



**URGENSI PERLINDUNGAN DATA PRIBADI DALAM ERA DIGITAL: ANALISIS  
UNDANG-UNDANG NOMOR 27 TAHUN 2022**

**Asep Mahbub Junaedi**

Hukum Keluarga Islam Pasca Sarjana UIN Syekh Nurjati Cirebon

Email: amjunaedi58@gmail.com

**ABSTRAK**

Perkembangan teknologi digital telah meningkatkan risiko terhadap perlindungan data pribadi, terutama dengan semakin masifnya pengumpulan dan pemrosesan informasi individu oleh berbagai pihak. Kebocoran data, penyalahgunaan informasi, dan pelanggaran privasi menjadi ancaman serius bagi masyarakat dalam era digital. Untuk menjawab tantangan ini, Indonesia mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi sebagai upaya memperkuat regulasi dan menjamin hak privasi warga negara. Penelitian ini bertujuan untuk menganalisis urgensi perlindungan data pribadi serta mengevaluasi efektivitas undang-undang tersebut dalam menutup kesenjangan antara teori perlindungan privasi dan praktik di lapangan. Dengan pendekatan normatif, penelitian ini mengkaji prinsip-prinsip yang mendasari regulasi perlindungan data serta implikasi kebijakan bagi individu, perusahaan, dan pemerintah. Hasil analisis menunjukkan bahwa meskipun undang-undang ini telah menetapkan kerangka hukum yang lebih jelas, tantangan masih muncul dalam aspek penegakan hukum, pengawasan terhadap pemrosesan data, serta peningkatan kesadaran masyarakat. Oleh karena itu, diperlukan upaya kolaboratif dari berbagai pihak guna memastikan implementasi undang-undang ini berjalan efektif dan mampu menjamin hak privasi setiap individu di era digital.

**Kata Kunci:** *Perlindungan Data Pribadi, Privasi Digital, Kebocoran Data, Regulasi Data, Undang-Undang Nomor 27 Tahun 2022, Keamanan Informasi, Hak Privasi.*

**ABSTRACT**

The development of digital technology has increased the risks to personal data protection, especially with the massive collection and processing of individual information by various parties. Data breaches, misuse of information, and privacy violations have become serious threats to society in the digital era. To address these challenges, Indonesia enacted Law Number 27 of 2022 on Personal Data Protection as an effort to strengthen regulation and guarantee citizens' privacy rights. This study aims to analyze the urgency of personal data protection and evaluate the effectiveness of the law in bridging the gap between privacy protection theory and real-world practices. Using a normative approach, this research examines the principles underlying data protection regulation and the policy implications for individuals, companies, and the government. The analysis shows that although the law has established a clearer legal framework, challenges persist in law enforcement, oversight of data processing, and raising public awareness. Therefore, collaborative efforts from various stakeholders are needed to ensure that the implementation of this law is effective and capable of safeguarding the privacy rights of every individual in the digital era.

**Keywords:** *Personal Data Protection, Digital Privacy, Data Breach, Data Regulation, Law Number 27 of 2022, Information Security, Privacy Rights.*

**PENDAHULUAN**

Perkembangan teknologi digital telah membawa perubahan signifikan dalam berbagai aspek kehidupan manusia, termasuk dalam pengelolaan dan pemanfaatan data pribadi. Di era digital saat ini, data pribadi menjadi aset berharga yang sering digunakan untuk kepentingan ekonomi, bisnis, dan pemerintahan. Namun, di balik manfaatnya, muncul berbagai tantangan



terkait perlindungan data pribadi yang mengancam hak privasi individu. Kasus kebocoran data semakin marak terjadi, menimbulkan dampak negatif seperti pencurian identitas, penyalahgunaan informasi, hingga tindakan kejahatan berbasis teknologi. Fenomena ini menunjukkan bahwa regulasi perlindungan data pribadi menjadi semakin krusial bagi masyarakat dan negara (Astriani, 2020).

Dalam praktiknya, banyak pihak masih mengabaikan aspek perlindungan data pribadi, baik karena kurangnya kesadaran maupun lemahnya pengawasan. Perusahaan teknologi, institusi pemerintahan, dan entitas bisnis sering kali mengumpulkan serta memproses data pengguna tanpa transparansi yang memadai. Hal ini menyebabkan ketidakpastian hukum bagi individu yang datanya diproses serta meningkatkan risiko penyalahgunaan informasi pribadi. Kondisi ini diperparah dengan minimnya pemahaman masyarakat mengenai hak-hak mereka terhadap data pribadi serta bagaimana data tersebut seharusnya dilindungi (Mahameru, et al., 2023).

Secara teoritis, perlindungan data pribadi merupakan hak fundamental yang harus dijamin oleh negara, sebagaimana tertuang dalam berbagai instrumen hukum internasional dan nasional. Teori-teori hukum tentang hak privasi menggarisbawahi pentingnya perlindungan data pribadi sebagai bagian dari hak asasi manusia. Namun, dalam kenyataannya, masih terdapat kesenjangan antara teori dan praktik di lapangan. Implementasi kebijakan perlindungan data pribadi di Indonesia masih menghadapi berbagai hambatan, mulai dari lemahnya infrastruktur keamanan siber hingga kurangnya penegakan hukum yang tegas terhadap pelanggaran data (Meher, et al., 2023).

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi hadir sebagai respons terhadap urgensi perlindungan data pribadi di Indonesia. Regulasi ini bertujuan untuk memberikan kepastian hukum, mengatur pemrosesan data pribadi secara bertanggung jawab, serta mencegah penyalahgunaan informasi individu oleh pihak yang tidak berwenang. Dengan adanya undang-undang ini, diharapkan ekosistem digital Indonesia menjadi lebih aman dan terpercaya bagi seluruh pengguna (Satria & Yusuf, 2024). Namun, keberadaan regulasi ini belum sepenuhnya menjawab tantangan yang ada. Masih terdapat berbagai aspek yang perlu diperkuat, seperti pengawasan terhadap penyelenggara sistem elektronik, peningkatan kesadaran masyarakat tentang hak-hak privasi, serta mekanisme penegakan hukum yang lebih efektif. Tantangan lain adalah bagaimana perusahaan teknologi dan instansi pemerintahan dapat menyesuaikan praktik mereka agar selaras dengan standar perlindungan data pribadi yang baru diterapkan.

Urgensi jurnal ini terletak pada pentingnya memahami sejauh mana Undang-Undang Perlindungan Data Pribadi dapat menutup kesenjangan antara teori dan realitas dalam perlindungan informasi individu. Dengan analisis yang mendalam terhadap regulasi ini, diharapkan jurnal ini dapat memberikan wawasan bagi masyarakat, akademisi, dan pembuat kebijakan tentang tantangan serta solusi dalam implementasi perlindungan data pribadi di Indonesia. Pada akhirnya, perlindungan data pribadi bukan hanya menjadi tanggung jawab pemerintah dan perusahaan teknologi, tetapi juga seluruh elemen masyarakat. Kesadaran akan pentingnya privasi digital harus ditanamkan sejak dulu agar setiap individu dapat menjaga informasi pribadinya dengan lebih baik. Dengan mengembangkan regulasi yang kokoh serta meningkatkan literasi digital, Indonesia dapat mewujudkan sistem perlindungan data pribadi yang efektif dan menjamin hak privasi bagi seluruh rakyatnya.

## METODE PENELITIAN

Penelitian ini menggunakan metode studi pustaka sebagai pendekatan utama dalam menganalisis Urgensi Perlindungan Data Pribadi dalam Era Digital berdasarkan Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. Studi pustaka dilakukan dengan



menelaah berbagai sumber literatur, termasuk undang-undang, jurnal akademik, laporan kebijakan, serta artikel ilmiah yang berkaitan dengan regulasi dan perlindungan data pribadi. Pendekatan ini memungkinkan peneliti untuk memahami secara komprehensif prinsip-prinsip hukum yang mendasari perlindungan data pribadi, membandingkannya dengan standar internasional seperti General Data Protection Regulation (GDPR), serta mengidentifikasi tantangan dan peluang dalam implementasi regulasi di Indonesia.

Melalui studi pustaka, penelitian ini mengkaji kesenjangan antara regulasi dan perkembangan teknologi, seperti Artificial Intelligence (AI), Big Data, dan Internet of Things (IoT), serta menyoroti peran undang-undang ITE dalam memperkuat perlindungan data pribadi. Selain itu, metode ini juga digunakan untuk menganalisis efektivitas sanksi administratif dan pidana, kesiapan lembaga pengawas, serta tingkat literasi digital masyarakat dalam menjaga privasi mereka. Dengan pendekatan berbasis literatur, penelitian ini memberikan landasan yang kuat untuk menilai sejauh mana undang-undang Perlindungan Data Pribadi dapat mengatasi tantangan privasi di era digital dan memastikan perlindungan hak-hak individu secara lebih optimal.

## HASIL DAN PEMBAHASAN

Dalam konsep perlindungan data pribadi, setiap individu memiliki hak fundamental atas privasi dan kendali terhadap informasi pribadinya, sebagaimana diatur dalam berbagai teori hukum dan regulasi internasional. Teori Hak Privasi yang dikemukakan oleh Warren dan Brandeis menyatakan bahwa hak atas privasi merupakan bagian integral dari kebebasan individu yang harus dilindungi oleh hukum. Selain itu, prinsip data sovereignty menekankan bahwa setiap pemilik data memiliki otoritas atas penggunaannya dan berhak menentukan bagaimana informasi pribadinya diproses (Yuniarti, 2019). Dalam konteks ini, Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) hadir sebagai instrumen hukum yang bertujuan untuk mengatur pemrosesan data pribadi serta memastikan perlindungan hak privasi bagi masyarakat Indonesia di tengah pesatnya perkembangan teknologi digital. Dengan berlandaskan teori hukum dan prinsip etika perlindungan data, UU PDP menetapkan standar transparansi, akuntabilitas, dan keamanan dalam pengelolaan informasi pribadi, sehingga dapat mencegah penyalahgunaan data serta menjamin hak individu di era digital.

### Kerangka Hukum dan Implementasi Undang-Undang Perlindungan Data Pribadi

Era digital telah membawa perubahan besar dalam cara data pribadi dikumpulkan, diolah, dan dimanfaatkan. Ketergantungan masyarakat pada teknologi digital menjadikan data pribadi sebagai aset berharga yang juga rentan terhadap penyalahgunaan. Undang-Undang Perlindungan Data Pribadi yaitu Undang-Undang No. 27 Tahun 2022 (UNDANG-UNDANG PDP) hadir sebagai respons terhadap kebutuhan hukum yang kuat dalam melindungi hak privasi individu. Regulasi ini menjadi penting karena menjamin hak asasi manusia, khususnya perlindungan diri pribadi, di tengah masifnya digitalisasi (Daeng, et al., 2023).

Undang-undang PDP memiliki tujuan utama untuk memberikan perlindungan hukum atas data pribadi warga negara Indonesia secara menyeluruh. Dengan pendekatan berbasis hak asasi manusia, undang-undang ini menetapkan prinsip kepastian hukum, kemanfaatan, kehati-hatian, dan kerahasiaan. Prinsip-prinsip ini dirancang untuk menghindari penyalahgunaan data pribadi dan memastikan bahwa setiap tahap pemrosesan data dilakukan secara bertanggung jawab sesuai dengan regulasi. Keberadaan prinsip-prinsip tersebut menjadi fondasi etik dan yuridis yang memperkuat kedudukan individu dalam relasi digital (Suari & Sarjana, 2023).

UNDANG-UNDANG PDP mengatur secara rinci mekanisme pengumpulan, penyimpanan, pemrosesan, dan pemanfaatan data pribadi. Regulasi ini berlaku untuk sektor publik dan swasta, termasuk entitas luar negeri yang memproses data warga negara Indonesia.



Pendekatan ini sejalan dengan prinsip jurisdiksi ekstrateritorial dalam hukum siber modern. Meskipun demikian, undang-undang ini memberikan pengecualian bagi pemrosesan data untuk kepentingan pribadi atau rumah tangga. Dengan cakupan yang luas, regulasi ini bertujuan untuk menyesuaikan perlindungan hukum terhadap kemajuan teknologi global (Yamin, et al., 2024).

Data pribadi dalam undang-undang PDP dikategorikan menjadi data umum dan spesifik. Data spesifik, seperti biometrik, kesehatan, dan genetika, mendapatkan perlakuan hukum yang lebih ketat karena sifatnya yang lebih sensitif. Pembagian ini penting untuk menentukan tingkat perlindungan dan tanggung jawab yang harus dipenuhi oleh pengendali data. Pendekatan ini sejalan dengan praktik internasional, seperti yang diterapkan dalam General Data Protection Regulation (GDPR) di Uni Eropa, guna memastikan perlindungan data pribadi yang lebih optimal (Ziqra, et al., 2021).

Undang-undang PDP juga memberikan hak kepada individu sebagai subjek data, termasuk hak akses, hak koreksi, hak penghapusan, dan hak untuk membatasi pemrosesan data. Hak-hak ini menandai pergeseran dari perlindungan pasif menuju kontrol aktif oleh individu terhadap data pribadinya. Jaminan atas hak-hak tersebut mencerminkan pengakuan negara terhadap kedaulatan data individu dalam ekosistem digital. Transparansi dan akuntabilitas dalam pengelolaan data menjadi bagian integral dari penerapan regulasi ini (Yuniarti, 2019). Dalam sistem perlindungan data, undang-undang PDP menetapkan tanggung jawab bagi pengendali dan prosesor data pribadi. Pengendali memiliki kewenangan menetapkan tujuan dan cara pemrosesan data, sementara prosesor bertugas melakukan pemrosesan sesuai instruksi pengendali. Regulasi ini memastikan bahwa setiap pihak memiliki kewajiban hukum yang jelas serta tidak dapat mengalihkan tanggung jawab secara sepihak. Pengaturan ini juga mendorong pembentukan sistem manajemen data yang profesional dan sesuai standar internasional.

Efektivitas implementasi undang-undang PDP sangat bergantung pada penegakan hukum dan keberadaan otoritas pengawas yang memiliki wewenang dalam menerima pengaduan, melakukan investigasi, serta menjatuhkan sanksi administratif maupun pidana. Lembaga pengawas menjadi elemen penting dalam menegakkan hak-hak individu dan mencegah praktik ilegal dalam pemrosesan data pribadi. Namun, tantangan ke depan mencakup kesiapan kelembagaan, keterbatasan sumber daya, serta perlunya peningkatan literasi digital masyarakat agar perlindungan data pribadi dapat berjalan optimal di Indonesia (Makkawaru, et al., 2025).

Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi menetapkan tanggung jawab hukum bagi pengendali data pribadi (data controller) dan prosesor data pribadi (data processor) dalam pengelolaan informasi individu. Pengendali data bertugas menentukan tujuan dan cara pemrosesan data, sementara prosesor data melakukan pemrosesan berdasarkan instruksi dari pengendali. Keduanya harus menerapkan prinsip akuntabilitas, transparansi, dan perlindungan hak subjek data, sehingga pengelolaan informasi dilakukan dengan standar yang ketat guna mencegah penyalahgunaan serta kebocoran data (Vania, et al., 2023). Pengendali data wajib memperoleh persetujuan sah dari subjek data sebelum pemrosesan, memberikan informasi jelas mengenai tujuan penggunaan, menjaga keamanan data dengan langkah teknis yang sesuai, serta melaporkan insiden kebocoran kepada otoritas pengawas. Sementara itu, prosesor data harus memproses informasi sesuai arahan pengendali, menjamin kerahasiaan selama pengelolaan berlangsung, dan menyediakan catatan pemrosesan untuk keperluan audit atau pengawasan. Pembagian tanggung jawab ini memastikan setiap pihak memiliki kewajiban hukum yang jelas dan tidak dapat mengalihkan tugasnya secara sepihak.

Dengan regulasi yang tegas, Undang-Undang No. 27 Tahun 2022 bertujuan memperkuat perlindungan hak privasi di Indonesia serta memastikan bahwa ekosistem digital berjalan dengan lebih aman. Efektifnya implementasi regulasi ini bergantung pada kepatuhan dari semua pihak yang terlibat dalam pemrosesan data pribadi, serta keberadaan mekanisme



pengawasan yang berfungsi secara optimal. Dengan kerangka hukum yang jelas dan pengawasan yang kuat, perlindungan data pribadi dapat terwujud sebagai bagian dari hak fundamental setiap individu di era digital (Mahameru et al., 2023).

Pelanggaran terhadap Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi dapat dikenai sanksi administratif dan pidana, bergantung pada tingkat dan dampak pelanggaran. Sanksi administratif biasanya diterapkan kepada entitas yang gagal memenuhi kewajiban kepatuhan, seperti tidak memperoleh persetujuan sah dalam pemrosesan data atau lalai dalam menjaga keamanan informasi pribadi. Bentuk sanksinya meliputi teguran tertulis, pembekuan izin usaha, atau denda yang jumlahnya disesuaikan dengan dampak pelanggaran. Sanksi ini bertujuan untuk memastikan kepatuhan perusahaan dan lembaga terhadap regulasi serta mencegah terjadinya pelanggaran di masa mendatang (Manurung & Thalib, 2022). Sanksi pidana, di sisi lain, berlaku bagi pelanggaran serius seperti penyalahgunaan data pribadi yang menyebabkan kerugian besar bagi individu atau masyarakat. Pengungkapan informasi tanpa izin, pencurian data, dan pemanfaatan data untuk tujuan ilegal dapat dikenai hukuman penjara serta denda dalam jumlah besar sesuai dengan tingkat keparahan pelanggaran. Sanksi pidana ini bertujuan memberikan efek jera bagi pelaku serta menegakkan keadilan bagi individu yang dirugikan akibat pelanggaran privasi. Namun, efektivitas penerapan sanksi pidana masih bergantung pada mekanisme hukum yang jelas serta kesiapan aparat penegak hukum dalam menangani kasus-kasus pelanggaran data.

Dalam implementasinya, Undang-Undang Perlindungan Data Pribadi menghadapi berbagai tantangan di lapangan, termasuk kesiapan lembaga pengawas yang bertanggung jawab dalam mengawasi kepatuhan terhadap regulasi. Otoritas pengawas harus memiliki sumber daya dan kewenangan yang cukup untuk menangani laporan pelanggaran, melakukan investigasi, serta menjatuhkan sanksi dengan transparansi dan akuntabilitas. Namun, kelembagaan yang masih dalam tahap penyesuaian menjadi hambatan tersendiri dalam memastikan regulasi berjalan secara efektif. Selain kesiapan lembaga, kesadaran masyarakat dan infrastruktur digital juga menjadi faktor utama dalam keberhasilan implementasi undang-undang Perlindungan Data Pribadi. Banyak individu masih belum memahami hak-hak mereka terkait perlindungan data pribadi, sehingga rentan terhadap eksploitasi oleh pihak yang tidak bertanggung jawab. Infrastruktur digital yang belum merata serta minimnya standar keamanan dalam pemrosesan data juga memperbesar risiko kebocoran informasi. Oleh karena itu, diperlukan edukasi yang lebih luas serta perbaikan sistem keamanan digital guna menciptakan ekosistem perlindungan data yang efektif dan berkelanjutan (Mahameru, et al., 2023).

Indonesia memiliki dua regulasi utama yang berfungsi untuk melindungi keamanan data pribadi, yaitu Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (Undang-Undang PDP) dan Undang-Undang Informasi dan Transaksi Elektronik (Undang-Undang ITE). Undang-undang ITE lebih berfokus pada aspek kejahatan siber, termasuk penyalahgunaan data pribadi, peretasan, serta akses ilegal terhadap sistem elektronik. Sementara itu, undang-undang PDP secara khusus mengatur hak dan kewajiban terkait pengelolaan data pribadi, menetapkan standar pemrosesan yang lebih ketat, serta memberikan mekanisme penegakan hukum terhadap pelanggaran yang berkaitan dengan privasi digital. Dengan sinergi antara kedua regulasi ini, Indonesia berupaya menciptakan ekosistem digital yang aman dan terpercaya bagi masyarakat (Tsamara, 2023).

Undang-undang ITE menjadi instrumen hukum yang menindak berbagai bentuk pelanggaran keamanan data pribadi, seperti pengungkapan informasi tanpa izin, pencurian identitas, dan eksploitasi data dalam transaksi digital. Regulasi ini juga mengatur tanggung jawab penyelenggara sistem elektronik, mewajibkan mereka untuk memastikan keamanan sistem guna menghindari kebocoran data. Sementara itu, undang-undang PDP melengkapi regulasi ini dengan memastikan perlindungan yang lebih spesifik terhadap pemrosesan data



pribadi oleh pengendali dan prosesor data, mewajibkan mereka untuk memperoleh persetujuan subjek data dan menerapkan langkah-langkah keamanan yang memadai (Julianti & Sugiantari, 2021).

Dalam aspek penegakan hukum, undang-undang PDP menyediakan mekanisme sanksi administratif dan pidana terhadap pihak yang melanggar prinsip perlindungan data pribadi. Sanksi administratif meliputi teguran, pembekuan izin usaha, serta denda dalam jumlah tertentu, sedangkan sanksi pidana mencakup hukuman penjara bagi pelanggar yang terbukti menyalahgunakan data pribadi untuk kepentingan ilegal. undang-undang ITE turut memperkuat upaya penegakan hukum dengan menetapkan pidana bagi pelaku kejahatan siber yang mengakses atau menyebarluaskan data tanpa izin. Meskipun sudah memiliki dasar hukum yang jelas, tantangan utama masih berkaitan dengan implementasi regulasi, kesiapan lembaga pengawas, serta kesadaran masyarakat dalam menjaga privasi digital mereka (Wibowo, 2023).

Agar perlindungan data pribadi dapat berjalan secara efektif, diperlukan edukasi dan sosialisasi yang lebih luas mengenai hak dan kewajiban dalam ekosistem digital. Kesadaran masyarakat tentang pentingnya perlindungan privasi harus ditingkatkan, baik melalui regulasi yang lebih kuat maupun penerapan teknologi keamanan yang lebih canggih. Selain itu, penguatan infrastruktur digital serta sistem pengawasan terhadap kepatuhan regulasi menjadi faktor penting dalam memastikan bahwa setiap individu dan institusi menjalankan tanggung jawabnya dalam menjaga keamanan data pribadi. Dengan kerja sama yang solid antara pemerintah, industri, dan masyarakat, Indonesia dapat mewujudkan sistem perlindungan data pribadi yang lebih komprehensif dan efektif.

### Tantangan Perlindungan Data Pribadi di Era Digital

Perkembangan teknologi digital telah mempermudah berbagai aspek kehidupan, namun juga membawa risiko serius terhadap keamanan data pribadi. Seiring dengan meningkatnya penggunaan internet dan sistem berbasis data, potensi eksploitasi oleh pihak tidak bertanggung jawab juga semakin besar. Peretasan menjadi salah satu ancaman utama karena memungkinkan pelaku untuk mengakses informasi sensitif tanpa izin. Teknologi yang semakin kompleks tidak selalu disertai dengan sistem keamanan yang memadai, sehingga banyak platform digital, termasuk layanan keuangan dan perusahaan teknologi, menjadi target utama bagi serangan siber. Hal ini menempatkan individu dan organisasi pada risiko tinggi terkait pencurian serta penyalahgunaan data (Sulianta, 2025).

Salah satu metode yang sering digunakan oleh peretas adalah phishing, yaitu teknik penipuan di mana pelaku menyamar sebagai pihak terpercaya untuk mengelabui korban agar memberikan informasi sensitif seperti kata sandi atau data keuangan. Malware, sebagai perangkat lunak berbahaya, juga menjadi ancaman signifikan karena mampu menyusup ke sistem komputer, mencuri data, dan bahkan merusak file penting. Selain itu, eksploitasi terhadap sistem keamanan yang lemah menjadi celah utama bagi para peretas untuk memperoleh akses tanpa terdeteksi. Ketika keamanan digital tidak diperkuat dengan baik, sistem yang mengelola data pengguna dalam jumlah besar menjadi sasaran empuk bagi serangan ini (Budiono et al., 2025).

Dampak dari peretasan terhadap data pribadi sangat serius, terutama jika informasi yang dicuri digunakan untuk penipuan atau pencurian identitas. Dengan data yang telah diperoleh, pelaku dapat melakukan transaksi ilegal, mengakses akun korban, atau bahkan menyalahgunakan identitas untuk tindakan kriminal lainnya. Pencurian identitas tidak hanya menimbulkan kerugian finansial tetapi juga berdampak pada reputasi dan hak individu yang terdampak. Oleh karena itu, perlindungan data harus menjadi prioritas utama bagi perusahaan teknologi, lembaga keuangan, serta pengguna individu. Peningkatan kesadaran akan keamanan digital, penerapan sistem proteksi yang lebih kuat, serta regulasi ketat dalam pengelolaan data



pribadi sangat diperlukan untuk mengurangi risiko serangan siber dan melindungi informasi sensitif dari eksploitasi (Sulianta, 2025). Pencurian identitas juga menjadi masalah serius dalam era digital, di mana data pribadi seseorang seperti nama, nomor identitas, atau informasi finansial disalahgunakan untuk melakukan transaksi keuangan atau tindakan kriminal atas nama korban. Pelaku sering kali memperoleh data ini melalui kebocoran sistem, pembelian informasi di pasar gelap, atau eksploitasi kelemahan dalam kebijakan privasi platform digital. Dampaknya bisa sangat luas, mulai dari kerugian finansial, penyalahgunaan dokumen resmi, hingga pemalsuan akun yang dapat merugikan korban dalam jangka panjang.

Selain ancaman dari pihak eksternal, platform digital sendiri sering kali menjadi sumber penyalahgunaan data pribadi. Banyak perusahaan teknologi mengumpulkan informasi pengguna untuk keperluan komersial, seperti periklanan berbasis data, analisis perilaku, atau personalisasi layanan tanpa transparansi yang memadai. Dalam beberapa kasus, data pribadi dijual atau dibagikan tanpa persetujuan eksplisit dari pengguna, menciptakan risiko privasi yang besar. Kurangnya regulasi yang tegas dalam pengelolaan data oleh platform digital juga memperbesar kemungkinan eksploitasi informasi pribadi tanpa perlindungan yang layak (Dhianty, 2022).

Untuk mengatasi ancaman ini, diperlukan penguatan regulasi dan kesadaran masyarakat dalam menjaga keamanan data pribadi. Pemerintah dan otoritas terkait harus memastikan bahwa platform digital memiliki standar keamanan yang tinggi, serta menerapkan sanksi tegas terhadap pelaku pelanggaran privasi. Di sisi lain, individu juga perlu meningkatkan literasi digital dengan memahami hak-hak mereka serta menerapkan tindakan pencegahan, seperti menggunakan kata sandi yang kuat, mengaktifkan autentikasi dua faktor, dan berhati-hati dalam membagikan informasi pribadi secara online. Dengan langkah-langkah yang tepat, perlindungan data pribadi dapat semakin diperkuat di tengah pesatnya perkembangan teknologi digital (Suari & Sarjana, 2023).

Perkembangan teknologi seperti Artificial Intelligence (AI), Big Data, dan Internet of Things (IoT) telah melampaui kecepatan adaptasi regulasi, menciptakan kesenjangan yang signifikan antara kebijakan hukum dan realitas teknologi. AI kini digunakan dalam berbagai sektor, termasuk keuangan, kesehatan, dan pemerintahan, namun regulasi masih tertinggal dalam menetapkan standar etik serta pengawasan terhadap pemrosesan data secara otomatis. Sementara itu, Big Data memungkinkan pengolahan informasi dalam skala besar, tetapi tanpa regulasi yang jelas, penyalahgunaan data pribadi tetap menjadi ancaman bagi privasi individu. IoT, yang semakin terintegrasi dalam kehidupan sehari-hari, menambah tantangan baru terkait keamanan dan aksesibilitas informasi, mengingat banyak perangkat IoT beroperasi dengan protokol keamanan yang belum sepenuhnya diatur oleh regulasi (Kushariadi, et al., 2024).

Kesenjangan ini semakin terlihat dalam aspek perlindungan hak privasi, keamanan data, dan transparansi dalam pemanfaatan teknologi. Banyak sistem berbasis AI dan Big Data dapat membuat keputusan secara otomatis, namun regulasi belum sepenuhnya memberikan mekanisme audit yang memungkinkan pengguna memahami atau menantang keputusan yang dibuat oleh algoritma. Selain itu, keamanan dalam ekosistem IoT sering kali menjadi isu utama karena banyak perangkat yang mengumpulkan dan berbagi data tanpa standar keamanan yang memadai. Ketidakseimbangan antara regulasi dan perkembangan teknologi ini berisiko meningkatkan eksploitasi data oleh korporasi serta menciptakan ketidakpastian hukum bagi individu yang terdampak (Hartati, 2025).

Untuk menjembatani kesenjangan ini, diperlukan pembaruan regulasi yang lebih adaptif, mencakup standar internasional serta mekanisme pengawasan yang lebih kuat terhadap pemanfaatan teknologi. Kebijakan harus memastikan akuntabilitas dan transparansi dalam pemrosesan data, termasuk memberi hak kepada individu untuk mengontrol informasi mereka sendiri. Selain itu, kolaborasi antara pemerintah, akademisi, dan pelaku industri teknologi harus



diperkuat guna memastikan regulasi tidak hanya menghambat inovasi tetapi juga menciptakan keseimbangan antara kemajuan teknologi dan perlindungan hak-hak masyarakat. Dengan regulasi yang lebih fleksibel dan berbasis prinsip keadilan, teknologi dapat berkembang secara bertanggung jawab tanpa mengabaikan hak-hak fundamental pengguna.

Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (undang-undang PDP) dan General Data Protection Regulation (GDPR) memiliki kesamaan dalam menegakkan hak privasi individu, khususnya dalam aspek transparansi dan akuntabilitas pengelolaan data. Keduanya memastikan bahwa pemrosesan data dilakukan dengan dasar hukum yang jelas, serta memberikan hak kepada subjek data untuk mengakses, mengoreksi, dan menghapus informasi pribadi mereka. GDPR lebih ketat dalam penerapan prinsip lawfulness, fairness, dan transparency, menetapkan standar tinggi bagi perusahaan dan organisasi dalam menjaga data pengguna, termasuk dengan mekanisme yang mengharuskan perusahaan memiliki Data Protection Officer (DPO) untuk mengawasi kepatuhan terhadap regulasi. Sementara Undang-undang PDP mengadopsi prinsip yang sama, pengawasannya masih memerlukan penguatan agar dapat memastikan kepatuhan dari entitas pemroses data di Indonesia (Ariesta & Sukron, 2024).

Perbedaan lainnya terletak pada struktur penegakan hukum dan sanksi yang diberlakukan. GDPR menerapkan sanksi berat bagi pelanggar, dengan denda mencapai 4% dari pendapatan tahunan global perusahaan, menjadikannya regulasi yang memiliki daya tekan tinggi terhadap kepatuhan industri. Undang-undang PDP juga mengenakan sanksi administratif dan pidana, termasuk denda dan hukuman penjara bagi pelanggar, tetapi jumlahnya lebih rendah dibandingkan GDPR. Selain itu, implementasi undang-undang PDP masih menghadapi tantangan seperti kesiapan lembaga pengawas dan penegakan hukum yang efektif. Agar dapat mencapai efektivitas seperti GDPR, undang-undang PDP perlu disertai dengan peningkatan kapasitas kelembagaan serta sosialisasi yang luas bagi pelaku industri dan masyarakat mengenai pentingnya perlindungan data pribadi (Hakim, et al., 2023).

Salah satu perbedaan mendasar adalah dalam struktur penegakan hukum dan sanksi. GDPR memiliki sistem sanksi yang lebih tegas, di mana pelanggaran serius dapat dikenakan denda hingga 4% dari pendapatan tahunan global perusahaan atau sejumlah yang lebih besar sesuai dengan tingkat pelanggaran. Undang-undang PDP juga menetapkan sanksi administratif dan pidana, termasuk denda dan hukuman penjara bagi pelanggar, namun jumlahnya cenderung lebih rendah dibandingkan dengan standar GDPR. Selain itu, GDPR menekankan keberadaan Data Protection Officer (DPO) di setiap perusahaan yang menangani data pribadi dalam skala besar, sedangkan undang-undang PDP belum secara eksplisit mewajibkan adanya DPO untuk semua entitas yang memproses data (Ariesta & Sukron, 2024).

Meskipun undang-undang PDP telah menetapkan kerangka hukum yang lebih jelas dibandingkan regulasi sebelumnya, tantangan dalam implementasi dan penegakan hukum menjadi faktor yang perlu diperhatikan. GDPR telah membangun sistem pengawasan yang kuat dengan otoritas perlindungan data independen di setiap negara Uni Eropa, sedangkan undang-undang PDP masih dalam tahap membentuk lembaga pengawas yang efektif. Selain itu, kesiapan perusahaan dan lembaga pemerintah dalam memenuhi standar perlindungan data juga menjadi aspek penting yang menentukan keberhasilan regulasi ini. Untuk dapat mencapai efektivitas setara dengan GDPR, undang-undang PDP perlu terus disempurnakan melalui peningkatan pengawasan, sanksi yang lebih kuat, serta edukasi bagi masyarakat dan pelaku industri mengenai pentingnya perlindungan data pribadi (Hakim, et al., 2023).

Di era digital yang semakin kompleks, literasi digital dan kesadaran hukum masyarakat menjadi faktor krusial dalam menjaga data pribadi dari berbagai ancaman siber. Banyak individu masih belum memahami bagaimana informasi mereka dikumpulkan, digunakan, atau dibagikan oleh berbagai platform digital. Rendahnya kesadaran ini membuat mereka rentan



terhadap praktik eksplorasi data, seperti peretasan, pencurian identitas, dan penyalahgunaan oleh pihak yang tidak bertanggung jawab. Dengan literasi digital yang lebih baik, masyarakat dapat mengenali risiko-risiko ini serta mengambil langkah proaktif dalam melindungi informasi pribadi mereka, seperti menggunakan autentikasi dua faktor, memperkuat kata sandi, dan memahami kebijakan privasi dari layanan digital yang mereka gunakan (Arief, et al., 2024).

Kesadaran hukum terkait perlindungan data pribadi juga menjadi aspek penting dalam menciptakan ekosistem digital yang lebih aman dan transparan. Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan dasar hukum bagi individu untuk mengontrol dan melindungi informasi mereka dari penyalahgunaan. Namun, tanpa pemahaman yang cukup mengenai hak-hak yang diberikan oleh regulasi ini, banyak masyarakat tidak menyadari bahwa mereka memiliki mekanisme hukum untuk mengajukan keluhan atau menuntut pertanggungjawaban dari pihak yang melanggar privasi mereka. Oleh karena itu, edukasi mengenai hak-hak individu dalam pengelolaan data pribadi perlu diperkuat, baik melalui sosialisasi regulasi maupun peningkatan literasi hukum di masyarakat.

Untuk mewujudkan perlindungan data yang efektif, diperlukan kerja sama antara pemerintah, pelaku industri digital, dan masyarakat dalam meningkatkan literasi serta kesadaran hukum terkait privasi data. Pemerintah harus aktif melakukan kampanye edukasi dan pengawasan, sementara perusahaan teknologi perlu menerapkan standar keamanan yang tinggi serta kebijakan privasi yang lebih transparan. Di sisi lain, masyarakat juga harus lebih berhati-hati dalam membagikan informasi pribadi serta memanfaatkan teknologi dengan lebih bijak. Dengan meningkatnya kesadaran digital dan pemahaman hukum, masyarakat dapat berpartisipasi dalam menciptakan ekosistem digital yang lebih aman dan menjamin hak privasi setiap individu.

## KESIMPULAN

Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi hadir sebagai langkah penting dalam menjamin hak privasi individu di era digital. Regulasi ini memberikan dasar hukum yang lebih jelas terkait pengelolaan dan pemrosesan data pribadi, memastikan bahwa setiap entitas yang mengolah informasi pribadi harus mematuhi prinsip transparansi, akuntabilitas, dan persetujuan eksplisit dari subjek data. Namun, implementasi regulasi ini masih menghadapi berbagai tantangan, termasuk kesiapan lembaga pengawas, kesadaran masyarakat, serta kepatuhan industri terhadap standar perlindungan data. Oleh karena itu, diperlukan penguatan infrastruktur hukum dan sosialisasi yang lebih luas agar undang-undang ini dapat berfungsi secara efektif dalam menghadapi berbagai ancaman privasi yang semakin kompleks.

Selain penguatan regulasi, sinergi antara pemerintah, pelaku industri digital, dan masyarakat menjadi kunci keberhasilan dalam menciptakan ekosistem perlindungan data yang lebih aman dan berkelanjutan. Kesadaran masyarakat terhadap pentingnya literasi digital dan hak-hak privasi harus terus ditingkatkan agar mereka dapat lebih proaktif dalam menjaga informasi pribadi. Di sisi lain, industri teknologi wajib memastikan kepatuhan terhadap regulasi serta menerapkan standar keamanan yang tinggi dalam pemrosesan data. Dengan kolaborasi yang kuat antara berbagai pihak, Undang-Undang Perlindungan Data Pribadi diharapkan dapat menjadi instrumen yang efektif dalam melindungi hak-hak individu serta membangun ekosistem digital yang lebih bertanggung jawab di Indonesia.

## DAFTAR PUSTAKA

- Arief, M. H., Fitri, K. A., & Sakti, E. M. S. (2024). Analisis kesadaran cyber crime di kalangan masyarakat menengah kebawah. *Jurnal Ilmiah Teknik Informatika (TEKINFO)*, 25(2), 24–39.



- Ariesta, W., & Sukron, A. (2024). Studi komparasi perlindungan hukum data pribadi Uni Eropa dan Indonesia dalam prinsip the right to be forgotten menurut Pasal 26 UU Nomor 19 Tahun 2016 tentang perubahan atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. *Yurijaya: Jurnal Ilmiah Hukum*, 6(2), 162–177.
- Astriani, R. (2020). Perlindungan data pribadi dalam era digital: Tantangan dan solusi. *Jurnal Ilmiah Hukum*, 20(2), 241–254.
- Budiono, B., Fadillah, F. R., & Arinudin, N. (2025). The dangers of phishing to personal data security. *Formosa Journal of Applied Sciences*, 4(3), 831–844.
- Daeng, Y., Linra, N., Darham, A., Handrianto, D., Sianturi, R. R., Martin, D., ... & Saputra, H. (2023). Perlindungan data pribadi dalam era digital: Tinjauan terhadap kerangka hukum perlindungan privasi. *Innovative: Journal of Social Science Research*, 3(6), 2898–2905.
- Dhianty, R. (2022). Kebijakan privasi (privacy policy) dan peraturan perundang-undangan sektoral platform digital vis a vis kebocoran data pribadi. *Scripta: Jurnal Kebijakan Publik dan Hukum*, 2(1), 186–199.
- Hakim, G., Haris, O. K., & Mohammad, M. (2023). Analisis perbandingan hukum mengenai regulasi perlindungan data pribadi antara Uni Eropa dan Indonesia. *Halul Oleo Legal Research*, 5(2), 443–453.
- Hartati, D. (2025, January). Literature review: Dampak artificial intelligence (AI) dan big data dalam pengambilan keputusan kebijakan publik. In *Prosiding Seminar Nasional Sosial* (Vol. 1, No. 1, pp. 48–57).
- Julianti, L., & Sugiantari, A. A. P. W. (2021). Tanggung jawab hukum pihak perbankan dalam pencurian data pribadi nasabah dengan teknik “phising” pada transaksi perbankan. In *Prosiding Seminar Nasional Fakultas Hukum Universitas Mahasasawati Denpasar 2020* (Vol. 1, No. 1, pp. 96–105).
- Kushariyadi, K., Apriyanto, H., Herdiana, Y., Asy’ari, F. H., Judijanto, L., Pasrun, Y. P., & Mardikawati, B. (2024). *Artificial intelligence: Dinamika perkembangan AI beserta penerapannya*. PT. Sonpedia Publishing Indonesia.
- Mahameru, D. E., Nurhalizah, A., Badjeber, H., Wildan, A., & Rahmadi, H. (2023). Implementasi undang-undang perlindungan data pribadi terhadap keamanan informasi identitas di Indonesia. *Jurnal Esensi Hukum*, 5(2), 115–131.
- Makkawaru, I. W., Nur, A. R., Djidar, H., & Mannuhung, S. (2025). Penegakan hukum perlindungan data pribadi melalui sarana hukum perdata. *Journal of Innovation Research and Knowledge*, 4(9), 6473–6488.
- Manurung, E. A. P., & Thalib, E. F. (2022). Tinjauan yuridis perlindungan data pribadi berdasarkan UU Nomor 27 Tahun 2022. *Jurnal Hukum Saraswati*, 4(2), 139–148.
- Meher, C., Sidi, R., & Risdawati, I. (2023). Penggunaan data kesehatan pribadi dalam era big data: Tantangan hukum dan kebijakan di Indonesia. *Jurnal Ners*, 7(2), 864–870.
- Purba, Y. O., & Mauluddin, A. (2023). Kejahatan siber dan kebijakan identitas kependudukan digital: Sebuah studi tentang potensi pencurian data online. *JCIC: Jurnal CIC Lembaga Riset dan Konsultan Sosial*, 5(2), 55–66.
- Satria, M. K., & Yusuf, H. (2024). Analisis yuridis tindakan kriminal doxing ditinjau berdasarkan Undang Undang Nomor 27 Tahun 2022 tentang perlindungan data pribadi. *Jurnal Intelek dan Cendikiawan Nusantara*, 1(2), 2442–2456.
- 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.
- Sulianta, F. (2025). *Masyarakat digital: Tren, tantangan, dan perubahan di era teknologi*. Feri Sulianta.



- Tsamara, N. (2021). Perbandingan aturan perlindungan privasi atas data pribadi antara Indonesia dengan beberapa negara. *Jurnal Suara Hukum*, 3(1), 53–84.
- Vania, C., Markoni, M., Saragih, H., & Widarto, J. (2023). Tinjauan yuridis terhadap perlindungan data pribadi dari aspek pengamanan data dan keamanan siber. *Jurnal Multidisiplin Indonesia*, 2(3), 654–666.
- Wibowo, A. (2023). *Hukum di era globalisasi digital*. Penerbit Yayasan Prima Agus Teknik.
- Yamin, A. F., Rachmawati, A., Pratama, R. A., & Wijaya, J. K. (2024). Perlindungan data pribadi dalam era digital: Tantangan dan solusi. *Meraja Journal*, 7(2), 138–155.
- Yuniarti, S. (2019). Perlindungan hukum data pribadi di Indonesia. *Business Economic, Communication, and Social Sciences Journal (BECOSS)*, 1(1), 147–154.
- Ziqra, Y., Sunarmi, S., Siregar, M., & Leviza, J. (2021). Analisis hukum General Data Protection Regulation (GDPR) terhadap data pribadi konsumen dalam melakukan transaksi online. *Iuris Studia: Jurnal Kajian Hukum*, 2(2), 330–336.