuntabel. Langkah tersebut menjadi bagian dari tanggung jawab hukum pengendali data pribadi dalam menjamin keamanan data yang dipercayakan oleh masyarakat. Penguatan kapasitas sumber daya manusia juga menjadi kebutuhan yang tidak dapat diabaikan. Aparat penegak hukum, hakim, jaksa, penyidik, penyelenggara sistem elektronik, dan pejabat yang bertanggung jawab terhadap pengelolaan data pribadi perlu memperoleh pelatihan yang berkelanjutan mengenai hukum pelindungan data pribadi, keamanan siber, pembuktian digital, serta forensik digital. Kompetensi tersebut akan meningkatkan kualitas penegakan hukum sekaligus mempercepat penyelesaian perkara yang berkaitan dengan pelanggaran data pribadi. Masyarakat perlu memperoleh edukasi yang lebih luas mengenai hak dan kewajiban sebagai subjek data pribadi, risiko penyalahgunaan data pribadi, serta mekanisme hukum yang dapat ditempuh apabila terjadi pelanggaran. Peningkatan literasi digital akan memperkuat kesadaran masyarakat dalam menjaga keamanan data pribadinya serta mendorong partisipasi aktif dalam pengawasan terhadap penyelenggara sistem elektronik. Pelindungan data pribadi pada akhirnya tidak hanya bergantung pada keberadaan regulasi dan lembaga pengawas, tetapi juga pada terbentuknya budaya hukum digital yang menempatkan privasi sebagai bagian dari hak asasi manusia yang harus dihormati dan dilindungi.

### **Kontribusi Author**

Penulis bertanggung jawab secara penuh terhadap keseluruhan proses penelitian, yang meliputi perumusan konsep penelitian, identifikasi dan analisis permasalahan hukum, pengumpulan serta analisis bahan hukum, penyusunan naskah, interpretasi hasil penelitian, revisi substansi artikel, hingga persetujuan akhir terhadap naskah yang diterbitkan.

### **Acknowledgment (Opsional)**

Penulis menyampaikan apresiasi kepada seluruh pihak yang telah memberikan dukungan akademik selama proses penyusunan penelitian ini. Ucapan terima kasih juga disampaikan kepada institusi yang telah menyediakan akses terhadap berbagai sumber hukum, literatur ilmiah, dan dokumen pendukung yang menjadi dasar analisis dalam penelitian ini. Penulis turut menghargai masukan konstruktif dari para mitra bestari (reviewer) yang berkontribusi dalam penyempurnaan kualitas artikel ini.

## **REFERENSI**

### **Bahan Hukum (Peraturan Perundang-undangan)**

- Indonesia. (1945). *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*.
- Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 115, Tambahan Lembaran Negara Republik Indonesia Nomor 4843.
- Indonesia. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952.
- Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6824.
- Indonesia. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.

Lembaran Negara Republik Indonesia Tahun 2024 Nomor 3, Tambahan Lembaran Negara Republik Indonesia Nomor 6924.

### **Buku, Jurnal, dan Laporan (Bahan Hukum Sekunder)**

- Amirulloh, M. (2025). Sinkronisasi hukum pidana siber: Analisis tumpang tindih regulasi antara rezim UU ITE dan Undang-Undang Pelindungan Data Pribadi. *Jurnal Ius Quia Iustum*, 32(2), 115–119.
- Amirulloh, M., & Sastrawan, A. (2025). Akuntabilitas badan publik sebagai pengendali data: Problematika penerapan sanksi administratif Undang-Undang Pelindungan Data Pribadi. *Jurnal Hukum Tata Negara dan Siber*, 13(2), 112–115.
- Badan Siber dan Sandi Negara. (2023). *Laporan tahunan keamanan siber Indonesia tahun 2023*. BSSN.
- Budhijanto, D. (2024). *Hukum komunikasi digital dan dinamika sosiologis ruang siber*. Refika Aditama.
- Budhijanto, D. (2024). *Kedaulatan digital dan konformitas hukum siber global*. Refika Aditama.
- Dewi, S. (2015). *Cyber law: Perlindungan privasi atas informasi pribadi dalam e-commerce*. Refika Aditama.
- Djafar, W. (2021). *Hukum perlindungan data pribadi di Indonesia*. Lembaga Studi dan Advokasi Masyarakat (ELSAM).
- Makarim, E. (2020). Tanggung jawab hukum penyelenggara sistem elektronik atas kegagalan perlindungan data pribadi. *Jurnal Hukum & Pembangunan*, 50(2), 289–292.
- Manan, B. (2021). *Konstruksi asas-asas hukum dalam sistem peraturan perundang-undangan negara*. FH UI Press.
- Rahardjo, S. (2020). *Ilmu hukum: Teori, filsafat, dan aspek sosiologisnya*. PT Citra Aditya Bakti.
- Ramli, A. M., & Amirulloh, M. (2025). Problematika adjudikasi kejahatan data digital: Tantangan struktur hukum dalam implementasi Undang-Undang Pelindungan Data Pribadi. *Jurnal Hukum dan Pasar Modal*, 14(2), 102–105.
- Rosadi, S. D. (2025). Konvergensi standar global pelindungan data pribadi ke dalam rezim hukum siber Indonesia pasca-pengundangan UU PDP. *Jurnal Hukum Ius Quia Iustum*, 32(1), 55–58.
- Rosadi, S. D., & Pratama, G. G. (2025). Budaya hukum dan kesadaran masyarakat terhadap hak privasi atas pelindungan data pribadi di era digital. *Jurnal Hukum Padjadjaran*, 12(1), 94–97.
- Suseno, S. (2022). *Yurisdiksi tindak pidana siber: Teori dan praktik penegakan hukum transnasional*. Sinar Grafika.
- Suseno, S., & Takariawan, A. (2025). Ambiguitas norma dan problematika penafsiran unsur 'tanpa hak' dalam tindak pidana akses ilegal menurut perubahan UU ITE. *Jurnal Hukum Siber dan Teknologi*, 14(1), 22–25.
- Wahyono, T. (2023). *Digital forensics: Panduan praktis investigasi kejahatan siber dan pembuktian hukum*. Andi Offset.