Al-Zayn: Jurnal Ilmu Sosial & Hukum e-ISSN 3026-2917
https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZyn p-ISSN 3026-2925
Volume 4 Number 2, 2026
DOI: https://doi.org/10.61104/alz.v4i2.5682

Analisis Yuridis terhadap Perlindungan Hak Privasi dalam Komunikasi Digital Berdasarkan Undang-Undang Pelindungan Data Pribadi di Indonesia

Siti Kajar Rejeki
Ilmu Hukum, Universitas Terbuka, Indonesia
Email Korespondensi: 053144491@ecampus.ut.ac.id

Article received: 01 Januari 2026, Review process: 12 Januari 2026
Article Accepted: 22 Februari 2026, Article published: 24 April 2026

ABSTRACT
The rapid development of information technology in the digital era poses serious threats to individual privacy rights, particularly in digital communication activities. Indonesia responded to this situation by enacting Law Number 27 of 2022 concerning Personal Data Protection as the first comprehensive legal instrument in the field of national data governance. This study aims to examine the legal construction of privacy regulations in digital communication, measure the effectiveness of its implementation, and identify obstacles encountered in the enforcement process. The method used is normative legal research with statutory, conceptual, and comparative approaches. The study results indicate that the law structuredly regulates data subject rights, data controller obligations, data minimization principles, and the right to be forgotten mechanism. However, its effectiveness is hampered by the lack of operational and independent frameworks, low public digital legal literacy, and inconsistencies between the Personal Data Protection Law and the Electronic Information and Transactions Law. Strengthening efforts are needed through regulatory harmonization, the establishment of a credible supervisory authority, and regulatory updates that adapt to developments in artificial intelligence and the Internet of Things.
Keywords: *Privacy Rights Protection, Digital Communication, Personal Data Protection Law.*

ABSTRAK
Pesatnya perkembangan teknologi informasi di era digital memunculkan ancaman serius terhadap hak privasi individu, khususnya dalam aktivitas komunikasi berbasis digital. Indonesia merespons kondisi ini dengan mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi sebagai instrumen hukum komprehensif pertama di bidang tata kelola data nasional. Penelitian ini bertujuan menelaah secara yuridis konstruksi pengaturan privasi dalam komunikasi digital, mengukur tingkat efektivitas implementasinya, serta mengidentifikasi hambatan yang dihadapi dalam proses penegakannya. Metode yang digunakan adalah penelitian hukum normatif dengan pendekatan statute, konseptual, dan komparatif. Hasil kajian menunjukkan bahwa undang-undang tersebut telah mengatur secara terstruktur hak-hak data subject, kewajiban data controller, prinsip data minimization, hingga mekanisme right to be forgotten. Tetapi efektivitasnya masih terhambat oleh belum terbentuk secara operasional dan independen, rendahnya digital legal literacy masyarakat, serta inkonsistensi norma antara UU PDP dan UU Informasi dan Transaksi Elektronik. Upaya penguatan diperlukan melalui harmonisasi

regulasi, pembentukan otoritas pengawas yang kredibel, serta pembaruan regulasi yang adaptif terhadap perkembangan teknologi artificial intelligence dan Internet of Things.
Kata Kunci: *Perlindungan Hak Privasi, Komunikasi Digital, UU PDP.*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang pesat pada era digital telah membawa perubahan fundamental dalam cara manusia berinteraksi dan berkomunikasi. *Digital communication* kini menjadi medium utama pertukaran informasi, baik dalam ranah pribadi maupun profesional. Namun di balik kemudahan tersebut, terdapat ancaman serius terhadap hak privasi individu yang semakin rentan terekspos. Data pribadi pengguna kerap dikumpulkan, diproses, bahkan disalahgunakan oleh berbagai pihak tanpa sepengetahuan atau persetujuan pemiliknya. Kondisi ini memunculkan urgensi Pelindungan hukum yang komprehensif terhadap *right to privacy* dalam ekosistem digital, khususnya di Indonesia yang tingkat penetrasi internetnya terus meningkat signifikan setiap tahun (Zakiya & Farhah, 2026). Indonesia sebagai salah satu negara dengan penggunaan internet dan media sosial tertinggi secara global menghadapi tantangan besar dalam menjamin keamanan data pribadi warganya (DataReportal, 2025). Berbagai kasus kebocoran data yang melibatkan instansi pemerintah maupun sektor swasta mencerminkan lemahnya tata kelola pelindungan data di tanah air. Selama bertahun-tahun, Indonesia hanya mengandalkan Pasal 28G Undang-Undang Dasar 1945 dan beberapa regulasi sektoral yang bersifat parsial sebagai landasan Pelindungan privasi (Wiraguna & Barthos, 2025). Ketiadaan payung hukum yang khusus dan menyeluruh menjadi celah yang dieksploitasi oleh berbagai pihak yang tidak bertanggung jawab, sehingga masyarakat kehilangan kendali atas *personal data* mereka sendiri (Bahram, 2023).

Merespons kondisi tersebut, pemerintah Indonesia akhirnya mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) yang menjadi tonggak penting dalam sejarah hukum digital nasional. Undang-undang ini mengadopsi pendekatan *comprehensive data governance* yang mengatur hak-hak subjek data, kewajiban pengendali data, serta sanksi bagi para pelanggar. UU PDP hadir sebagai respons terhadap desakan publik dan tekanan internasional, terutama setelah serangkaian insiden *data breach* berskala besar yang mengguncang kepercayaan masyarakat terhadap keamanan sistem digital nasional (Seftiyana et al., 2026). Meskipun UU PDP telah disahkan, implementasinya dalam konteks komunikasi digital masih menghadapi berbagai tantangan yuridis yang kompleks. Ketentuan mengenai *consent*, *data minimization*, dan hak untuk dilupakan (*right to be forgotten*) masih memerlukan penjabaran teknis yang lebih operasional. Di sisi lain mekanisme penegakan hukum dan pembentukan otoritas pengawas Pelindungan data belum sepenuhnya terwujud. Hal ini menciptakan kesenjangan antara norma hukum yang tertulis dengan praktik Pelindungan data yang sesungguhnya terjadi di lapangan, sehingga hak privasi dalam komunikasi digital belum terlindungi secara optimal (Judijanto et al., 2024).

Berdasarkan uraian di atas, kajian yuridis terhadap Pelindungan hak privasi dalam komunikasi digital berdasarkan UU PDP menjadi sangat relevan dan

mendesak untuk dilakukan. Analisis mendalam diperlukan untuk mengidentifikasi kekuatan dan kelemahan regulasi yang ada, serta memberikan rekomendasi konstruktif demi penguatan *privacy rights* di Indonesia. Penelitian ini diharapkan dapat berkontribusi dalam pengembangan hukum digital nasional yang lebih adaptif dan responsif terhadap dinamika teknologi yang terus berubah. Berdasarkan latar belakang yang telah diuraikan, penelitian ini merumuskan tiga pokok permasalahan. Pertama, bagaimana pengaturan hukum Pelindungan hak privasi dalam komunikasi digital menurut Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi di Indonesia? Kedua, bagaimana implementasi dan efektivitas Pelindungan hak privasi dalam komunikasi digital berdasarkan UU PDP ditinjau dari perspektif yuridis? Ketiga, apa saja hambatan dan tantangan yang dihadapi dalam penegakan Pelindungan hak privasi komunikasi digital berdasarkan UU PDP serta bagaimana solusi hukum yang dapat ditawarkan?

Penelitian ini bertujuan untuk menganalisis secara yuridis pengaturan Pelindungan hak privasi dalam komunikasi digital berdasarkan UU PDP sebagai regulasi terbaru di bidang Pelindungan data pribadi di Indonesia. Penelitian ini juga bertujuan untuk mengkaji tingkat efektivitas implementasi ketentuan UU PDP dalam memberikan Pelindungan nyata bagi subjek data dalam aktivitas komunikasi digital sehari-hari. Penelitian ini berupaya mengidentifikasi hambatan yuridis yang ada serta merumuskan rekomendasi hukum yang konstruktif demi penguatan sistem Pelindungan *privacy rights* dalam ekosistem digital Indonesia. Penelitian ini diharapkan memberikan manfaat teoritis berupa sumbangan pemikiran bagi pengembangan ilmu hukum, khususnya di bidang hukum teknologi informasi dan hukum Pelindungan data pribadi di Indonesia. Secara praktis, hasil penelitian ini dapat menjadi referensi bagi pembuat kebijakan, praktisi hukum, dan lembaga pengawas dalam menyempurnakan regulasi serta mekanisme penegakan UU PDP. Di samping itu penelitian ini juga bermanfaat bagi masyarakat luas, khususnya pengguna layanan digital, dalam memahami hak-hak privasi mereka serta langkah-langkah hukum yang dapat ditempuh apabila terjadi pelanggaran terhadap *personal data* dalam aktivitas komunikasi digital.

METODE

Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan metode penelitian hukum normatif (*normative legal research*), yakni suatu metode yang menempatkan hukum sebagai sistem norma yang dikaji secara mendalam melalui bahan-bahan kepustakaan (Diantha, 2016). Metode ini dipilih karena permasalahan yang diteliti bersifat yuridis, yaitu berkaitan dengan pengaturan dan implementasi Pelindungan hak privasi dalam komunikasi digital berdasarkan regulasi yang berlaku di Indonesia (Djulaeka & Rahayu, 2020). Penelitian hukum normatif pada dasarnya mengkaji hukum yang dikonsepkan sebagai norma atau kaidah yang menjadi acuan perilaku manusia, sehingga penelitian ini berfokus pada analisis substansi peraturan perundang-undangan, asas hukum, dan doktrin yang relevan (Widiarty, 2024). Pendekatan ini dianggap paling tepat untuk menjawab rumusan masalah yang bersifat preskriptif, yakni

memberikan penilaian dan rekomendasi terhadap kualitas norma hukum yang mengatur Pelindungan data pribadi di Indonesia.

Pendekatan yang Digunakan

Dalam penelitian ini digunakan tiga pendekatan utama yang saling melengkapi. Pertama, *statute approach* atau pendekatan perundang-undangan, yaitu dengan menelaah seluruh regulasi yang berkaitan dengan objek penelitian, meliputi Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dan Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Kedua, *conceptual approach* atau pendekatan konseptual, yang merujuk pada pandangan-pandangan dan doktrin-doktrin yang berkembang dalam ilmu hukum untuk membangun argumentasi hukum yang koheren dan sistematis. Ketiga, *comparative approach* atau pendekatan perbandingan hukum, yakni membandingkan ketentuan hukum Pelindungan data pribadi di Indonesia dengan regulasi sejenis di negara lain sebagai bahan perbandingan dalam rangka memperkaya analisis.

Sumber dan Bahan Hukum

Bahan hukum yang digunakan dalam penelitian ini terdiri atas tiga lapisan. Bahan hukum primer mencakup seluruh peraturan perundang-undangan yang berlaku dan memiliki keterkaitan langsung dengan tema penelitian, termasuk konstitusi, undang-undang, peraturan pemerintah, serta putusan pengadilan yang relevan (Sukmawan & Damayanti, 2025). Bahan hukum sekunder meliputi literatur ilmiah berupa buku teks hukum, artikel jurnal nasional dan internasional, hasil penelitian terdahulu, serta karya ilmiah lainnya yang membahas isu Pelindungan data pribadi dan privasi digital. Adapun bahan hukum tersier terdiri dari kamus hukum, ensiklopedia, dan berbagai sumber pendukung lainnya yang berfungsi untuk memperjelas konsep-konsep yang digunakan dalam penelitian ini (Karunia & Jamin, 2023). Penggunaan tiga lapisan bahan hukum tersebut dimaksudkan agar analisis yang dihasilkan bersifat komprehensif dan dapat dipertanggungjawabkan secara akademis.

Teknik Pengumpulan dan Analisis Bahan Hukum

Pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*) dengan cara mengidentifikasi, menginventarisasi, dan mengklasifikasikan bahan-bahan hukum yang relevan sesuai dengan permasalahan penelitian. Seluruh bahan hukum yang terkumpul kemudian dianalisis menggunakan metode analisis kualitatif yang bersifat preskriptif-analitis. Metode preskriptif digunakan untuk memberikan penilaian atas norma-norma hukum yang ada, sedangkan pendekatan analitis digunakan untuk menguraikan hubungan antara norma, fakta yuridis, dan tujuan hukum yang hendak dicapai (Sukmawan & Damayanti, 2025). Interpretasi hukum dilakukan melalui beberapa teknik, meliputi interpretasi gramatikal, sistematis, dan teleologis guna memperoleh pemahaman yang utuh terhadap maksud dan tujuan pembentuk undang-undang (Wiraguna, 2024). Dengan demikian, simpulan yang dihasilkan bukan sekadar deskripsi norma, melainkan

suatu konstruksi argumentatif yang mampu memberikan kontribusi nyata bagi pengembangan hukum Pelindungan data pribadi di Indonesia.

HASIL DAN PEMBAHASAN

Pengaturan Hukum Pelindungan Hak Privasi dalam Komunikasi Digital Menurut UU PDP

1. Landasan Konstitusional dan Filosofis Hak Privasi di Indonesia

Hak atas Pelindungan privasi pada dasarnya telah tertanam dalam konstruksi konstitusional Indonesia jauh sebelum era digital berkembang pesat. Pasal 28G ayat (1) UUD 1945 secara eksplisit menjamin hak setiap individu atas Pelindungan diri pribadi, kehormatan, martabat, serta rasa aman dari berbagai bentuk ancaman. Jaminan konstitusional ini menjadi fondasi normatif yang kemudian berkembang dalam rezim hukum Pelindungan data pribadi yang lebih spesifik. Transformasi dari *privacy* sebagai hak umum menuju *data privacy* sebagai hak yang terukur dan dapat ditegakkan secara hukum merupakan cerminan dari pergeseran paradigma dari *privacy as secrecy* menjadi *privacy as control*, yakni hak individu untuk mengendalikan data pribadinya secara aktif dalam ekosistem digital (Suvil et al., 2024).

Sebelum lahirnya UU PDP, Pelindungan privasi di Indonesia bersifat sektoral dan tersebar dalam berbagai regulasi parsial, sehingga menciptakan kesenjangan Pelindungan yang signifikan. Tidak adanya *single comprehensive framework* menjadikan data pribadi warga negara rentan tereksploitasi, baik oleh aktor privat maupun entitas publik. Kondisi ini mendorong urgensi pembentukan regulasi khusus yang mampu menjawab tantangan digital secara menyeluruh. Kehadiran UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) kemudian menjadi tonggak historis dalam pembangunan sistem hukum digital nasional, sebab untuk pertama kalinya Indonesia memiliki instrumen hukum yang secara komprehensif mengakui dan melindungi hak privasi sebagai bagian integral dari hak asasi manusia (Andika et al., 2026; Saly et al., 2023).

Konstruksi hak privasi dalam sistem hukum Indonesia tidak dapat dilepaskan dari perkembangan pemikiran hak asasi manusia secara global. Deklarasi Universal Hak Asasi Manusia (DUHAM) Pasal 12 menegaskan bahwa tidak seorang pun boleh diganggu secara sewenang-wenang dalam urusan pribadinya, keluarganya, rumah tangganya, maupun korespondensinya. Norma internasional ini kemudian menjadi referensi penting dalam pembangunan sistem hukum privasi di Indonesia, khususnya dalam mengisi kekosongan normatif yang selama ini terjadi. Sebelum UU PDP lahir, Pelindungan data pribadi hanya tersebar secara fragmentatif dalam berbagai regulasi sektoral seperti Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 serta ketentuan Pelindungan konsumen, yang jelas tidak memadai untuk menjawab kompleksitas ancaman privasi digital yang terus berkembang. Ketidakmemadaian kerangka regulasi tersebut tercermin dari maraknya penyalahgunaan data yang terjadi tanpa ada instrumen hukum yang cukup kuat untuk menindaknya secara efektif.

Dimensi filosofis Pelindungan privasi juga berkembang melampaui sekadar Pelindungan terhadap intervensi fisik. Dalam tradisi hukum modern, privasi

dipahami sebagai prasyarat bagi terwujudnya otonomi individu, martabat manusia, serta kebebasan berekspresi. Ketika data pribadi seseorang bocor atau disalahgunakan, dampaknya tidak hanya bersifat materiel, tetapi juga menyentuh dimensi psikologis dan sosial yang mendalam, mulai dari hilangnya kepercayaan diri hingga risiko diskriminasi berbasis data (Arndarnijariah & Kameo, 2024). Karena itu Pelindungan privasi harus dipahami bukan sekadar kewajiban hukum formal, melainkan sebagai komitmen etis negara terhadap martabat setiap warga negaranya dalam ruang digital yang semakin dominan dalam kehidupan sehari-hari.

2. Substansi dan Ruang Lingkup UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

UU PDP menghadirkan arsitektur hukum yang sistematis dan berlapis dalam mengatur Pelindungan data pribadi. Pasal 1 angka 1 mendefinisikan data pribadi sebagai data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi, baik secara langsung maupun tidak langsung. Ruang lingkup ini mencakup seluruh siklus pemrosesan data, mulai dari pengumpulan, penyimpanan, penggunaan, hingga penghapusan. Pasal 4 ayat (1) kemudian membedakan antara *data pribadi umum* dan *data pribadi spesifik* yang mencakup data kesehatan, biometrik, dan genetika kategori yang memiliki risiko penyalahgunaan lebih tinggi sehingga memerlukan Pelindungan yang lebih ketat. Pembedaan kategorikal ini mencerminkan pendekatan berbasis risiko (*risk-based approach*) yang juga diadopsi oleh rezim Pelindungan data internasional seperti *General Data Protection Regulation* (GDPR) Uni Eropa (Buckley et al., 2024).

Hak-hak *subjek data* diatur secara komprehensif dalam Pasal 5 hingga Pasal 13, yang meliputi hak atas informasi, hak akses, hak koreksi, *right to erasure*, hak menarik persetujuan, hingga hak portabilitas data. Di sisi lain, Pasal 20 menetapkan bahwa setiap pemrosesan data pribadi harus memiliki dasar hukum yang sah, dengan *consent* eksplisit sebagai salah satu dasar utamanya. Kewajiban *pengendali data* dan *prosesor data* untuk menerapkan prinsip *purpose limitation*, *data minimization*, serta keamanan data secara teknis juga dijabarkan secara rinci. Dalam konteks komunikasi digital, ketentuan ini sangat relevan mengingat setiap interaksi pada platform digital mulai dari media sosial hingga aplikasi pesan selalu melibatkan pemrosesan data pribadi pengguna secara masif dan real-time (Aulia & Umboh, 2025).

Salah satu keunggulan normatif UU PDP dibandingkan regulasi sebelumnya adalah diintroduksinya konsep *data protection by design and by default*, yang mewajibkan pengendali data untuk merancang sistem pemrosesan data dengan mempertimbangkan Pelindungan privasi sejak tahap awal pembangunan sistem, bukan sebagai tambahan pelengkap. Pendekatan ini mencerminkan adopsi standar internasional yang progresif dan menempatkan Indonesia sejajar dengan praktik terbaik Pelindungan data global. Selain itu, ketentuan mengenai *Data Protection Officer* (DPO) yang diwajibkan bagi pengendali data dengan skala pemrosesan tertentu juga menjadi instrumen penting dalam memastikan akuntabilitas internal organisasi terhadap kepatuhan Pelindungan data (Azzahra et al., 2025).

Dalam konteks komunikasi digital, ketentuan UU PDP juga relevan terhadap praktik *profiling* dan pengambilan keputusan otomatis berbasis data pengguna yang semakin lazim dilakukan oleh platform digital. Pasal 10 ayat (1) UU PDP mengatur hak subjek data untuk tidak menjadi objek pengambilan keputusan yang semata-mata didasarkan pada pemrosesan otomatis, termasuk *profiling*, yang menimbulkan akibat hukum atau dampak signifikan terhadap dirinya. Ketentuan ini sangat strategis mengingat praktik iklan bertarget, penilaian kredit otomatis, dan seleksi algoritmik telah menjadi bagian integral dari ekosistem digital yang bersentuhan langsung dengan hak-hak dasar individu. Pengaturan ini membuktikan bahwa UU PDP tidak hanya mengatur aspek teknis pemrosesan data, tetapi juga menjangkau dimensi keadilan algoritmik yang lebih substantive (Azzahra et al., 2025).

3. Keterkaitan UU PDP dengan UU ITE dalam Pelindungan Privasi Digital

Relasi antara UU PDP dan UU ITE bersifat komplementer namun tidak sepenuhnya harmonis. UU Nomor 11 Tahun 2008 jo. UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik berfungsi sebagai *lex generalis* yang mengatur aspek luas teknologi informasi, sementara UU PDP hadir sebagai *lex specialis* yang secara eksklusif mengatur siklus hidup data pribadi. Pasal 26 ayat (1) UU ITE telah memberikan pengakuan awal terhadap prinsip *consent* dengan menyatakan bahwa penggunaan data pribadi melalui media elektronik harus dilakukan atas persetujuan pemiliknya. Norma ini menjadi embrio yang kemudian dikembangkan lebih lanjut dalam UU PDP menjadi sistem Pelindungan yang jauh lebih komprehensif dan operasional (Jauhari & Simangunsong, 2026; Suari & Sarjana, 2023)

Terdapat sejumlah *legal gap* yang masih perlu diperhatikan. Inkonsistensi substantif antara Pasal 67 UU PDP dan Pasal 48 UU ITE mengenai ketentuan pelanggaran data pribadi menciptakan ambiguitas hukum yang berpotensi menghasilkan putusan yang tidak konsisten dalam praktik penegakan hukum. Selain itu, mekanisme penegakan sanksi antara kedua undang-undang ini belum sepenuhnya terharmonisasi, khususnya dalam hal alur penanganan kasus *data breach* dan prosedur ganti kerugian bagi subjek data. Kondisi tumpang tindih norma ini memperbesar celah bagi pelaku pelanggaran untuk mengelak dari pertanggungjawaban hukum yang semestinya (Saly et al., 2023).

Dalam perspektif hierarki norma, relasi antara UU PDP dan UU ITE perlu dikonstruksi secara cermat agar tidak menimbulkan konflik penerapan hukum di lapangan. Asas *lex specialis derogat legi generali* memang memberikan UU PDP kedudukan yang lebih kuat dalam mengatur Pelindungan data pribadi secara spesifik, namun penerapan asas ini tidak bersifat otomatis menggantikan seluruh ketentuan UU ITE yang relevan. Terdapat sejumlah ketentuan dalam UU ITE yang masih berlaku secara komplementer, khususnya yang berkaitan dengan tindak pidana siber seperti akses ilegal dan intersepsi data, yang tidak secara eksplisit diatur dalam UU PDP. Kondisi ini menuntut adanya mekanisme interpretasi hukum yang konsisten dari aparat penegak hukum agar tidak terjadi kevakuman dalam penanganan kasus-kasus pelanggaran privasi digital (Gustryan & Hoesein, 2025).

Persoalan *cross-border data transfer* juga menjadi salah satu celah hukum paling krusial yang belum terjembatani secara memadai antara UU PDP dan UU ITE. Komunikasi digital pada dasarnya tidak mengenal batas yurisdiksi, sehingga data warga negara Indonesia kerap mengalir ke server yang berlokasi di luar negeri tanpa pengawasan yang memadai. UU PDP sebenarnya telah mengatur ketentuan transfer data lintas negara, namun mekanisme implementasinya masih memerlukan perjanjian bilateral maupun standar teknis yang belum seluruhnya terwujud. Kekosongan pengaturan teknis ini menjadi kerentanan serius yang harus segera diatasi melalui harmonisasi regulasi yang lebih komprehensif dan koordinasi internasional yang lebih aktif (Nafisa et al., 2025).

Implementasi dan Efektivitas Pelindungan Hak Privasi dalam Komunikasi Digital Berdasarkan UU PDP

1. Mekanisme Pelindungan Data Pribadi dalam Praktik Komunikasi Digital

Implementasi Pelindungan data pribadi dalam ekosistem komunikasi digital bertumpu pada sejumlah mekanisme kunci yang diatur dalam UU PDP. Kewajiban memperoleh persetujuan eksplisit dari pengguna sebelum pemrosesan data sebagaimana diatur dalam Pasal 20 ayat (2) dan Pasal 22 ayat (1) menjadi garis pertahanan pertama dalam Pelindungan privasi digital. Lebih lanjut, prinsip *data minimization* dan *purpose limitation* yang termuat dalam Pasal 16 ayat (2) mengharuskan penyelenggara sistem elektronik untuk tidak mengumpulkan data melebihi kebutuhan dan hanya menggunakannya sesuai tujuan yang telah dinyatakan secara transparan kepada pengguna. Dalam praktiknya, implementasi prinsip-prinsip ini masih menghadapi tantangan serius karena banyak penyelenggara platform digital yang menerapkan mekanisme *consent* secara formalistik melalui dokumen *terms and conditions* yang panjang dan sulit dipahami oleh pengguna awam (Simanjuntak et al., 2026).

Mekanisme *right to be forgotten* yang diatur dalam Pasal 43 ayat (1) UU PDP juga menjadi instrumen penting dalam Pelindungan privasi digital, namun penerapannya masih belum optimal. Kewajiban pengendali data untuk menghapus data yang tidak lagi diperlukan atau atas permintaan subjek data secara konkret kerap terhambat oleh kendala teknis maupun ketidakjelasan prosedur yang berlaku. Lebih lanjut, kewajiban pelaporan kebocoran data (*data breach notification*) dalam waktu paling lambat 3×24 jam kepada subjek data dan lembaga pengawas sebagaimana diatur Pasal 46 ayat (1) juga belum dipatuhi secara konsisten oleh penyelenggara sistem elektronik. Rendahnya kepatuhan ini mencerminkan bahwa norma hukum yang baik di atas kertas belum tentu berhasil diterapkan secara efektif di lapangan tanpa disertai mekanisme pengawasan yang kuat (Jauhari & Simangunsong, 2026).

Salah satu tantangan terbesar dalam implementasi mekanisme *consent* dalam komunikasi digital adalah fenomena *consent fatigue*, yakni kondisi di mana pengguna secara refleks menyetujui seluruh ketentuan layanan tanpa memahami implikasinya karena terlalu sering dihadapkan pada formulir persetujuan yang panjang dan teknis. Kondisi ini secara substantif melemahkan validitas *consent* sebagai dasar hukum pemrosesan data, karena persetujuan yang diberikan tidak

mencerminkan kehendak bebas yang sesungguhnya dari subjek data. UU PDP memang mensyaratkan persetujuan yang diberikan secara eksplisit, namun belum mengatur secara rinci standar keterbacaan dan aksesibilitas dokumen persetujuan yang harus dipenuhi oleh penyelenggara layanan digital, sehingga ruang untuk eksploitasi formal tetap terbuka.

Lebih jauh, mekanisme Pelindungan data dalam komunikasi digital juga harus mempertimbangkan kelompok pengguna yang rentan, seperti anak-anak dan lansia, yang memiliki kemampuan literasi digital terbatas. UU PDP memang mengatur Pelindungan khusus terhadap pemrosesan data anak di bawah umur, namun mekanisme verifikasi usia yang efektif di platform digital masih menjadi persoalan teknis yang belum terpecahkan secara sistematis. Tanpa mekanisme verifikasi yang andal, ketentuan Pelindungan data anak hanya akan bersifat normatif tanpa implementasi yang nyata. Hal ini menunjukkan bahwa efektivitas Pelindungan privasi dalam komunikasi digital sangat bergantung pada kemampuan teknis penyelenggara sistem elektronik dalam mengimplementasikan standar Pelindungan yang ditetapkan regulasi.

2. Peran dan Kewenangan Lembaga Pengawas Pelindungan Data Pribadi

UU PDP mengamanatkan pembentukan lembaga pengawas independen melalui Pasal 58, yang bertanggung jawab langsung kepada Presiden. Lembaga ini diberikan kewenangan luas meliputi pengawasan kepatuhan, penegakan sanksi administratif, penyelesaian sengketa, serta investigasi pelanggaran sebagaimana tertuang dalam Pasal 59 dan Pasal 60 huruf c. Secara normatif, desain kelembagaan ini cukup memadai; namun dalam tataran implementasi, keberadaan lembaga yang berada langsung di bawah Presiden menimbulkan kekhawatiran mengenai independensinya dalam menangani kasus-kasus yang melibatkan instansi pemerintah. Bila dibandingkan dengan *Data Protection Authority* dalam rezim GDPR Uni Eropa yang dirancang secara ketat sebagai lembaga independen dengan kewenangan sanksi denda yang signifikan, kapasitas kelembagaan pengawas data di Indonesia masih memerlukan penguatan sistemik yang substansial (Prastyanti, 2025).

Kesiapan kelembagaan pengawas Pelindungan data pribadi di Indonesia juga perlu diukur dari aspek kapasitas sumber daya manusia dan infrastruktur teknologi yang dimiliki. Pengawasan terhadap pemrosesan data dalam skala masif oleh platform digital raksasa membutuhkan tenaga ahli yang tidak hanya menguasai aspek hukum, tetapi juga memiliki kompetensi teknis di bidang keamanan siber, forensik digital, dan analisis algoritma. Tanpa kapasitas teknis yang memadai, fungsi pengawasan lembaga tersebut akan terbatas pada pemeriksaan dokumen formal semata dan tidak mampu mendeteksi pelanggaran yang bersifat teknis dan tersembunyi di balik sistem pemrosesan data yang kompleks.

3. Studi Kasus Pelanggaran Privasi Digital di Indonesia Pasca UU PDP

Berbagai insiden kebocoran data yang terjadi pasca pengesahan UU PDP menunjukkan bahwa tantangan implementasi regulasi ini masih sangat nyata. Kasus-kasus kebocoran data pada penyelenggara layanan digital dan instansi

pemerintah dapat dikategorikan sebagai pelanggaran kewajiban pengendali data berdasarkan Pasal 30, 31, dan 32 UU ITE, sekaligus pelanggaran terhadap kewajiban keamanan data dalam UU PDP. Namun, efektivitas respons hukum terhadap kasus-kasus ini masih sangat terbatas akibat minimnya koordinasi antar lembaga penegak hukum dan lemahnya mekanisme pembuktian digital. Kondisi ini mengonfirmasi bahwa keberadaan regulasi yang komprehensif saja tidak cukup tanpa ekosistem penegakan hukum yang mendukung secara menyeluruh (Suari & Sarjana, 2023).

Analisis yuridis terhadap kasus-kasus kebocoran data di Indonesia mengungkapkan pola yang konsisten, yakni lemahnya sistem keamanan teknis, absennya prosedur *incident response* yang terstandar, serta tidak adanya mekanisme pertanggungjawaban yang jelas kepada subjek data yang dirugikan. Dalam perspektif UU PDP, kegagalan pengendali data untuk menerapkan langkah-langkah keamanan yang proporsional terhadap risiko pemrosesan dapat dikategorikan sebagai kelalaian yang menimbulkan kewajiban ganti kerugian. Namun dalam praktik, pembuktian hubungan kausalitas antara kelalaian pengendali data dengan kerugian yang dialami subjek data masih menjadi tantangan hukum tersendiri yang membutuhkan pengembangan yurisprudensi lebih lanjut.

Di sisi lain, respons korektif yang dilakukan oleh perusahaan setelah terjadinya kebocoran data seringkali bersifat defensif dan tidak memadai. Praktik menutup-nutupi insiden kebocoran data atau memberikan informasi yang tidak lengkap kepada pengguna yang terdampak bertentangan secara langsung dengan prinsip transparansi dan kewajiban notifikasi yang diatur dalam UU PDP. Penegakan kewajiban ini memerlukan mekanisme pelaporan yang terstandar dan terintegrasi antara pengendali data, lembaga pengawas, serta aparat penegak hukum, sehingga seluruh rantai penanganan insiden kebocoran data dapat berjalan secara cepat, transparan, dan akuntabel demi pemulihan hak subjek data yang terdampak.

Hambatan, Tantangan, dan Rekomendasi Hukum Pelindungan Hak Privasi dalam Komunikasi Digital

1. Hambatan Yuridis dalam Penegakan UU PDP

Implementasi UU PDP menghadapi sejumlah hambatan yuridis yang bersifat struktural. Belum lengkapnya peraturan pelaksana menjadikan banyak ketentuan UU PDP belum dapat dioperasionalkan secara penuh di lapangan. Multitafsir norma pada beberapa pasal, dikombinasikan dengan ancaman sanksi pidana dalam Pasal 67 yang dinilai belum proporsional, menciptakan celah yang dimanfaatkan oleh pelanggar. Di samping itu, rendahnya *digital legal literacy* masyarakat menyebabkan banyak subjek data tidak memahami hak-hak yang dimilikinya, sehingga potensi pengaduan dan tuntutan hukum atas pelanggaran privasi jauh di bawah angka kejadian yang sesungguhnya (M. N. Huda & Kifli, 2024).

Hambatan yuridis dalam penegakan UU PDP juga bersumber dari belum terbangunnya yurisprudensi yang memadai di bidang hukum Pelindungan data pribadi di Indonesia. Minimnya putusan pengadilan yang secara khusus menganalisis dan menerapkan ketentuan UU PDP menciptakan ketidakpastian hukum bagi para penegak hukum, pengendali data, maupun subjek data dalam

memahami batas-batas kewajiban dan hak masing-masing. Pembangunan yurisprudensi yang konsisten membutuhkan waktu dan volume perkara yang memadai, sementara akses keadilan bagi korban pelanggaran privasi digital masih sangat terbatas akibat tingginya biaya litigasi dan rendahnya pemahaman masyarakat terhadap mekanisme hukum yang tersedia.

Persoalan beban pembuktian dalam sengketa Pelindungan data pribadi juga menjadi hambatan yuridis yang signifikan. Dalam konteks teknologi digital, data dan bukti elektronik memiliki karakteristik yang berbeda dengan bukti konvensional, sehingga membutuhkan standar pembuktian khusus yang belum sepenuhnya terakomodasi dalam hukum acara yang berlaku. Reformasi hukum acara yang mengakomodasi kekhasan pembuktian dalam sengketa digital menjadi kebutuhan mendesak agar mekanisme penegakan UU PDP dapat berjalan secara efektif dan tidak terhalang oleh keterbatasan prosedural yang bersifat teknis.

2. Tantangan Teknis dan Struktural Pelindungan Privasi Digital

Di luar dimensi yuridis, perkembangan teknologi *artificial intelligence*, *big data*, dan *surveillance technology* menghadirkan tantangan yang bergerak jauh lebih cepat dari kapasitas regulasi untuk meresponsnya. Pasal 10 ayat (1) UU PDP yang mengatur pemrosesan data secara otomatis belum mampu sepenuhnya mengantisipasi implikasi dari sistem pemrosesan data berbasis kecerdasan buatan yang kini semakin dominan dalam ekosistem komunikasi digital. Ketimpangan posisi tawar antara konsumen dan pelaku usaha digital yang memiliki kapasitas teknologi jauh lebih besar juga memperbesar kerentanan privasi pengguna secara struktural. Rendahnya literasi digital masyarakat memperparah kondisi ini, karena pengguna seringkali tidak menyadari bahwa data mereka sedang dikumpulkan dan diproses untuk kepentingan komersial dalam skala massif (U. N. Huda et al., 2024).

Teknologi *Internet of Things* (IoT) yang semakin merambah kehidupan sehari-hari juga menghadirkan dimensi baru dalam tantangan Pelindungan privasi digital. Perangkat rumah pintar, *wearable technology*, dan sistem transportasi cerdas secara terus-menerus mengumpulkan data pribadi penggunanya, bahkan tanpa interaksi aktif dari subjek data (Dhinakaran et al., 2025). Karakteristik pengumpulan data yang pasif dan tidak terasa ini sangat bertentangan dengan prinsip transparansi dan *consent* yang menjadi fondasi UU PDP . Regulasi yang ada saat ini belum secara spesifik mengatur standar Pelindungan data dalam konteks IoT, sehingga diperlukan peraturan pelaksana yang lebih teknis dan adaptif terhadap perkembangan ekosistem teknologi yang terus berevolusi dengan cepat.

Ancaman *deepfake* dan manipulasi data berbasis kecerdasan buatan generatif juga muncul sebagai tantangan baru yang belum diantisipasi secara memadai dalam kerangka regulasi Pelindungan privasi yang ada. Teknologi ini memungkinkan penciptaan konten palsu yang menggunakan identitas visual dan suara seseorang tanpa izin, yang berpotensi menimbulkan kerugian reputasional dan psikologis yang sangat serius. Celah regulasi dalam menghadapi ancaman ini perlu segera ditutup melalui adaptasi normatif yang responsif, baik melalui penerbitan peraturan pelaksana UU PDP yang spesifik maupun melalui penguatan ketentuan dalam revisi UU ITE ke depannya.

3. Rekomendasi Penguatan Hukum Pelindungan Hak Privasi di Indonesia

Berdasarkan analisis komprehensif di atas, beberapa rekomendasi konstruktif dapat dirumuskan. Pertama, harmonisasi substantif antara UU PDP dan UU ITE perlu segera dilakukan untuk menutup inkonsistensi norma yang ada, khususnya terkait ketentuan sanksi dan mekanisme penegakan hukum. Kedua, pembentukan lembaga pengawas Pelindungan data yang benar-benar independen dan memiliki kapasitas teknis serta anggaran memadai menjadi prasyarat mutlak efektivitas UU PDP. Ketiga, penguatan sanksi administratif melalui revisi Pasal 57 perlu dilakukan agar memiliki efek jera yang setara dengan standar internasional. Keempat, program edukasi *digital legal literacy* harus diintegrasikan ke dalam kebijakan nasional secara sistematis agar masyarakat mampu menjadi subjek hukum yang aktif dalam melindungi data pribadinya. Kelima, adaptasi regulasi terhadap perkembangan teknologi AI dan *big data* perlu dilakukan secara berkala melalui mekanisme revisi regulasi yang responsif dan partisipatif (Asherli & Wiraguna, 2025).

Penguatan Pelindungan hak privasi dalam komunikasi digital juga memerlukan pendekatan multistakeholder yang melibatkan tidak hanya pemerintah dan industri, tetapi juga masyarakat sipil dan komunitas akademik secara aktif. Model tata kelola data yang partisipatif terbukti lebih efektif dalam menghasilkan regulasi yang relevan, adaptif, dan mendapat kepercayaan publik. Indonesia dapat belajar dari pengalaman negara-negara seperti Jepang dan Korea Selatan yang berhasil membangun ekosistem Pelindungan data yang kuat melalui kombinasi antara regulasi yang tegas, edukasi publik yang masif, dan kerja sama erat antara pemerintah dengan industri teknologi.

Selain itu pembangunan infrastruktur keamanan siber nasional yang andal juga merupakan prasyarat teknis yang tidak dapat diabaikan dalam upaya Pelindungan privasi digital secara menyeluruh. Badan Siber dan Sandi Negara (BSSN) perlu diperkuat kapasitasnya agar mampu memberikan dukungan teknis yang efektif kepada lembaga pengawas Pelindungan data dan penyelenggara sistem elektronik dalam mengimplementasikan standar keamanan yang ditetapkan UU PDP. Sinergi kelembagaan yang kuat antara BSSN, lembaga pengawas Pelindungan data, Kementerian Komunikasi dan Digital, serta aparat penegak hukum menjadi arsitektur kelembagaan yang mutlak diperlukan demi terwujudnya ekosistem digital Indonesia yang benar-benar aman, terpercaya, dan menghormati hak privasi setiap warganya.

SIMPULAN

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi merupakan lompatan besar dalam tata kelola hukum digital Indonesia, sebab untuk pertama kalinya negara hadir secara komprehensif melindungi *right to privacy* warga negaranya di ruang digital. Regulasi ini mengatur secara rinci hak-hak *subject data*, kewajiban *data controller*, prinsip *data minimization*, hingga mekanisme *right to be forgotten*. Namun efektivitasnya masih terkendala oleh belum terbentuk secara operasional dan independen, rendahnya literasi hukum digital masyarakat, serta celah harmonisasi antara UU PDP dan UU *Informasi dan Transaksi Elektronik* yang menciptakan ketidakpastian dalam penegakan hukum di lapangan.

Penguatan Pelindungan privasi digital di Indonesia memerlukan langkah nyata yang melampaui sekadar pembenahan teks regulasi. Pemerintah perlu segera membentuk lembaga pengawas *data protection* yang benar-benar independen dan dilengkapi kapasitas teknis memadai, sekaligus menyelaraskan ketentuan UU PDP dengan UU *Informasi dan Transaksi Elektronik* guna menutup celah norma yang ada. Program edukasi *digital legal literacy* harus dirancang secara nasional agar masyarakat memahami hak-haknya sebagai *subject data*. Selain itu regulasi perlu diperbarui secara berkala agar mampu merespons perkembangan teknologi *artificial intelligence* dan *Internet of Things* yang terus bergerak melampaui batas kemampuan hukum konvensional.

DAFTAR RUJUKAN

Andika, F., Rasmuddin, & Hamzah, I. F. (2026). Perlindungan Hukum Terhadap Data Pribadi Dalam Era Digital. *Unes Journal of Swara Justisia*, *9*(4), 825–832. https://doi.org/10.31933/ysc6n689

Arndarnijariah, F. R., & Kameo, J. (2024). The Right to Be Forgotten Sebagai Hukum Perlindungan Data Pribadi Korban Revenge Porn. *Jurnal Ilmu Hukum: ALETHEA*, *8*(1), 69–82. https://doi.org/10.24246/alethea.vol8.no1.p69-82

Asherli, B. F., & Wiraguna, S. A. (2025). Perlindungan Keamanan Data Pribadi di Era Digital Menghadapi Serangan Phishing Ditinjau dari Undang-Undang Pelindungan Data Pribadi Nomor 27 Tahun 2022. *Jurnal Hukum, Administrasi Publik Dan Negara*, *2*(4), 01–14. https://doi.org/10.62383/hukum.v2i4.290

Aulia, H., & Umboh, N. K. (2025). Kajian Anlisis Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadipada Sektor Keuangan. *Jurnal Intelek Dan Cendikiawan Nusantara*, *2*(4), 4808–4816.

Azzahra, A., Rizky, A. M., Muharrom, N. W., Basuki, R. M., Angelica, D., & Hadji, K. (2025). Analisis Asas Pembentukan UU Perlindungan Data Pribadi dalam Menjamin Hak Privasi Warga Negara. *IKRA-ITH HUMANIORA : Jurnal Sosial Dan Humaniora*, *9*(3), 1235–1246.

Bahram, M. (2023). Transformasi Masyarakat Di Era Digital: Menjaga Kaidah Hukum Sebagai Landasan Utama. *SENTRI: Jurnal Riset Ilmiah*, *2*(5), 1733–1746. https://doi.org/10.55681/sentri.v2i5.884

Buckley, G., Caulfield, T., & Becker, I. (2024). GDPR and the indefinable effectiveness of privacy regulators: Can performance assessment be improved? *Journal of Cybersecurity*, *10*(1), tyae017. https://doi.org/10.1093/cybsec/tyae017

DataReportal. (2025, February 5). *Digital 2025: Global Overview Report*. DataReportal – Global Digital Insights. https://datareportal.com/reports/digital-2025-global-overview-report

Dhinakaran, D., Edwin Raja, S., Ramathilagam, A., Vennila, G., & Alagulakshmi, A. (2025). Ethical and legal challenges with IoT in home digital twins. *MethodsX*, *14*, 103409. https://doi.org/10.1016/j.mex.2025.103409

Diantha, M. P. (2016). *Metodologi Penelitian Hukum Normatif dalam Justifikasi Teori Hukum*. Prenada Media.

Djulaeka, & Rahayu, D. (2020). *Metode Penelitian Hukum*. Scopindo Media Pustaka.

Gustryan, M., & Hoesein, Z. A. (2025). Peran Undang-Undang ITE dan Undang-Undang Perlindungan Data Pribadi dalam Perlindungan Data dan Privasi di Era Ekonomi Digital. *Jurnal Minfo Polgan*, *14*(2), 3333–3343. https://doi.org/10.33395/jmp.v14i2.15746

Huda, M. N., & Kifli, Z. (2024). Perlindungan Hukum Data Pribadi Dalam Keilmuan Multi Disipliner. *Desiderata Law Review*, *1*(2), 44–58. https://doi.org/10.25299/dlr.2024.19592

Huda, U. N., Astaruddin, T., Nasution, M. I., Haddad, A. A., & Gumelar, D. R. (2024). *Data Pribadi, Hak Warga, dan Negara Hukum: Menjaga Privasi di Tengah Ancaman Digital*. CV Widina Media Utama.

Jauhari, A. A. A., & Simangunsong, F. (2026). Perlindungan hukum terhadap data pribadi pengguna platform digital dalam persfektif kepastian hukum. *Journal Equitable*, *11*(1), 44–74. https://doi.org/10.37859/jeq.v11i1.9798

Judijanto, L., Lubis, A. F., Karauwan, D. E. S., Bungin, S. S., & Mau, H. A. (2024). Efektivitas Kebijakan Perlindungan Data Pribadi dalam Menjaga Hak Asasi Manusia di Era Teknologi di Indonesia. *Sanskara Hukum dan HAM*, *3*(01), 34–42. https://doi.org/10.58812/shh.v3i01.445

Karunia, A. A., & Jamin, M. (2023). Perlindungan Hukum Kepemilikan Data Kependudukan di Indonesia Dalam Perspektif Teori Pembentukan Peraturan Perundang-Undangan. *KRTHA BHAYANGKARA*, *17*(2), 217–234. https://doi.org/10.31599/krtha.v17i2.796

Nafisa, T. A., Alam, M. Z., & Maharani, D. P. (2025). Analisis pengaturan pengalihan data pribadi lintas negara pasca akuisisi dalam Undang-Undang Perlindungan Data Pribadi. *Jurnal Dialektika Hukum*, *7*(1), 97–135. https://doi.org/10.36859/jdh.v7i1.3548

Prastyanti, R. A. (2025). *Monograf Perlindungan Data Pribadi Konsumen Pengguna Transaksi Elektronik*. Penerbit NEM.

Saly, J. N., Artamevia, H., Kheista, K., Gulo, B. J. S., Rhemrev, E. A., & Christie, M. (2023). Analisis Perlindungan Data Pribadi Terkait UU No.27 Tahun 2022. *Jurnal Serina Sosial Humaniora*, *1*(3), 145–153.

Seftiyana, H., Ansorullah, & Muhammad. (2026). Perlindungan Hukum Terhadap Data Pribadi: Menjamin Hak Warga Negara Dalam Perspektif Peraturan Perundang-Undangan. *Limbago: Journal of Constitutional Law*, *6*(1), 151–171. https://doi.org/10.22437/limbago.v6i1.52847

Simanjuntak, F. A., Anjawai, N. B., Permatasari, R., & Rachmadhanto, D. A. S. (2026). Penyalahgunaan Data Pribadi Konsumen dalam Perjanjian Digital Berdasarkan KUHPerdata dan Undang-Undang Perlindungan Data Pribadi. *Jurnal Alwatzikhoebillah : Kajian Islam, Pendidikan, Ekonomi, Humaniora*, *12*(1), 578–590. https://doi.org/10.37567/alwatzikhoebillah.v12i1.5135

Suari, K. R. A., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132–142. https://doi.org/10.38043/jah.v6i1.4484

Sukmawan, Y. A., & Damayanti, D. (2025). Metode Penelitian Hukum Normatif dan Empiris sebagai Strategi Penguatan Perspektif Kajian Ilmu Hukum. *Notary Law Journal*, *4*(3), 114–128. https://doi.org/10.32801/nolaj.v4i3.116

Suvil, A. A., Firdaus, F., Ramadhan, M. A., Putra, W. D., & Lestarika, D. P. (2024). Implementasi Perlindungan Data Pribadi Berdasarkan Undang-Undang Nomor 11 Tahun 2020. *Jurnal Hukum, Politik dan Ilmu Sosial*, *3*(4), 70–80. https://doi.org/10.55606/jhpis.v3i4.4235

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Widiarty, W. S. (2024). *Buku Ajar Metode Penelitian Hukum* (M. Tajuddin, Ed.). Publika Global Media.

Wiraguna, S. A. (2024). Metode Normatif dan Empiris dalam Penelitian Hukum: Studi Eksploratif di Indonesia. *Public Sphere: Jurnal Sosial Politik, Pemerintahan Dan Hukum*, *3*(3). https://doi.org/10.59818/jps.v3i3.1390

Wiraguna, S. A., & Barthos, M. (2025). *Hukum Privasi dan Pelindungan Data Pribadi di Indonesia*. CV Widina Media Utama. https://repository.penerbitwidina.com/publications/631846/

Zakiya, H. H., & Farhah, S. F. (2026). Analisis Kebocoran Data Pengguna Tokopedia dan Implikasinya Terhadap Keamanan Siber Indonesia. *SHARE: Sharia Economic Review*, *3*(1). https://journal.stai-almujtama.ac.id/index.php/share/article/view/192