

Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan Peretasan

Winda Agustina^{1*}, Sidi Ahyar Wiraguna²

Fakultas Ilmu Hukum, Hukum, Universitas Esa Unggul Jakarta

*Corresponding Author e-mail: agustinawinda276@gmail.com

Abstract: *This study aims to analyze the form of legal protection of the right to privacy of personal data in the face of hacking crimes according to Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). The research method used is normative juridical with a statutory approach. The results show that the PDP Law provides a strong legal basis for the protection of personal data, including data subject rights mechanisms, data controller obligations, and administrative and criminal sanctions for violations. However, the implementation of this law still faces challenges, such as weak cyber law enforcement infrastructure and limited public digital literacy. Therefore, it is necessary to strengthen the institutionalization of supervisory authorities, increase the capacity of law enforcement officers, and educate the public to support the effectiveness of legal protection of personal data from hacking crimes.*

Abstract: Penelitian ini bertujuan untuk menganalisis bentuk perlindungan hukum terhadap hak privasi atas data pribadi dalam menghadapi kejahatan peretasan menurut Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan. Hasil penelitian menunjukkan bahwa UU PDP (Undang-Undang Perlindungan Data Pribadi) memberikan dasar hukum yang kuat bagi perlindungan data pribadi, termasuk mekanisme hak subjek data, kewajiban pengendali data, serta sanksi administratif dan pidana bagi pelanggaran. Namun demikian, implementasi undang-undang ini masih menghadapi tantangan, seperti lemahnya infrastruktur penegakan hukum siber dan keterbatasan literasi digital masyarakat. Oleh karena itu, perlu penguatan kelembagaan otoritas pengawas, peningkatan kapasitas aparat penegak hukum, serta edukasi publik untuk mendukung efektivitas perlindungan hukum atas data pribadi dari kejahatan peretasan.

Article History

Article History

Received: April 30, 2025

Revised: May 10, 2025

Published: May 17, 2025

Keywords :

Legal Protection, Personal Data, Privacy Rights, Hacking, PDP Law

Kata kunci :

Perlindungan Hukum, Data Pribadi, Hak Privasi, Peretasan, UU PDP



<https://doi.org/10.5281/zenodo.15486554>

This is an open-access article under the [CC-BY-SA License](#).



PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi (TIK) pada era Revolusi Industri 4.0 telah melahirkan disrupsi *digital* yang mengubah secara fundamental cara manusia berinteraksi, bertransaksi, dan menjalankan aktivitas sehari-hari (A Sulaiman, 2024). Dalam hal ini, data pribadi menjadi komoditas strategis yang tak terelakkan dalam berbagai aspek kehidupan, mulai dari layanan kesehatan, perbankan, pendidikan, hingga administrasi pemerintahan. Informasi yang sebelumnya bersifat privat kini terekspos secara digital dan menjadi bagian dari ekosistem siber global (Elvina Putri Maheswari, Urgensi persetujuan pemilik data dalam pengelolaan data pribadi oleh platform digital, 2025). Fenomena ini berdampak langsung pada semakin tingginya urgensi untuk melindungi hak privasi individu terhadap penyalahgunaan data pribadi. Menurut konsep hak asasi manusia, privasi merupakan

hak fundamental yang harus dilindungi oleh negara, sebagaimana diatur dalam Pasal 12 Deklarasi Universal Hak Asasi Manusia (*Universal Declaration of Human Rights*) dan ditegaskan pula dalam Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Namun, kemajuan teknologi tidak hanya membawa manfaat, tetapi juga melahirkan tantangan serius berupa meningkatnya ancaman kejahatan siber, khususnya peretasan (*hacking*) terhadap sistem informasi yang menyimpan data pribadi. Peretasan merupakan tindakan ilegal yang melibatkan akses tanpa izin terhadap sistem elektronik dengan tujuan mencuri, mengubah, atau menghancurkan data. Di Indonesia, berbagai kasus kebocoran data telah terjadi dalam skala masif. Pada tahun 2022, publik dihebohkan dengan dugaan kebocoran data 105 juta penduduk dari sistem Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan yang dijual di forum *online* oleh pelaku dengan nama samaran “Bjorka”. Tak hanya itu, situs resmi Komisi Pemilihan Umum (KPU) juga menjadi sasaran peretasan, menyebabkan tersebarnya data pemilih secara luas di dunia maya¹. Laporan dari Badan Siber dan Sandi Negara (BSSN) mencatat bahwa, di antaranya berupa *ransomware*, *phishing*, dan *SQL injection*, yang sebagian besar menargetkan sistem penyimpanan data pribadi². Kondisi ini menunjukkan bahwa Indonesia sangat rentan terhadap ancaman keamanan siber, terutama terkait perlindungan data pribadi yang menyangkut hak privasi setiap warga negara.

Sebelum hadirnya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), regulasi yang mengatur perlindungan data pribadi di Indonesia tersebar dalam berbagai peraturan sektoral seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Administrasi Kependudukan, dan Peraturan Menteri Komunikasi dan Informatika (Ahmad Redi, 2023). Fragmentasi ini menimbulkan ketidakpastian hukum dan lemahnya penegakan terhadap pelanggaran data (Faisal Santiago, 2022). Beberapa penelitian sebelumnya lebih banyak menyoroti aspek normatif dan perbandingan internasional terhadap perlindungan data pribadi³. Namun, belum banyak kajian yang secara spesifik dan mendalam mengkaji efektivitas perlindungan hukum terhadap hak privasi masyarakat dalam konteks kejahatan peretasan pasca disahkannya UU PDP (Undang-Undang Perlindungan Data Pribadi). Hal ini menimbulkan kesenjangan penelitian, terutama terkait antara pengaturan ideal yang tertuang dalam undang-undang (*das Sollen*) dengan praktik implementasi hukum di lapangan (*das Sein*). Padahal, untuk menjamin keadilan dan kepastian hukum, diperlukan instrumen hukum yang tidak hanya memuat norma, tetapi juga mampu dioperasionalkan secara konkret dan responsif terhadap perkembangan ancaman digital (Elda Septi Darmayanti, 2025).

Urgensi penelitian ini terletak pada meningkatnya intensitas dan kompleksitas kejahatan peretasan di Indonesia serta belum optimalnya upaya perlindungan hukum terhadap korban pelanggaran hak privasi. UU PDP (Undang-Undang Perlindungan Data Pribadi) merupakan tonggak dalam sistem hukum nasional karena untuk pertama kalinya memberikan landasan hukum yang komprehensif mengenai hak subjek data, kewajiban pengendali data, prinsip pengolahan data, serta mekanisme sanksi administratif, perdata, dan pidana terhadap pelanggaran data pribadi (Elvina Putri Maheswari, Urgensi persetujuan pemilik data dalam pengelolaan data pribadi oleh platform digital, 2025). Namun demikian, dalam praktiknya masih terdapat sejumlah hambatan, baik dari sisi infrastruktur kelembagaan, koordinasi antarlembaga, kapasitas aparat penegak hukum, maupun literasi digital masyarakat.

Penelitian ini memiliki kebaruan (*novelty*) karena secara khusus mengkaji perlindungan hukum terhadap hak privasi sebagai bentuk hak konstitusional yang dilanggar akibat peretasan, dengan menggunakan pendekatan yuridis terhadap norma-norma yang diatur dalam UU PDP (Undang-Undang Perlindungan Data Pribadi) serta dikaitkan dengan konteks faktual yang terjadi pasca pengesahan undang-undang tersebut. Selain itu, penelitian ini mengisi kekosongan kajian empiris dengan

¹ Ricky Febriansyah et al., “Keamanan Sistem Informasi Pemilu Melalui Computer Security Incident Response Team (Csirt) Pemilu Serentak 2024” 3, no. 4 (2024).

² Manayra Aisha Putri Indradjaja, Sigid Suseno, and Budi Arta Atmaja, “Implementasi Penyidikan Terhadap Tindak Pidana Siber Dalam Perspektif Perbandingan Hukum: Indonesia Dan Inggris Raya,” *Jurnal Ilmiah Penegakan Hukum* 11, no. 2 (December 26, 2024): 162–72, <https://doi.org/10.31289/jiph.v11i2.12931>.

³ Naufal Rizqiyanto et al., “Media Hukum Indonesia (MHI) Published by Yayasan Daarul Huda Krueng Mane Politik Hukum Pembentukan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi” 2, no. 2 (2024): 3032–6591, <https://doi.org/10.5281/zenodo.10995150>.

menganalisis kesesuaian antara prinsip-prinsip perlindungan hukum data pribadi dengan implementasi yang dilakukan oleh institusi terkait dalam menghadapi kasus nyata peretasan. Dengan pendekatan tersebut, hasil penelitian diharapkan dapat memberikan kontribusi terhadap pengembangan teori hukum perlindungan data pribadi, sekaligus sebagai masukan kebijakan bagi penguatan sistem regulasi dan tata kelola keamanan siber nasional. Oleh karena itu, penulis merasa tertarik untuk melakukan penelitian dengan judul “Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi Dari Kejahatan Perteasan Menurut Undang-Undang Nomor 27 Tahun 2022”.

METODE

Penelitian ini merupakan penelitian hukum normatif, yaitu suatu penelitian yang difokuskan pada studi terhadap norma-norma hukum positif, baik yang tertulis dalam peraturan perundang-undangan maupun yang terdapat dalam putusan pengadilan, doktrin, dan prinsip-prinsip hukum. Metode penelitian hukum normatif dipilih karena mampu memberikan kerangka hukum yang sistematis dan jelas untuk dianalisis secara konseptual dan dogmatis. Seperti yang dijelaskan oleh Wiraguna, pendekatan ini unggul dalam membentuk konstruksi hukum yang logis dan terstruktur karena berangkat dari sumber-sumber hukum formal seperti undang-undang dan dokumen yuridis lainnya⁴. Fokus utama dari pendekatan ini adalah untuk menelaah secara sistematis ketentuan-ketentuan hukum yang relevan, dalam hal ini Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta peraturan pelaksanaannya, guna mengetahui sejauh mana instrumen hukum tersebut memberikan perlindungan terhadap hak privasi data pribadi dari kejahatan peretasan.

Jenis dan sumber data dalam penelitian ini terdiri dari data sekunder yang mencakup bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi peraturan perundang-undangan yang relevan dengan pokok bahasan. Bahan hukum sekunder berupa literatur ilmiah, jurnal, hasil penelitian sebelumnya, serta pendapat para ahli yang membahas isu perlindungan data pribadi dan kejahatan siber. Adapun bahan hukum tersier berupa kamus hukum, ensiklopedia hukum, dan sumber-sumber penunjang lainnya.

Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*), yaitu dengan menelusuri dan menganalisis dokumen-dokumen hukum, jurnal ilmiah, dan literatur terkait yang relevan. Studi kepustakaan menjadi metode utama dalam penelitian hukum normatif karena seluruh data yang dikaji berasal dari dokumen hukum yang telah disahkan dan/atau diakui secara akademik. Menurut Wiraguna et al, kajian pustaka diperlukan untuk membangun argumen hukum secara menyeluruh dan mendalam, serta untuk menghindari generalisasi atau asumsi yang tidak berdasar⁵.

Seluruh bahan hukum yang diperoleh dianalisis menggunakan metode deskriptif-analitis, yaitu dengan mendeskripsikan peraturan yang berlaku dan menganalisis implementasi serta kekurangannya dalam memberikan perlindungan hukum terhadap data pribadi dari tindakan peretasan. Pendekatan analisis dilakukan secara kualitatif, yakni berfokus pada penalaran hukum, interpretasi sistematis, serta evaluasi terhadap celah atau kekosongan hukum. Pendekatan ini diperkuat dengan metode reflektif yang bertujuan untuk menelaah norma hukum tidak hanya dari segi teks, tetapi juga dari praktik pelaksanaannya di masyarakat. Konsep refleksi ini ditekankan oleh Wiraguna et al. sebagai langkah untuk memahami konteks hukum secara utuh dan logis⁶.

HASIL DAN PEMBAHASAN

Perlindungan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022

⁴ Sidi Ahyar Wiraguna, “Metode Normatif Dan Empiris Dalam Penelitian Hukum: Studi Eksploratif Di Indonesia,” *Public Sphere: Jurnal Sosial Politik, Pemerintahan Dan Hukum* 3, no. 3 (November 30, 2024), <https://doi.org/10.59818/jps.v3i3.1390>.

⁵ Sidi Wiraguna, L.M.F. Purwanto, and Robert Rianto Widjaja, “Metode Penelitian Kualitatif Di Era Transformasi Digital Qualitative Research Methods in the Era of Digital Transformation,” *Arsitekta : Jurnal Arsitektur Dan Kota Berkelanjutan* 6, no. 01 (May 31, 2024): 46–60, <https://doi.org/10.47970/arsitekta.v6i01.524>.

⁶ Wiraguna, Purwanto, and Rianto Widjaja.

Perlindungan terhadap data pribadi merupakan isu hukum yang semakin memperoleh perhatian, terutama di tengah pesatnya perkembangan teknologi informasi dan komunikasi (Al Satria Diaha, 2025). Sebagai respons atas kebutuhan hukum yang mendesak terkait privasi dan keamanan informasi, Pemerintah Indonesia menetapkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (selanjutnya disebut UU PDP). Undang-undang ini secara resmi diundangkan pada tanggal 17 Oktober 2022 dan mencerminkan komitmen negara dalam menjamin hak konstitusional warga negara atas perlindungan data pribadi.

UU PDP (Undang-Undang Perlindungan Data Pribadi) mengatur secara komprehensif hak, kewajiban, prinsip, hingga sanksi pidana terkait pengelolaan data pribadi, baik oleh individu, badan hukum, maupun entitas lainnya (Naswa Fiolla Anggraini, 2025). Berdasarkan Berdasarkan Pasal 1 angka 2, perlindungan data pribadi didefinisikan sebagai segala bentuk upaya untuk menjaga dan mengamankan data pribadi individu, guna menjamin hak-hak konstitusional yang melekat pada setiap warga negara. Hal ini menunjukkan bahwa perlindungan data bukan hanya isu teknis, melainkan bagian integral dari perlindungan hak asasi manusia yang dilindungi oleh konstitusi (Anesya Fritiana, 2025).

Cakupan keberlakuan UU PDP (Undang-Undang Perlindungan Data Pribadi) diatur dalam Pasal 2, yang mencakup subjek hukum di dalam maupun luar wilayah Indonesia sepanjang memiliki akibat hukum terhadap data pribadi warga negara Indonesia. Pengaturan ini mencerminkan pendekatan yurisdiksi ekstrateritorial, yaitu suatu prinsip hukum yang memperluas jangkauan perlindungan hukum melintasi batas wilayah negara, asalkan subjek hukumnya berkaitan langsung dengan individu Indonesia. Dengan kata lain, setiap pihak yang memproses data pribadi warga negara Indonesia, termasuk entitas asing, wajib tunduk pada ketentuan dalam UU PDP (Undang-Undang Perlindungan Data Pribadi) apabila aktivitas mereka berdampak terhadap subjek data Indonesia.

Asas penyelenggaraan perlindungan data pribadi ditegaskan dalam Pasal 3, yang mencakup asas perlindungan, kepastian hukum, kepentingan umum, kemanfaatan, kehati-hatian, keseimbangan, pertanggungjawaban, dan kerahasiaan. Setiap pihak yang terlibat dalam pemrosesan data pribadi wajib berpegang pada prinsip-prinsip ini sebagai pedoman dalam mengambil keputusan dan tindakan, guna memastikan bahwa pengelolaan data dilakukan secara sah, etis, dan proporsional.

Terkait klasifikasi data, Pasal 4 membedakan antara data pribadi umum dan data pribadi spesifik. Data pribadi umum mencakup informasi yang bersifat umum dan dapat dikenali secara langsung, seperti nama lengkap, jenis kelamin, kewarganegaraan, agama, dan status perkawinan. Sementara itu, data pribadi spesifik meliputi informasi yang lebih sensitif dan berisiko tinggi terhadap penyalahgunaan, antara lain data biometrik, genetika, kesehatan, orientasi seksual, serta riwayat kriminal. Data jenis ini memerlukan standar keamanan yang lebih tinggi dan prosedur pengelolaan yang ketat agar tidak disalahgunakan untuk kepentingan yang bertentangan dengan hak asasi manusia.

Hak-hak subjek data pribadi diuraikan secara komprehensif dalam Pasal 5 hingga Pasal 13, di mana setiap individu sebagai pemilik data pribadi berhak untuk mengetahui secara jelas dasar hukum dan tujuan pemrosesan data mereka, mengakses informasi yang disimpan, melakukan perbaikan terhadap data yang tidak akurat, membatasi atau menghentikan pemrosesan, serta menghapus atau memindahkan data tersebut. Selain itu, subjek data juga memiliki hak untuk menolak penggunaan data pribadi mereka dalam konteks tertentu, serta hak untuk mengajukan keberatan atau gugatan apabila ditemukan indikasi penyalahgunaan data oleh pengendali atau prosesor data (Sri Mulyati, 2025).

Pasal 14 sampai Pasal 25 mengatur kewajiban bagi pengendali dan prosesor data pribadi. Pengendali data wajib memberikan informasi secara transparan kepada subjek data mengenai rincian pemrosesan, jangka waktu penyimpanan data, serta identitas pihak ketiga yang memperoleh data tersebut. Dalam hal ini, setiap proses pengumpulan atau pemanfaatan data harus terlebih dahulu mendapatkan persetujuan eksplisit dari pemilik data, kecuali dalam keadaan tertentu seperti pelaksanaan kontrak, kewajiban hukum, atau untuk kepentingan vital subjek data (Verina Dwi Muryani, 2025).

UU PDP (Undang-Undang Perlindungan Data Pribadi) juga memberikan perlindungan khusus bagi kelompok rentan seperti anak-anak dan penyandang disabilitas, sebagaimana diatur dalam Pasal 25 dan Pasal 26. Pemrosesan data pribadi anak harus mendapatkan persetujuan dari orang tua atau wali,

sedangkan untuk penyandang disabilitas, persetujuan wajib diberikan dengan memperhatikan cara komunikasi yang sesuai dengan kebutuhan mereka.

Tanggung jawab pengendali data ditegaskan lebih lanjut dalam Pasal 35 dan Pasal 38, yang mewajibkan pengendali data untuk menerapkan sistem keamanan informasi, menjamin integritas dan kerahasiaan data, serta menyusun dokumentasi perlindungan data. Selain itu, pengendali data berkewajiban menunjuk petugas perlindungan data pribadi dalam kondisi tertentu.

Apabila terjadi insiden pelanggaran atau kebocoran data pribadi, UU PDP (Undang-Undang Perlindungan Data Pribadi) menegaskan bahwa pengendali data harus segera bertindak transparan dan responsif. Dalam Pasal 46, ditegaskan bahwa pengendali data wajib memberikan pemberitahuan tertulis kepada subjek data (pemilik data pribadi) serta lembaga pengawas yang berwenang dalam waktu paling lambat 3 x 24 jam setelah pelanggaran diketahui. Pemberitahuan ini harus memuat informasi penting seperti jenis data pribadi yang bocor, potensi dampak negatif yang mungkin timbul akibat kebocoran tersebut, serta langkah-langkah penanganan dan mitigasi yang telah dan akan dilakukan untuk mengurangi risiko kerugian. Ketentuan ini bertujuan agar subjek data dapat segera mengambil tindakan pencegahan, misalnya mengganti kata sandi atau membatasi akses yang berpotensi disalahgunakan, sehingga dampak dari kebocoran data dapat diminimalisasi.

UU PDP (Undang-Undang Perlindungan Data Pribadi) juga memberikan hak-hak khusus kepada subjek data, salah satunya hak untuk menghapus data pribadi mereka, yang dikenal dengan istilah *the right to be forgotten*. Ketentuan ini diatur dalam Pasal 43 hingga Pasal 45, yang menyatakan bahwa subjek data berhak mengajukan permohonan penghapusan data apabila data tersebut sudah tidak relevan lagi, telah melewati masa simpan yang ditentukan, atau diproses secara melanggar hukum. Namun, hak ini tidak bersifat mutlak; penghapusan data harus tetap mempertimbangkan ketentuan peraturan perundang-undangan lain yang berlaku, seperti kewajiban penyimpanan data untuk kepentingan hukum tertentu. Dengan demikian, hak untuk menghapus data memberikan keseimbangan antara perlindungan privasi dan kepentingan hukum yang lebih luas.

UU PDP (Undang-Undang Perlindungan Data Pribadi) mengatur secara rinci sanksi administratif bagi pihak yang melanggar ketentuan perlindungan data pribadi. Pasal 57 menyebutkan bahwa sanksi administratif ini dapat berupa teguran tertulis, penghentian sementara kegiatan pemrosesan data, hingga penghapusan data yang tidak sesuai ketentuan. Selain itu, pelanggar juga dapat dikenakan denda administratif dengan jumlah maksimal sebesar 2% dari total pendapatan tahunan pelaku pelanggaran. Besarnya denda ini dirancang untuk memberikan efek jera yang signifikan dan mendorong kepatuhan terhadap aturan perlindungan data pribadi. Pengawasan terhadap pelaksanaan UU ini dilakukan oleh lembaga khusus yang dibentuk oleh Presiden, sebagaimana diatur dalam Pasal 58 hingga Pasal 60. Lembaga ini memiliki tugas utama untuk mengawasi implementasi UU, menangani pengaduan dan sengketa, serta memastikan bahwa seluruh pelaku pengelolaan data mematuhi standar perlindungan data yang ditetapkan.

Pasal 63 memberikan ruang bagi partisipasi masyarakat dalam mendukung perlindungan data pribadi melalui edukasi, pelatihan, sosialisasi, serta pengawasan. Sedangkan penyelesaian sengketa terkait pelanggaran data dapat dilakukan melalui pengadilan atau melalui mekanisme alternatif seperti mediasi atau arbitrase sesuai dengan ketentuan dalam Pasal 64. Kemudian, Pasal 65 hingga Pasal 68 memberikan dasar hukum terkait sanksi pidana bagi setiap orang yang dengan sengaja dan melawan hukum memperoleh, mengungkapkan, atau menggunakan data pribadi bukan miliknya. Sanksi pidana yang diatur meliputi pidana penjara paling lama 5 tahun dan/atau denda hingga Rp5 miliar, tergantung pada jenis pelanggaran dan dampak yang ditimbulkan. Ketentuan pidana ini menegaskan keseriusan negara dalam memberikan efek jera kepada pelaku penyalahgunaan data pribadi.

Dengan demikian, Undang-Undang Nomor 27 Tahun 2022 tidak hanya menjadi tonggak dalam perkembangan hukum siber di Indonesia, tetapi juga memperkuat posisi subjek data sebagai pemilik sah atas informasi pribadinya. Undang-undang ini juga menciptakan mekanisme pengawasan yang lebih ketat terhadap pelaku pemrosesan data serta menyediakan jalur hukum yang jelas untuk penyelesaian sengketa dan pemulihan hak.

Kelebihan dan Kekurangan Undang-Undang Nomor 27 Tahun 2022

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) memberikan kemajuan dalam upaya perlindungan hak asasi manusia di ranah digital, khususnya hak individu atas kendali terhadap data pribadinya. Salah satu keunggulan utama UU ini adalah penekanan pada prinsip transparansi dan pengakuan terhadap hak-hak subjek data, yang mencakup hak untuk mengakses, mengoreksi, menghapus, serta menarik kembali persetujuan atas pemrosesan data pribadi. UU PDP juga mengadopsi prinsip-prinsip dasar dari *General Data Protection Regulation* (GDPR) milik Uni Eropa, termasuk peran dan tanggung jawab pengendali data (*Data Controller*) serta pemroses data (*Data Processor*).

Kehadiran regulasi ini memberikan kepastian hukum bagi masyarakat Indonesia dalam era *digital*, sekaligus menumbuhkan kepercayaan publik terhadap penyelenggara sistem elektronik yang mengelola data pribadi. Selain itu, UU PDP (Undang-Undang Perlindungan Data Pribadi) mengatur sanksi yang tegas, baik administratif maupun pidana, yang mencakup peringatan tertulis, denda administratif, hingga pidana penjara bagi pelanggar, dengan tujuan menciptakan efek jera dan meningkatkan kepatuhan terhadap regulasi yang ada. Sejumlah penelitian mendukung efektivitas pendekatan sanksi ini yang menyimpulkan bahwa penegakan hukum yang tegas mampu mendorong pengelola data untuk lebih bertanggung jawab⁷.

Namun demikian, implementasi UU PDP (Undang-Undang Perlindungan Data Pribadi) juga menghadapi sejumlah kelemahan yang cukup signifikan. Salah satunya terletak pada lemahnya pengaturan mengenai perlindungan data pribadi anak dan penyandang disabilitas. Pasal 25 dan 26 memang menyebutkan bahwa data kelompok rentan ini harus diproses dengan persetujuan orang tua atau wali, namun ketentuan tersebut belum menjelaskan secara rinci bentuk perlindungan khusus yang harus diterapkan. Akibatnya, banyak platform digital, terutama yang bergerak di bidang media sosial dan pendidikan daring, masih mengalami kesulitan dalam menyesuaikan kebijakan privasi mereka terhadap kelompok ini⁸.

Mamonto mencatat bahwa ketidakjelasan ini menyebabkan lambatnya adaptasi oleh perusahaan teknologi terhadap kebijakan baru yang ditetapkan⁹. Selain itu, UU PDP (Undang-Undang Perlindungan Data Pribadi) juga belum menetapkan secara tegas batas usia anak, yang berimplikasi pada ketidakselarasan dengan peraturan lain seperti UU Perlindungan Anak, UU Perkawinan, dan KUH Perdata. Ketidakkonsistenan ini menciptakan ruang abu-abu dalam pelaksanaan hukum, sehingga menyulitkan aparat penegak hukum dalam menangani kasus pelanggaran data pribadi anak¹⁰.

Kelemahan lain yang tak kalah krusial adalah ketiadaan peraturan pelaksana yang diamanatkan oleh UU PDP (Undang-Undang Perlindungan Data Pribadi). Meskipun undang-undang ini mengharuskan pembentukan sepuluh peraturan pemerintah sebagai panduan teknis pelaksanaan, hingga lebih dari satu tahun sejak diundangkan, belum satu pun regulasi tersebut diterbitkan. Kekosongan hukum ini menimbulkan ketidakpastian dalam penafsiran dan pelaksanaan UU PDP (Undang-Undang Perlindungan Data Pribadi), serta membuka peluang terjadinya pelanggaran terhadap hak data pribadi masyarakat. Rafasya et al. menggarisbawahi bahwa ketidakjelasan ini dapat merugikan pemilik data pribadi karena tidak adanya acuan yang pasti untuk pengajuan perlindungan atau penegakan hukum¹¹.

Selain itu, Pasal 12 ayat (1) UU PDP (Undang-Undang Perlindungan Data Pribadi) memang memberikan hak kepada pemilik data untuk menuntut ganti rugi, namun tidak menjelaskan secara rinci mengenai mekanisme gugatan, pengadilan yang berwenang, maupun tata cara proses peradilan yang

⁷ Juan Matheus and Ariawan Gunadi, "Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital : Kajian Perbandingan Dengan KPPU," *JUSTISI* 10, no. 1 (October 18, 2023): 20–35, <https://doi.org/10.33506/jurnaljustisi.v10i1.2757>.

⁸ Sidi Ahyar Wiraguna, Abdullah Sulaiman, and Megawati Barthos, "Implementation of Consumer Personal Data Protection in Ecommerce from the Perspective of Law No. 27 of 2022," *Journal of World Science* 3, no. 3 (March 31, 2024): 410–18, <https://doi.org/10.58344/jws.v3i3.584>.

⁹ D. F Mamonto, "Analisis Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022," *LEX PRIVATUM* 13, no. 4 (2024).

¹⁰ Y., Linra, N., Darham, A., Handrianto, D., Sianturi, R. R., Martin, D., ... & Saputra, H Daeng, "Perlindungan Data Pribadi Dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi," *Innovative: Journal Of Social Science Research* 3, no. 6 (2023).

¹¹ R., Citra, H., & Fauzi, E Rafasya, "Perlindungan Hukum Terhadap Konsumen Atas Pencurian Data Pribadi Dalam Transaksi Elektronik," *Jurnal Ilmu Sosial, Humaniora Dan Seni* 2, no. 1 (2023).

harus ditempuh. Ketidakjelasan ini menciptakan hambatan praktis dalam implementasi hak-hak hukum pemilik data, dan berpotensi melemahkan efektivitas perlindungan yang dijanjikan oleh undang-undang ini¹².

Kritik lain yang cukup mendasar adalah belum terbentuknya lembaga independen pengawas perlindungan data pribadi yang diamanatkan dalam Pasal 58 UU PDP (Undang-Undang Perlindungan Data Pribadi). Lembaga ini seharusnya bertanggung jawab langsung kepada Presiden dan memiliki kewenangan luas dalam pengawasan, audit, penegakan hukum, serta pengelolaan sengketa data pribadi. Namun hingga saat ini, belum ada regulasi turunan yang mengatur pembentukan dan tata kerja lembaga tersebut. Padahal, keberadaan lembaga independen ini sangat penting sebagai instrumen pengawasan yang objektif dan profesional, sekaligus menjadi jaminan bahwa pelaksanaan perlindungan data tidak sekadar bersifat formalitas hukum. Pranata et al. menekankan bahwa lembaga pengawas independen merupakan elemen kunci dalam sistem perlindungan data pribadi yang terpercaya dan sesuai standar internasional¹³. Oleh karena itu, keterlambatan pemerintah dalam membentuk lembaga ini tidak hanya menghambat implementasi UU PDP, tetapi juga dapat menurunkan kepercayaan publik terhadap komitmen negara dalam menjamin keamanan data warganya.

Bentuk Perlindungan Hukum Undang-Undang Nomor 27 Tahun 2022

Perlindungan hukum merupakan suatu mekanisme yang dihadirkan oleh negara untuk menjamin hak-hak subjek hukum, baik individu maupun badan hukum, agar tidak dirugikan oleh tindakan yang melawan hukum. Perlindungan ini diwujudkan dalam bentuk pengaturan hukum yang dilengkapi dengan ketentuan sanksi guna mendorong kepatuhan terhadap norma-norma yang berlaku. Dalam konteks hukum Indonesia, bentuk perlindungan hukum terbagi ke dalam dua kategori utama, yaitu:

1. Perlindungan Hukum Preventif

Perlindungan hukum preventif yang diatur dalam UU PDP (Undang-Undang Perlindungan Data Pribadi) dirancang secara khusus agar setiap aktivitas yang berhubungan dengan pengumpulan, penyimpanan, pemrosesan, hingga distribusi data pribadi dilakukan secara sah dan transparan. Tujuan utama dari perlindungan preventif ini adalah memastikan bahwa setiap proses pengelolaan data pribadi memenuhi prinsip-prinsip perlindungan privasi yang kuat dan tidak merugikan subjek data.

Salah satu aspek dari perlindungan preventif adalah kewajiban bagi pengendali data untuk memperoleh persetujuan yang jelas dan tegas dari pemilik data sebelum data tersebut digunakan. Persetujuan ini harus diberikan secara eksplisit, artinya tidak boleh bersifat implisit atau tersirat. Subjek data harus secara sadar dan sukarela memberikan izin setelah mendapatkan informasi yang cukup mengenai tujuan penggunaan data, ruang lingkup pemrosesan, dan dampak yang mungkin timbul. Hal ini menegaskan prinsip transparansi dan kontrol oleh individu terhadap data pribadinya, yang menempatkan subjek data bukan sebagai objek pasif, melainkan sebagai pemilik sah dari data pribadi tersebut.

Selain kewajiban mendapatkan persetujuan, UU PDP (Undang-Undang Perlindungan Data Pribadi) juga memberikan hak-hak luas kepada subjek data sebagai bentuk perlindungan lebih lanjut. Hak-hak tersebut meliputi hak untuk mengetahui jenis data yang dikumpulkan, hak untuk mengakses data tersebut, hak untuk memperbaiki jika terdapat kesalahan, hak untuk menghapus data, hak untuk membatasi proses pemrosesan data, serta hak untuk menarik kembali persetujuan yang telah diberikan. Dengan adanya hak-hak ini, subjek data memiliki kontrol penuh atas informasi pribadinya sehingga mereka dapat menjaga privasi dan keamanan data mereka secara lebih efektif.

¹² Elfian Fauzi and Nabila Alif Radika Shandy, "Hak Atas Privasi Dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi," *Jurnal Lex Renaissance* 7, no. 3 (July 1, 2022): 445–61, <https://doi.org/10.20885/JLR.vol7.iss3.art1>.

¹³ A., Juono, A. A., & Binarida, A. V. Y Pranata, "Implementasi Asas Kehati-Hatian Dalam Perlindungan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Di Era Digital 5.0," *JOURNAL OF LAW AND NATION* 3, no. 3 (2024).

Selanjutnya, UU PDP (Undang-Undang Perlindungan Data Pribadi) mengharuskan pengendali data untuk menerapkan langkah-langkah perlindungan yang memadai, baik dari sisi teknis maupun administratif. Ini termasuk pengamanan sistem informasi agar data pribadi tidak mudah diakses oleh pihak yang tidak berwenang, pencegahan terhadap kebocoran data, serta langkah-langkah mitigasi risiko lainnya. Apabila terjadi insiden kebocoran data, pengendali data wajib melakukan pemberitahuan secara cepat dan transparan kepada subjek data dan otoritas perlindungan data. Tujuannya adalah agar pihak-pihak yang terdampak dapat mengambil tindakan preventif yang tepat, seperti mengganti kata sandi, menutup akses yang berpotensi disalahgunakan, atau tindakan lain yang dapat meminimalisir dampak buruk dari kebocoran tersebut.

Selain pengaturan teknis dan administratif, UU PDP (Undang-Undang Perlindungan Data Pribadi) juga menempatkan edukasi dan literasi digital sebagai bagian dari perlindungan preventif. Pemerintah dan pihak-pihak terkait didorong untuk melaksanakan program sosialisasi dan peningkatan kesadaran masyarakat mengenai hak dan kewajiban mereka dalam menjaga data pribadi di era digital. Dengan tingkat literasi digital yang tinggi, masyarakat diharapkan menjadi lebih waspada dan cermat dalam memberikan data pribadi kepada pihak ketiga, sehingga risiko penyalahgunaan data dapat diminimalkan. Edukasi ini sangat penting mengingat perkembangan teknologi digital yang pesat dan semakin banyaknya interaksi *online* yang berpotensi menimbulkan kerawanan terhadap pelanggaran privasi.

Secara keseluruhan, perlindungan hukum preventif dalam UU PDP (Undang-Undang Perlindungan Data Pribadi) bertujuan untuk menciptakan ekosistem pengelolaan data pribadi yang aman, transparan, dan bertanggung jawab. Hal ini tidak hanya melindungi individu dari potensi penyalahgunaan data, tetapi juga membangun kepercayaan publik terhadap penggunaan teknologi informasi dan layanan digital yang semakin meluas di berbagai sektor kehidupan.

2. Perlindungan Hukum Represif

Perlindungan hukum represif dalam kerangka Undang-Undang Perlindungan Data Pribadi (UU PDP) berfungsi sebagai mekanisme penegakan hukum yang ditujukan untuk menindak tegas pelanggaran yang telah terjadi terkait dengan pengelolaan dan perlindungan data pribadi. Dengan kata lain, pendekatan represif ini berfokus pada pemberian sanksi atau hukuman terhadap pihak-pihak yang terbukti melanggar aturan pengelolaan data pribadi, sebagai bentuk pertanggungjawaban dan pencegahan agar pelanggaran serupa tidak terulang di masa depan. Instrumen ini mencakup:

a. Sanksi Administratif

UU PDP (Undang-Undang Perlindungan Data Pribadi) memberikan kewenangan khusus kepada lembaga pengawas data pribadi untuk mengambil tindakan administratif terhadap pengendali data maupun prosesor data yang melanggar ketentuan undang-undang. Sanksi administratif ini merupakan langkah awal yang bersifat preventif sekaligus korektif, dengan tujuan mendorong pelaku agar segera memperbaiki kesalahan dan menjalankan kewajiban sesuai dengan ketentuan yang berlaku. Bentuk sanksi administratif yang dapat dijatuhkan sangat beragam, mulai dari teguran tertulis sebagai peringatan resmi, penghentian sementara aktivitas pemrosesan data pribadi yang bermasalah, hingga perintah penghapusan data yang telah diproses secara ilegal atau tidak sesuai aturan. Selain itu, UU PDP (Undang-Undang Perlindungan Data Pribadi) juga mengatur pengenaan denda administratif yang memiliki batas maksimal cukup signifikan, yakni hingga dua persen dari total pendapatan tahunan entitas atau perusahaan yang melakukan pelanggaran tersebut. Keunikan dari sanksi administratif ini adalah sifatnya yang progresif, artinya besaran dan jenis sanksi dapat ditingkatkan apabila pelanggaran dilakukan secara berulang kali atau ketika pelanggaran tidak segera diperbaiki oleh pelaku. Hal ini memberikan fleksibilitas bagi regulator untuk menyesuaikan sanksi dengan tingkat keseriusan pelanggaran yang terjadi.

b. Sanksi Pidana

Selain sanksi administratif, UU PDP (Undang-Undang Perlindungan Data Pribadi) juga menetapkan mekanisme penindakan melalui jalur pidana sebagai bentuk perlindungan yang lebih tegas dan keras terhadap pelanggaran pengelolaan data pribadi. Sanksi pidana ini dikenakan kepada individu atau badan hukum yang secara sengaja mengakses, menyebarkan, atau menggunakan data pribadi milik orang lain tanpa memiliki izin atau hak yang sah. Ketentuan Pasal 67 UU PDP (Undang-Undang Perlindungan Data Pribadi) mengatur bahwa pelaku pelanggaran dapat dijatuhi hukuman penjara hingga lima tahun dan/atau denda yang jumlahnya dapat mencapai lima miliar rupiah. Ketentuan ini menunjukkan bahwa pemerintah sangat serius dalam memberikan efek jera bagi pelaku pelanggaran data pribadi. Jika pelanggaran dilakukan oleh korporasi atau badan usaha, UU PDP (Undang-Undang Perlindungan Data Pribadi) memperbolehkan pengenaan sanksi denda pidana yang besarnya bisa sampai sepuluh kali lipat dari batas maksimum denda yang berlaku bagi perorangan, menandakan bahwa perusahaan sebagai entitas juga harus bertanggung jawab penuh atas kelalaian atau kesengajaan dalam menjaga data pribadi.

Selain itu, UU PDP (Undang-Undang Perlindungan Data Pribadi) juga mengatur sanksi tambahan yang lebih berat seperti perampasan keuntungan yang diperoleh secara ilegal dari tindak pelanggaran, pembekuan aktivitas usaha, pencabutan izin operasional, bahkan sampai pembubaran korporasi jika pelanggaran dianggap sangat serius dan merugikan masyarakat luas. Bentuk-bentuk sanksi pidana ini memperlihatkan betapa perlindungan data pribadi bukan hanya perkara administratif, melainkan juga menjadi masalah hukum yang serius dengan dampak sosial dan ekonomi yang besar, seperti yang terlihat dalam beberapa kasus besar kebocoran data di Indonesia, contohnya pada lembaga BPJS Kesehatan dan perusahaan Kredit Plus.

c. Sanksi Perdata

Selain dua jenis sanksi di atas, UU PDP (Undang-Undang Perlindungan Data Pribadi) juga memberikan ruang bagi korban pelanggaran data pribadi untuk menempuh jalur perdata guna menuntut ganti rugi atas kerugian yang diderita akibat kebocoran atau penyalahgunaan data pribadi mereka. Sanksi perdata ini sesuai dengan prinsip hukum yang tertuang dalam Pasal 1365 Kitab Undang-Undang Hukum Perdata (KUH Perdata), yang menyatakan bahwa setiap tindakan yang melanggar hukum dan menyebabkan kerugian kepada pihak lain wajib untuk diganti kerugiannya. Dengan demikian, korban dapat mengajukan gugatan kepada pengendali data pribadi yang dianggap bertanggung jawab atas pelanggaran tersebut untuk memperoleh kompensasi atau restitusi.

Namun demikian, dalam praktiknya mekanisme pengajuan gugatan perdata terkait perlindungan data pribadi masih menghadapi kendala, karena UU PDP (Undang-Undang Perlindungan Data Pribadi) belum mengatur secara teknis dan rinci prosedur pelaksanaan tuntutan perdata ini dalam peraturan pelaksanaannya. Ketidakjelasan dan kekosongan aturan ini menyebabkan hambatan dalam pelaksanaan hak-hak korban, khususnya bagi masyarakat umum yang biasanya tidak memiliki akses atau sumber daya hukum yang memadai untuk mengupayakan haknya. Situasi ini menimbulkan tantangan tersendiri dalam aspek perlindungan hukum represif, karena tanpa mekanisme yang jelas dan mudah dijangkau, maka upaya penegakan hak korban dan pemberian efek jera kepada pelaku bisa menjadi kurang efektif

SIMPULAN

Berdasarkan hasil pembahasan, dapat disimpulkan bahwa Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah memberikan kerangka hukum yang jelas dan tegas dalam melindungi hak-hak subjek data serta mengatur kewajiban para pengendali dan prosesor data. Regulasi ini menjadi langkah penting dalam menjawab tantangan digitalisasi yang semakin kompleks, meskipun implementasinya masih menghadapi berbagai hambatan, seperti kesiapan lembaga pengawas dan



rendahnya literasi masyarakat. Oleh karena itu, diperlukan penguatan kelembagaan, peningkatan kesadaran publik, serta penegakan hukum yang konsisten agar perlindungan data pribadi dapat terwujud secara optimal.

REFERENSI

- Ahyar Wiraguna, Sidi, Abdullah Sulaiman, and Megawati Barthos. "Implementation of Consumer Personal Data Protection in Ecommerce from the Perspective of Law No. 27 of 2022." *Journal of World Science* 3, no. 3 (March 31, 2024): 410–18. <https://doi.org/10.58344/jws.v3i3.584>.
- Ahmad Redi, S. A. (2023). Harmonization of Law on Transactions E-Commerce in order to support Indonesia's Economic Development. *Journal of Social Research*, 1929-1936.
- A Sulaiman, M. B. (2024). Implementation of Consumer Personal Data Protection in Ecommerce from the Perspective of Law No. 27 of 2022. *Jurnal Word of Science (JWS)*, 410-418.
- Al Satria Diaha, S. A. (2025). Tanggung Jawab Hukum Platform E-Commerce atas Kebocoran Data Pribadi dalam Perspektif UU No. 27 Tahun 2022. *Jurnal Kajian Hukum Dan Kebijakan Publik*, 1089-1096.
- Anesya Fritiana, S. A. (2025). Penyalahgunaan Data Pribadi Pada Layanan Pinjaman Online: Analisis Perlindungan dan Sanksi Hukum. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 523-529.
- Daeng, Y., Linra, N., Darham, A., Handrianto, D., Sianturi, R. R., Martin, D., ... & Saputra, H. "Perlindungan Data Pribadi Dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi." *Innovative: Journal Of Social Science Research* 3, no. 6 (2023).
- Elda Septi Darmayanti, S. A. (2025). Tanggung jawab hukum pinjaman online terhadap penyebaran data nasabah secara ilegal. *ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora*, 233-251.
- Elvina Putri Maheswari, S. A. (2025). Urgensi persetujuan pemilik data dalam pengelolaan data pribadi oleh platform digital. 908-914.
- Elvina Putri Maheswari, S. A. (2025). Urgensi persetujuan pemilik data dalam pengelolaan data pribadi oleh platform digital. *Jurnal Ilmu Komunikasi Dan Sosial Politik*, 908-914.
- Faisal Santiago, S. A. (2022). The Implementation of Electronic Contract on Business to Business (B2B) Electronic Transaction. *Interdisciplinary Social Studies*, 35-42.
- Fauzi, Elfian, and Nabila Alif Radika Shandy. "Hak Atas Privasi Dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi." *Jurnal Lex Renaissance* 7, no. 3 (July 1, 2022): 445–61. <https://doi.org/10.20885/JLR.vol7.iss3.art1>.
- Febriansyah, Ricky, Ana Husnayanti, Kpu Kabupaten, Bangka Tengah, and Indonesia Koba. "Keamanan Sistem Informasi Pemilu Melalui Computer Security Incident Response Team (Csirt) Pemilu Serentak 2024" 3, no. 4 (2024).
- Indradjaja, Manayra Aisha Putri, Sigid Suseno, and Budi Arta Atmaja. "Implementasi Penyidikan Terhadap Tindak Pidana Siber Dalam Perspektif Perbandingan Hukum: Indonesia Dan Inggris Raya." *Jurnal Ilmiah Penegakan Hukum* 11, no. 2 (December 26, 2024): 162–72. <https://doi.org/10.31289/jiph.v11i2.12931>.
- Mamonto, D. F. "Analisis Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022." *LEX PRIVATUM* 13, no. 4 (2024).



- Matheus, Juan, and Ariawan Gunadi. "Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital : Kajian Perbandingan Dengan KPPU." *JUSTISI* 10, no. 1 (October 18, 2023): 20–35. <https://doi.org/10.33506/jurnaljustisi.v10i1.2757>.
- Naswa Fiolla Anggraini, S. A. (2025). Tanggung Jawab Hukum Platform Pinjaman Online terhadap Penyalahgunaan dan Penyebaran Data Pribadi Konsumen secara Ilegal. *Jurnal Riset Sosial Humaniora dan Pendidikan*, 144-167.
- Pranata, A., Juono, A. A., & Binarida, A. V. Y. "Implementasi Asas Kehati-Hatian Dalam Perlindungan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Di Era Digital 5.0." *JOURNAL OF LAW AND NATION* 3, no. 3 (2024).
- Rafasya, R., Citra, H., & Fauzi, E. "Perlindungan Hukum Terhadap Konsumen Atas Pencurian Data Pribadi Dalam Transaksi Elektronik." *Jurnal Ilmu Sosial, Humaniora Dan Seni* 2, no. 1 (2023).
- Rizqiyanto, Naufal, Azmi Fathu Rohman, Faiz Al-Haq, and Maulabeta Raya. "Media Hukum Indonesia (MHI) Published by Yayasan Daarul Huda Krueng Mane Politik Hukum Pembentukan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi" 2, no. 2 (2024): 3032–6591. <https://doi.org/10.5281/zenodo.10995150>.
- Sri Mulyati, S. A. (2025). PERLINDUNGAN DATA PRIBADI DI ERA DIGITAL. Causa: *Jurnal Hukum dan Kewarganegaraan*, 91-100.
- Wiraguna, Sidi Ahyar. "Metode Normatif Dan Empiris Dalam Penelitian Hukum: Studi Eksploratif Di Indonesia." *Public Sphere: Jurnal Sosial Politik, Pemerintahan Dan Hukum* 3, no. 3 (November 30, 2024). <https://doi.org/10.59818/jps.v3i3.1390>.
- Wiraguna, Sidi, L.M.F. Purwanto, and Robert Rianto Widjaja. "Metode Penelitian Kualitatif Di Era Transformasi Digital Qualitative Research Methods in the Era of Digital Transformation." *Arsitekta : Jurnal Arsitektur Dan Kota Berkelanjutan* 6, no. 01 (May 31, 2024): 46–60. <https://doi.org/10.47970/arsitekta.v6i01.524>.
- Verina Dwi Muryani, S. A. (2025). EFEKTIVITAS UNDANG-UNDANG PERLINDUNGAN DATA PRIBADI DALAM MENJAWAB TANTANGAN KEAMANAN SIBER DI INDONESIA. Causa: *Jurnal Hukum dan Kewarganegaraan*, 81-90.