

Perlindungan Terhadap Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022

Nur Alfiana Alfitri ^{1*}, Rahmawati ², Firmansyah ³

^{1, 2, 3} Institut Agama Islam Negeri Palopo, Indonesia

* alnuralfiana@gmail.com

Abstract

Penelitian ini bertujuan untuk mengkaji perlindungan hukum terhadap data pribadi dalam konteks perkembangan teknologi digital, dengan fokus pada Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Jenis penelitian ini adalah penelitian hukum normatif dengan pendekatan perundang-undangan. Teknik pengumpulan data dilakukan melalui studi pustaka, dan data dianalisis secara deskriptif kualitatif. Hasil penelitian menunjukkan bahwa pesatnya perkembangan teknologi informasi telah membawa dampak signifikan pada berbagai aspek kehidupan manusia, termasuk pengelolaan data pribadi. Data pribadi kini menjadi aset yang sangat bernilai dan rentan terhadap penyalahgunaan, yang dapat mengakibatkan konsekuensi negatif seperti penipuan, pencurian identitas, dan pelanggaran privasi. UU PDP dirancang untuk memberikan perlindungan hukum terhadap data pribadi dengan mengatur pengumpulan, pengolahan, dan pemanfaatannya, serta menetapkan sanksi bagi pihak yang melanggar ketentuan tersebut. Sebelumnya, perlindungan data pribadi tersebar dalam regulasi sektoral yang tidak komprehensif. Kasus kebocoran data di beberapa platform besar seperti *Tokopedia*, *KreditPlus*, BPJS Kesehatan, *SIM Card*, dan BSI menunjukkan adanya celah dalam sistem keamanan yang perlu diperbaiki, baik dalam perangkat lunak maupun dari sisi human error. Oleh karena itu, sistem keamanan yang lebih kuat, seperti enkripsi data, autentikasi ganda, dan pembaruan perangkat lunak secara berkala, sangat diperlukan. UU PDP memberikan perlindungan hukum preventif dengan mewajibkan persetujuan dari subjek data, hak akses dan pembaruan data, serta kewajiban pengendali data untuk melaporkan kebocoran data. Perlindungan represif berupa sanksi administratif, pidana, dan perdata juga diterapkan bagi pelanggaran. Namun, implementasi UU PDP memerlukan peraturan pemerintah dan pembentukan lembaga independen yang dapat mengawasi pelaksanaan perlindungan data pribadi secara efektif. Penelitian ini penting untuk mendorong penguatan regulasi dan mekanisme pengawasan guna memastikan perlindungan data pribadi yang optimal di era digital.

Keywords: *Perlindungan Hukum, Data Pribadi, Era Digital*

Pendahuluan

Era Digital merupakan masa dimana teknologi informasi dan komunikasi memainkan peran yang sangat penting dalam kehidupan manusia. Informasi dapat dengan mudah diakses dan disebarkan melalui berbagai perangkat digital seperti komputer, ponsel pintar, dan tablet (Annan, 2024). Perkembangan teknologi yang sangat cepat telah mengubah cara kita bekerja, berkomunikasi, dan berinteraksi dengan lingkungan sekitar. Era ini dimulai dengan munculnya internet pada akhir abad ke-20, yang menjadi landasan bagi berbagai inovasi teknologi yang

sebelumnya tidak terbayangkan. Transformasi teknologi ini memungkinkan akses informasi dan komunikasi yang lebih mudah antara individu dan organisasi di seluruh dunia (Hisbulloh, 2021). Namun, meskipun menawarkan kenyamanan dan kemudahan, teknologi juga dapat menimbulkan dampak negatif, seperti digunakan sebagai sarana untuk melakukan tindak kejahatan di dunia maya.

Dampak buruk dari kemajuan teknologi adalah meningkatnya kasus pencurian data pribadi. Pencurian data pribadi merupakan bentuk kejahatan yang sangat berbahaya, karena dapat menjadi pintu gerbang bagi berbagai tindak kejahatan lainnya di dunia maya (Widigdo & Rosando, 2023). Kerugian yang ditanggung oleh korban pencurian data bisa mencakup kerugian finansial, penipuan, penyalahgunaan identitas, serta pelanggaran terhadap privasi (Hasan et al., 2024). Data pribadi sering dianggap sebagai bagian dari hak privasi seseorang, yang merupakan hak dasar manusia yang sangat penting karena berkaitan dengan otonomi dan kontrol individu atas kehidupannya. Konsep privasi ini pada awalnya diartikan sebagai hak untuk tidak diganggu oleh orang lain, atau "*the right to be alone*", yang menegaskan bahwa manusia memiliki batasan untuk melindungi diri dari gangguan yang tidak diinginkan dalam hidup mereka (Suryanto & Riyanto, 2024).

Berdasarkan pandangan Hukum Islam, yang merupakan sistem hukum Ilahi yang membimbing umat Muslim dalam kehidupan sehari-hari, privasi dianggap sebagai sesuatu yang sangat penting untuk dihormati, karena berkaitan dengan kerahasiaan individu (Anantama & Dewantara, 2022). Prinsip perlindungan privasi ini tercermin dalam ajaran Al-Qur'an, salah satunya dalam QS. An-Nur ayat 27-24, yang menegaskan pentingnya menjaga privasi dan menghormati ruang pribadi orang lain. Ayat tersebut menekankan pentingnya etika dalam memasuki rumah orang lain, di mana Allah melarang umat Islam memasuki rumah tanpa izin terlebih dahulu serta menyapa pemilik rumah dengan salam. Tujuan dari larangan ini adalah untuk menghindari kemungkinan melihat sesuatu yang seharusnya tidak dilihat atau mengganggu penghuni rumah, yang dapat menimbulkan ketidaksenangan. Allah SWT berfirman untuk meminta izin sebelum masuk, sehingga kita mengetahui siapa yang ada di dalam rumah dan mendapatkan izin terlebih dahulu. Sunnah juga mengajarkan bahwa permintaan izin hanya diperbolehkan hingga tiga kali, tanpa melebihi jumlah tersebut.

Perlindungan data pribadi di Indonesia juga diatur dalam Undang-Undang Dasar 1945, tepatnya pada Pasal 28G ayat (1), yang menyatakan bahwa setiap orang berhak atas perlindungan pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada dalam kekuasaannya, serta berhak merasa aman dan dilindungi dari ancaman yang menghalangi hak asasi manusia (Sulistianingsih et al., 2023). Pasal ini sangat relevan dengan perlindungan terhadap hak-hak pribadi. Namun, regulasi mengenai perlindungan data pribadi sebelumnya tersebar dalam berbagai undang-undang dan peraturan pemerintah, yang menyebabkan ketidakpastian hukum dalam penerapannya. Untuk itu, pada 10 September 2022, pemerintah Indonesia mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang memberikan pengaturan komprehensif tentang perlindungan data pribadi,

termasuk hak-hak pemilik data dan sanksi bagi penyelenggara sistem elektronik yang mengelola data pribadi (Zahwani & Nasution, 2024).

Indonesia sendiri telah menghadapi sejumlah kasus kebocoran data yang semakin meningkat sebelum diberlakukannya undang-undang ini (Mahuli, 2023). Kasus dugaan pelanggaran perlindungan data pribadi terus meningkat, mulai dari tiga kasus pada tahun 2019, kemudian 21 kasus pada tahun 2020, 20 kasus pada tahun 2021, hingga mencapai 35 kasus pada tahun 2022 hingga 2023. Semakin pesatnya kemajuan teknologi membuat risiko kebocoran data semakin besar, terutama dengan meningkatnya peretasan yang dilakukan oleh *hacker* (Priscyllia, 2019). Salah satu insiden besar adalah kebocoran data Tokopedia pada 20 Maret 2020 yang mengungkapkan 91 juta akun pengguna (Raihan, 2023). Peretasan ini dilakukan oleh kelompok hacker internasional bernama "*why so dank*". Selanjutnya, *KreditPlus* mengalami kebocoran data nasabah sebanyak 890.000 akun yang kemudian diperjualbelikan di situs *RaidForums*. BPJS Kesehatan juga mengalami kebocoran data yang mengungkapkan informasi pribadi sekitar 279 juta warga Indonesia. Selanjutnya, pada 2022, terjadi kebocoran data sebanyak 1,3 miliar nomor kartu SIM yang dijual di forum *breached.to*. Bank Syariah Indonesia (BSI) menjadi korban peretasan, di mana *hacker grup Lookbit* berhasil mencuri sekitar 1,5 *terabyte* data yang mencakup informasi pribadi nasabah dan karyawan BSI. Kebocoran data ini menunjukkan betapa rentannya data yang tidak dilindungi dengan enkripsi, yang bisa disalahgunakan oleh pihak yang tidak bertanggung jawab. Kejadian-kejadian tersebut menggarisbawahi bahwa internet tidak sepenuhnya aman bagi mereka yang berharap privasinya terlindungi.

Beberapa insiden kebocoran data yang terjadi menunjukkan bahwa perlindungan terhadap data pribadi masih perlu diperkuat. Hal ini karena perlindungan data pribadi merupakan kebutuhan mendasar bagi masyarakat guna menciptakan rasa aman dan membangun kepercayaan dalam penggunaan teknologi dan layanan digital. Melalui pengesahan Undang-Undang Perlindungan Data Pribadi, diharapkan dapat mengurangi jumlah korban kebocoran data lebih lanjut dan memberikan perlindungan hukum yang lebih baik terhadap data pribadi warga negara.

Penelitian ini mengangkat masalah empiris dan teoritis terkait perlindungan data pribadi di era digital, khususnya terkait dengan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Segi empiris, penelitian ini mencatat bahwa meskipun UU Perlindungan Data Pribadi telah disahkan, kasus kebocoran data pribadi di Indonesia tetap meningkat, menunjukkan bahwa implementasi regulasi tersebut belum sepenuhnya efektif. Penelitian ini bertujuan untuk menganalisis faktor-faktor yang menyebabkan kebocoran data, seperti celah teknis, kurangnya pemahaman tentang regulasi, serta tantangan dalam kepatuhan terhadap UU Perlindungan Data Pribadi, baik di sektor publik maupun privat. Selain itu, penelitian ini juga akan mengeksplorasi peran pengguna dalam perlindungan data pribadi, mengingat banyak individu yang masih kurang sadar akan hak mereka terkait privasi digital dan potensi dampak buruk dari kebocoran data. Secara teoritis, penelitian ini akan membahas perlindungan privasi dalam perspektif Hukum Islam, yang menekankan pentingnya menjaga

kerahasiaan individu, serta perbandingannya dengan prinsip-prinsip perlindungan data pribadi dalam hukum positif Indonesia. Hukum Islam memandang perlindungan privasi sebagai hak yang sangat penting, yang sejalan dengan nilai-nilai yang terkandung dalam UU Perlindungan Data Pribadi. Penelitian ini juga akan mengkaji etika teknologi dan tanggung jawab sosial perusahaan teknologi dalam mengelola data pribadi pengguna, terutama terkait dengan transparansi dan keadilan dalam pengumpulan serta penyimpanan data pribadi.

Kebaharuan dari penelitian ini terletak pada fokusnya terhadap penerapan UU Perlindungan Data Pribadi 2022 yang baru disahkan, serta analisis mendalam mengenai efektivitas regulasi tersebut dalam mengatasi kasus kebocoran data yang terus meningkat. Selain itu, penelitian ini juga menawarkan perspektif baru dengan membandingkan prinsip perlindungan data pribadi dalam UU PDP dengan nilai-nilai yang terkandung dalam Hukum Islam. Penelitian ini berbeda dengan penelitian sebelumnya yang lebih terfokus pada aspek teknis atau hukum perlindungan data pribadi, dengan mengintegrasikan pendekatan multidisipliner yang menghubungkan teori hukum dengan implementasi di lapangan. Oleh karena itu, penelitian ini diharapkan dapat memberikan kontribusi signifikan dalam pemahaman dan pengembangan kebijakan perlindungan data pribadi yang lebih efektif di Indonesia. Berdasarkan permasalahan yang telah dijelaskan sebelumnya, penulis merasa tertarik untuk melakukan penelitian dengan judul "Perlindungan Terhadap Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022".

Metode

Penelitian yang dilakukan oleh penulis ini menggunakan jenis penelitian hukum normatif, yang juga dikenal sebagai penelitian hukum murni, penelitian hukum positif, dan penelitian hukum doktrinal. Penelitian hukum normatif berfokus pada peraturan perundang-undangan yang tertulis, yang sering disebut sebagai *law in books*. Jenis penelitian ini menekankan pada kajian terhadap kaidah atau norma hukum yang berlaku di masyarakat. Penelitian ini bertujuan untuk menganalisis secara mendalam berbagai peraturan hukum yang ada, yang berupa undang-undang, peraturan, serta norma-norma hukum yang diterima dalam tatanan hukum masyarakat.

Penelitian hukum normatif sering dianggap sebagai penelitian yang berbasis pada kajian pustaka. Sumber data yang digunakan dalam penelitian ini mencakup bahan hukum *primer*, *sekunder*, dan *tersier*. Bahan hukum *primer* biasanya berupa peraturan perundang-undangan yang berlaku, seperti Undang-Undang dan Peraturan Pemerintah yang terkait dengan topik penelitian. Selain itu, bahan *sekunder* dan *tersier* juga digunakan untuk memberikan penjelasan yang lebih mendalam mengenai substansi hukum yang dianalisis. Penelitian ini sangat bergantung pada dokumen-dokumen tertulis yang mengatur berbagai aspek hukum dalam masyarakat.

Pendekatan yang digunakan dalam penelitian ini adalah pendekatan perundang-undangan atau *statute approach*. Pendekatan ini diterapkan untuk memeriksa seluruh undang-undang dan peraturan yang relevan dengan masalah yang sedang diteliti, yaitu perlindungan data pribadi. Melalui pendekatan ini, penulis menelaah berbagai regulasi yang mengatur bagaimana data pribadi harus dilindungi dalam konteks hukum yang berlaku di Indonesia. Pendekatan ini memungkinkan penulis untuk memetakan dan mengevaluasi perlindungan data pribadi berdasarkan kerangka hukum yang ada.

Teknik pengumpulan data yang digunakan dalam penelitian ini adalah studi kepustakaan, atau *library research*. Teknik ini mengharuskan peneliti untuk mengumpulkan dan mempelajari berbagai literatur yang berkaitan dengan topik yang diteliti. Sumber-sumber literatur yang digunakan meliputi buku-buku, jurnal ilmiah, serta penelitian-penelitian sebelumnya yang relevan. Proses pengumpulan data ini bertujuan untuk mendapatkan pemahaman yang lebih mendalam mengenai teori-teori hukum yang ada serta praktik perlindungan data pribadi yang diatur oleh hukum yang berlaku. Penulis juga berupaya untuk memastikan bahwa bahan pustaka yang digunakan berasal dari referensi yang kredibel dan relevan dengan topik penelitian.

Metode analisis yang diterapkan dalam penelitian ini adalah analisis deskriptif kualitatif. Data dianalisis dengan cara yang tidak mengandalkan angka, melainkan menggunakan deskripsi atau gambaran yang disampaikan dengan kata-kata. Analisis ini mengambil data dari dokumen-dokumen hukum yang ada, seperti peraturan perundang-undangan dan sumber hukum lainnya. Metode ini bertujuan untuk menggambarkan secara jelas dan mendalam mengenai berbagai regulasi yang berkaitan dengan perlindungan data pribadi. Penulis menggunakan model analisis interaktif dalam proses analisis data ini, yang terdiri dari tiga langkah utama: reduksi data, sajian data, dan penarikan kesimpulan.

Tahap pertama, yaitu reduksi data, peneliti menyaring dan menyusun data yang telah dikumpulkan agar lebih jelas dan terfokus. Reduksi data ini bertujuan untuk menghilangkan informasi yang tidak relevan atau tidak penting, sehingga data yang tersisa lebih mudah dipahami dan dianalisis lebih lanjut. Setelah data dianalisis, langkah berikutnya adalah sajian data, yaitu penyajian data yang sudah dianalisis secara sistematis agar mudah dipahami oleh pembaca. Peneliti berusaha menyajikan data dalam bentuk yang jelas dan mudah diikuti, sehingga pembaca dapat memperoleh pemahaman yang mendalam mengenai hasil penelitian.

Langkah terakhir adalah penarikan kesimpulan. Tahap ini, penulis menarik kesimpulan berdasarkan data yang telah diperiksa dan dianalisis. Sebelum kesimpulan diambil, peneliti memastikan bahwa data yang digunakan telah diverifikasi untuk keakuratannya dan validitasnya. Kesimpulan yang ditarik diharapkan dapat memberikan gambaran yang jelas tentang perlindungan data pribadi dalam kerangka hukum yang ada di Indonesia, khususnya yang terkait dengan Undang-Undang Nomor 27 Tahun 2022. Proses ini juga memastikan bahwa hasil penelitian yang disajikan dapat dipertanggungjawabkan secara ilmiah dan memiliki relevansi yang kuat terhadap permasalahan hukum yang sedang dibahas.

Hasil

Perlindungan Hukum terhadap Data Pribadi

Perkembangan pesat Teknologi Informasi di era digital telah membawa perubahan besar dalam berbagai aspek kehidupan manusia, salah satunya dalam pengelolaan data pribadi. Data pribadi kini dianggap sebagai aset berharga yang memerlukan perlindungan serius dalam dunia digital. Penyalahgunaan data pribadi dapat berisiko menimbulkan dampak yang sangat merugikan, seperti penipuan, pencurian identitas, dan pelanggaran privasi. Oleh karena itu, dibutuhkan regulasi yang tegas untuk melindungi hak individu atas data pribadi mereka. Untuk menjawab kebutuhan ini, Undang-Undang Perlindungan Data Pribadi (UU PDP) disusun untuk memberikan perlindungan hukum bagi data pribadi masyarakat di era digital. Undang-undang ini mencakup berbagai aturan mengenai pengumpulan, pengelolaan, dan penggunaan data pribadi oleh pihak ketiga, serta menetapkan sanksi yang tegas bagi pihak yang melanggar hak privasi data pribadi konsumen. Samuel Abrijani Pangerapan, Dirjen Aplikasi dan Informatika (Aptika), menjelaskan bahwa data pribadi merupakan bagian dari hak asasi manusia dan privasi yang diakui dalam Pasal 12 Deklarasi Universal Hak Asasi Manusia 1948. UU Perlindungan Data Pribadi bertujuan untuk mengurangi pelanggaran terhadap privasi serta meningkatkan kesadaran masyarakat dalam menjaga keamanan data pribadi mereka.

Peraturan terkait Perlindungan Data Pribadi telah ada sebelum disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, pengaturan terkait perlindungan data pribadi di Indonesia tersebar dalam beberapa undang-undang, antara lain: Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, yang merupakan perubahan dari Undang-Undang Nomor 7 Tahun 1992; Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi; Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia; Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik; Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan; Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan; Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggara Sistem dan Transaksi Elektronik; serta Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

Kebocoran Data Pribadi di Era Digital

Data pribadi merujuk pada segala informasi yang berkaitan dengan individu yang tersimpan dalam sistem elektronik atau non-elektronik, yang memungkinkan identifikasi langsung atau tidak langsung. Informasi ini bisa berupa data tunggal atau hasil penggabungan dengan data lainnya. Data pribadi mencakup berbagai informasi seperti nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, nomor telepon, alamat email, alamat surat menyurat, nomor identitas seperti KTP atau paspor, serta informasi keuangan seperti nomor rekening bank, nomor kartu kredit, dan riwayat transaksi.

Data pribadi yang tersimpan dalam sistem elektronik membentuk jejak digital yang sulit dihapus, sehingga penting untuk memberikan perlindungan guna mencegah kebocoran dan penyalahgunaan data tersebut. Meskipun demikian, dalam praktiknya sering kali terjadi kesalahan yang tidak disengaja akibat sistem keamanan yang kurang memadai, sehingga membuka celah bagi pihak yang tidak bertanggung jawab untuk mencuri, memperjualbelikan, atau memanfaatkan data pribadi untuk tujuan yang tidak sah. Beberapa insiden kebocoran data yang mencuat di Indonesia selama era digital antara lain kebocoran data *Tokopedia* pada 2020, kebocoran data *Kredit Plus* pada 2020, peretasan terhadap situs BPJS Kesehatan pada 2021, kebocoran data kartu SIM prabayar pada 2022, serta kebocoran data nasabah Bank Syariah Indonesia pada 2023.

Perlindungan Data Pribadi Berdasarkan Undang-Undang nomor 27 Tahun 2022

Indonesia kini memiliki regulasi khusus yang mengatur perlindungan data pribadi melalui Undang-Undang Nomor 27 Tahun 2022, yang disahkan oleh pemerintah dan DPR pada 20 September 2022 dan mulai berlaku pada 17 Oktober 2022. Undang-undang ini bertujuan memberikan kepastian hukum untuk menjamin perlindungan data pribadi masyarakat. Pasal 1 ayat (2) Undang-Undang tersebut menyatakan bahwa "Perlindungan data pribadi adalah upaya menyeluruh untuk melindungi data pribadi dalam proses pengolahan data guna menjamin hak konstitusional subjek data pribadi." Hal ini menegaskan bahwa data pribadi dilindungi oleh hukum sebagai bagian dari hak dasar warga negara. Berdasarkan Pasal 2 ayat (1), Undang-Undang Perlindungan Data Pribadi berlaku untuk semua pihak, termasuk individu, badan publik, dan organisasi internasional. Hal ini mencakup pengaturan baik di dalam maupun luar wilayah Indonesia, dengan dampak hukum yang berlaku di Indonesia. Asas ini mencerminkan prinsip *extra territorial* dalam hukum Indonesia, yang mengatur perlindungan data pribadi di tingkat global. Sejalan dengan itu, Undang-Undang ini mengadopsi prinsip yurisdiksi perlindungan yang mengikat seluruh pihak yang memproses data pribadi, baik di dalam maupun luar negeri, selama memiliki dampak hukum di Indonesia.

Upaya untuk melindungi dan menjamin hak atas data pribadi, Undang-Undang ini menetapkan delapan asas utama, yaitu perlindungan, kepastian hukum, kepentingan umum, kemanfaatan, kehati-hatian, keseimbangan, pertanggungjawaban, dan kerahasiaan, sebagaimana diatur dalam Pasal 3. Data pribadi yang dilindungi meliputi informasi yang dapat mengidentifikasi individu secara langsung atau tidak langsung, baik dalam sistem elektronik maupun non-elektronik. Pasal 4 mengategorikan data pribadi menjadi dua jenis: spesifik dan umum. Data spesifik meliputi informasi kesehatan, biometrik, genetika, catatan kejahatan, data anak, dan lainnya sesuai peraturan yang berlaku, sementara data umum mencakup nama, jenis kelamin, kewarganegaraan, agama, status perkawinan, serta data yang dapat mengidentifikasi seseorang. Pasal 5 menyatakan bahwa subjek data pribadi berhak untuk mendapatkan informasi mengenai identitas, dasar hukum, tujuan pengumpulan data, dan akuntabilitas pihak yang meminta data tersebut. Undang-Undang ini memberikan kendali yang lebih besar kepada subjek data atas pengolahan data pribadinya, dengan fokus pada perlindungan hak-hak subjek data. Pasal 12 menegaskan hak subjek data untuk menggugat dan menerima ganti rugi jika

terjadi pelanggaran terhadap pemrosesan data pribadinya. Ketentuan lebih lanjut mengenai tata cara dan pengenaan ganti rugi atas pelanggaran ini akan diatur dalam peraturan pemerintah. Undang-undang ini memperkuat perlindungan hak privasi dan memberikan jalur hukum bagi individu untuk mengklaim hak mereka terkait data pribadi.

Pasal 13 ayat (1) dan (2) Undang-Undang Perlindungan Data Pribadi mengatur bahwa subjek data pribadi berhak untuk memperoleh dan menggunakan data pribadi miliknya dari pengendali data pribadi dalam format yang umum digunakan dan dapat dibaca oleh sistem elektronik. Selain itu, subjek data juga berhak untuk mentransfer data pribadinya ke pengendali data pribadi lain, dengan catatan bahwa sistem yang digunakan harus dapat berkomunikasi dengan aman sesuai dengan prinsip perlindungan data pribadi yang tercantum dalam undang-undang ini. Ketentuan lebih lanjut mengenai hak subjek data pribadi untuk mengakses dan mengirimkan data pribadi akan diatur dalam peraturan pemerintah. Undang-Undang ini juga mengatur tentang pemrosesan data pribadi dalam Pasal 16, yang menjadi prinsip dasar perlindungan data pribadi. Pemrosesan data pribadi mencakup berbagai kegiatan, seperti pengumpulan, pengolahan, analisis, penyimpanan, pembaruan, hingga penghapusan atau pemusnahan data. Pemrosesan tersebut harus dilakukan sesuai dengan prinsip perlindungan data pribadi, yaitu data harus diproses secara sah, terbatas, dan transparan.

Selain itu, tujuan pemrosesan harus jelas, akurat, lengkap, serta tidak menyesatkan dan harus dilakukan dengan menjamin hak subjek data. Pemrosesan data pribadi juga harus mengutamakan perlindungan terhadap data dari akses atau pengungkapan yang tidak sah, serta memastikan data dimusnahkan atau dihapus setelah periode retensinya berakhir, kecuali ada ketentuan lain dalam peraturan perundang-undangan. Pasal 19 dari undang-undang ini mengatur tentang pengendali data pribadi dan prosesor data pribadi, yang melibatkan individu, badan publik, dan organisasi internasional. Pengendali data pribadi adalah pihak yang menentukan tujuan dan mengendalikan pengolahan data pribadi, baik secara mandiri maupun bersama-sama. Sedangkan prosesor data pribadi adalah pihak yang memproses data pribadi atas nama pengendali data pribadi. Pasal 20 ayat (1) dan (2) menyatakan bahwa pengendali data pribadi wajib memiliki dasar hukum yang sah untuk memproses data pribadi. Dasar pemrosesan ini mencakup persetujuan eksplisit dari subjek data pribadi untuk tujuan tertentu, pemenuhan kewajiban perjanjian, pemenuhan kewajiban hukum, perlindungan kepentingan vital subjek data, atau pelaksanaan tugas untuk kepentingan umum dan pelayanan publik. Selain itu, pemrosesan data pribadi juga dapat dilakukan untuk memenuhi kepentingan sah lainnya, dengan mempertimbangkan keseimbangan antara kepentingan pengendali data dan hak subjek data pribadi. Pasal 21 ayat (1) Undang-Undang Perlindungan Data Pribadi mengatur bahwa dalam pemrosesan data pribadi, pengendali data pribadi wajib menyampaikan informasi yang jelas mengenai legalitas pemrosesan, tujuan pemrosesan, jenis dan relevansi data yang akan diproses, durasi penyimpanan data pribadi, serta rincian terkait informasi pemrosesan tersebut dan subjek data pribadi. Selain itu, Pasal 21 ayat (2) menegaskan bahwa jika ada perubahan terhadap informasi yang telah disampaikan sebelumnya, pengendali data pribadi harus memberitahukan perubahan tersebut kepada subjek data sebelum perubahan.

Berdasarkan pasal-pasal tersebut, jelas bahwa pemrosesan data pribadi hanya dapat dilakukan dengan persetujuan yang sah dari subjek data pribadi. Selain itu, pengendali data pribadi wajib memberikan informasi yang cukup tentang tujuan pemrosesan data pribadi tersebut. Persetujuan untuk pemrosesan data pribadi diatur lebih lanjut dalam Pasal 22, yang menetapkan bahwa persetujuan harus diberikan secara tertulis atau terekam, baik secara elektronik maupun non-elektronik, dengan kekuatan hukum yang setara. Jika persetujuan tersebut mencakup tujuan tambahan, maka harus dipisahkan dengan jelas dari informasi lainnya, menggunakan format yang mudah dipahami, dan bahasa yang sederhana. Apabila persetujuan tidak memenuhi ketentuan ini, maka akan dianggap batal demi hukum.

Undang-Undang Perlindungan Data Pribadi juga memberikan perhatian khusus pada pemrosesan data pribadi anak, seperti yang diatur dalam Pasal 25. Pemrosesan data anak harus dilakukan dengan persetujuan orang tua atau wali anak, sesuai dengan ketentuan yang berlaku. Berdasarkan Pasal 1 Konvensi Hak Anak (CRC), anak adalah individu yang berusia di bawah 18 tahun. Anak-anak memiliki kerentanannya sendiri karena mereka mungkin tidak sepenuhnya memahami dampak jangka panjang dari pemberian persetujuan untuk pengumpulan data pribadi mereka. Undang-undang ini juga memberikan perhatian khusus terhadap pemrosesan data pribadi bagi penyandang disabilitas, yang diatur dalam Pasal 26. Pemrosesan data pribadi bagi penyandang disabilitas harus dilakukan dengan cara yang sesuai dengan kebutuhan komunikasi mereka, dan harus memperoleh persetujuan dari penyandang disabilitas atau wali mereka sesuai dengan ketentuan peraturan yang berlaku.

Pasal 22 Undang-Undang Perlindungan Data Pribadi memberikan hak kepada penyandang disabilitas untuk mendapatkan perlindungan atas privasi mereka, yang mencakup kehidupan pribadi, keluarga, tempat tinggal, korespondensi, dan komunikasi lainnya. Perlindungan ini bertujuan untuk menjaga kehormatan dan reputasi penyandang disabilitas dari gangguan, serta memberikan hak hukum yang sah. Selain itu, dalam proses pemrosesan data pribadi, pengendali data diwajibkan untuk menjaga keamanan data pribadi sesuai dengan Pasal 35, yang mengharuskan pengendali data untuk mengambil langkah-langkah operasional dan teknis untuk melindungi data pribadi dari pemrosesan yang tidak sesuai dengan ketentuan hukum yang berlaku. Pengendali data juga perlu menetapkan tingkat keamanan yang sesuai berdasarkan sifat dan risiko data pribadi yang diproses.

Pasal 38 mengatur kewajiban pengendali data untuk melindungi data pribadi dari pemrosesan yang tidak sah. Hal ini sesuai dengan prinsip dasar dalam Undang-Undang Perlindungan Data Pribadi, yang mengharuskan pemrosesan data dilakukan secara sah, terbatas, spesifik, dan transparan. Pemrosesan data pribadi hanya dibolehkan jika ada dasar hukum yang sah, sebagaimana diatur dalam Pasal 20 ayat (2), dan pengendali data bertanggung jawab untuk memastikan bahwa semua pemrosesan dilakukan sesuai dengan ketentuan hukum. Jika pemrosesan dilakukan tanpa dasar hukum yang sah, pengendali data akan dikenakan sanksi.

Undang-Undang ini juga mencakup ketentuan mengenai penghapusan data pribadi dalam Pasal 43. Pengendali data wajib menghapus data pribadi jika data tersebut tidak lagi diperlukan untuk tujuan pemrosesan, jika subjek data mencabut persetujuan pemrosesan, jika ada permintaan penghapusan dari subjek data, atau jika data tersebut diperoleh dan diproses secara ilegal. Hal ini dikenal sebagai hak untuk dilupakan (*The Right to be Forgotten*). Namun, hak ini tidak bersifat mutlak dan hanya berlaku dalam kondisi tertentu.

Pengendali data diwajibkan untuk memberitahukan kegagalan perlindungan atau kebocoran data kepada subjek data pribadi dan lembaga yang berwenang dalam waktu 3 x 24 jam jika terjadi pelanggaran terhadap perlindungan data pribadi, sebagaimana diatur dalam Pasal 46. Pemberitahuan tertulis ini harus mencakup informasi terkait data yang terungkap, waktu dan cara pengungkapan data, serta langkah-langkah yang diambil untuk menangani dan memulihkan kebocoran tersebut. Pengendali data juga harus memberitahukan masyarakat mengenai kejadian kebocoran data tersebut. Pemberitahuan ini mengimplementasikan prinsip akuntabilitas, yang mengharuskan pengendali data untuk transparan dalam menangani pelanggaran terhadap perlindungan data pribadi.

Undang-Undang Perlindungan Data Pribadi mengatur sanksi administratif bagi pihak yang gagal melindungi data pribadi, sebagaimana tercantum dalam Pasal 57. Pelanggaran terhadap berbagai pasal yang berkaitan dengan pemrosesan data pribadi dapat dikenakan sanksi administratif, yang mencakup peringatan tertulis, penghentian sementara pemrosesan data pribadi, penghapusan atau pemusnahan data pribadi, dan denda administratif. Denda yang dikenakan dapat mencapai dua persen dari pendapatan tahunan atau penerimaan tahunan yang terkait dengan pelanggaran tersebut. Pemberian sanksi administratif ini dilakukan oleh lembaga yang ditunjuk, dan prosedur lebih lanjut mengenai pengenaan sanksi diatur dalam Peraturan Pemerintah.

Pasal 57 mencakup tanggung jawab pengendali data pribadi terkait dengan 30 pasal yang mengatur ketentuan perlindungan data pribadi. Jika pelanggaran terhadap ketentuan-ketentuan ini terjadi, subjek data pribadi dapat mengajukan tuntutan kepada lembaga yang berwenang. Lembaga Pengawas Pelindungan Data Pribadi akan memberikan sanksi administratif sesuai dengan hasil pemeriksaan. Selain itu, undang-undang ini juga mengatur pembentukan kelembagaan yang berfungsi untuk melindungi dan mengawasi pemrosesan data pribadi oleh pengendali dan prosesor data. Pasal 58 menyatakan bahwa pemerintah memiliki peran penting dalam penyelenggaraan perlindungan data pribadi, yang dilaksanakan oleh lembaga yang ditunjuk oleh Presiden. Lembaga ini bertanggung jawab langsung kepada Presiden, dan ketentuan lebih lanjut mengenai lembaga ini diatur dengan Peraturan Presiden.

Pasal 59 menjelaskan lebih lanjut mengenai peran lembaga tersebut, yang mencakup merumuskan dan menetapkan kebijakan serta strategi perlindungan data pribadi, mengawasi penerapan perlindungan data pribadi, menegakkan hukum administratif terkait pelanggaran yang terjadi, dan memfasilitasi penyelesaian sengketa di luar pengadilan. Lembaga ini berfungsi sebagai panduan bagi subjek data pribadi, pengendali, dan prosesor data pribadi.

Selain itu, lembaga pengawas juga memiliki kewenangan untuk memastikan penerapan kebijakan dan strategi perlindungan data pribadi, serta menegakkan sanksi administratif apabila terjadi pelanggaran, sebagaimana diatur dalam Pasal 57.

Pasal 60 Undang-Undang Perlindungan Data Pribadi mengatur tentang kewenangan lembaga yang bertanggung jawab atas perlindungan data pribadi, sebagaimana diatur dalam Pasal 58 ayat (2). Lembaga ini memiliki sejumlah kewenangan penting, di antaranya merumuskan kebijakan terkait perlindungan data pribadi, melakukan pengawasan terhadap kepatuhan pengendali data pribadi, dan menjatuhkan sanksi administratif jika terjadi pelanggaran. Selain itu, lembaga ini juga berperan dalam membantu aparat penegak hukum dalam menangani dugaan tindak pidana terkait data pribadi, bekerja sama dengan lembaga perlindungan data pribadi negara lain untuk menyelesaikan pelanggaran lintas negara, serta melakukan penilaian terhadap pemenuhan persyaratan transfer data pribadi ke luar wilayah Indonesia. Lembaga ini juga memiliki kewenangan untuk memberi perintah tindak lanjut kepada pengendali dan prosesor data pribadi, mempublikasikan hasil pengawasan, serta menerima laporan atau aduan tentang pelanggaran perlindungan data pribadi. Lebih lanjut, lembaga ini dapat memanggil pihak-pihak terkait, meminta keterangan dan dokumen, serta melakukan pemeriksaan terhadap sistem elektronik yang digunakan oleh pengendali dan prosesor data pribadi, termasuk meminta bantuan hukum kepada kejaksaan dalam penyelesaian sengketa terkait perlindungan data pribadi.

Pasal 63 dalam Undang-Undang Perlindungan Data Pribadi menekankan pentingnya peran masyarakat dalam melindungi data pribadi. Masyarakat dapat terlibat langsung atau tidak langsung dalam upaya perlindungan data pribadi, melalui berbagai kegiatan seperti pendidikan, pelatihan, advokasi, sosialisasi, dan pengawasan sesuai dengan ketentuan yang berlaku. Hal ini membuka peluang bagi berbagai pihak untuk berkontribusi, termasuk melalui pendidikan formal di sekolah dari tingkat dasar hingga perguruan tinggi, serta pelatihan yang diselenggarakan oleh lembaga nonformal. Edukasi dan penyuluhan kepada masyarakat dapat membantu mereka memahami hak-hak mereka dalam menjaga data pribadi dan mencegah pelanggaran. Pasal 64 mengatur tentang penyelesaian sengketa yang berkaitan dengan perlindungan data pribadi. Sengketa tersebut dapat diselesaikan melalui berbagai mekanisme, seperti *arbitrase*, pengadilan, atau lembaga penyelesaian sengketa alternatif lainnya, sesuai dengan ketentuan hukum yang berlaku. Proses peradilan terkait perlindungan data pribadi juga diatur berdasarkan hukum acara yang berlaku, memberikan landasan yang jelas bagi penyelesaian sengketa yang muncul terkait perlindungan data pribadi.

Undang-Undang Perlindungan Data Pribadi mengatur alat bukti yang sah dalam kasus pelanggaran data pribadi, yang meliputi alat bukti sesuai dengan hukum acara yang berlaku, serta bukti lain yang berupa informasi elektronik dan dokumen elektronik sesuai dengan peraturan yang ditetapkan. Proses persidangan dapat dilakukan secara tertutup jika diperlukan untuk melindungi data pribadi. Selain itu, Undang-Undang ini juga menyediakan berbagai mekanisme penyelesaian sengketa, baik melalui jalur litigasi maupun nonlitigasi, termasuk *arbitrase*, yang dilaksanakan sesuai dengan ketentuan hukum acara yang berlaku.

Pasal 65 dalam Undang-Undang ini menetapkan larangan terkait penggunaan data pribadi. Setiap individu dilarang secara melawan hukum untuk mengumpulkan atau memperoleh data pribadi yang bukan miliknya dengan tujuan untuk keuntungan pribadi atau pihak lain, yang dapat menyebabkan kerugian bagi subjek data pribadi. Selain itu, pasal ini juga melarang pengungkapan dan penggunaan data pribadi orang lain secara tidak sah, yang dipandang sebagai pelanggaran hukum. Ketentuan ini memberikan dasar hukum bagi subjek data untuk mengajukan gugatan jika terjadi pelanggaran, sejalan dengan prinsip perbuatan melawan hukum yang diatur dalam Pasal 1365 Kitab Undang-Undang Hukum Perdata (BW).

Lebih lanjut, Pasal 66 mengatur larangan untuk membuat atau memalsukan data pribadi dengan tujuan untuk keuntungan pribadi atau pihak lain, yang dapat merugikan orang lain. Pasal ini juga mencakup larangan terhadap tindakan *phishing*, yang dilakukan dengan cara memalsukan data untuk menipu korban dan mendapatkan informasi sensitif. *Phishing* seringkali dilakukan melalui komunikasi elektronik seperti email atau pesan instan dengan menyamar sebagai pihak atau perusahaan yang terpercaya. Tindakan ini dapat dikenakan sanksi hukum, baik perdata maupun pidana, karena menimbulkan kerugian bagi pihak yang menjadi korban.

Pasal 67 mengatur sanksi pidana bagi pelaku yang dengan sengaja memperoleh atau mengumpulkan data pribadi orang lain secara ilegal, dengan tujuan untuk keuntungan diri sendiri atau pihak lain, yang mengakibatkan kerugian bagi subjek data pribadi. Pelaku dapat dikenakan pidana penjara hingga lima tahun dan/atau denda maksimal sebesar Rp5.000.000.000. Sementara itu, Pasal 68 mengatur sanksi pidana lebih berat bagi pelaku yang memalsukan data pribadi dengan tujuan yang sama, yang dapat dijatuhi pidana penjara hingga enam tahun dan/atau denda maksimal Rp6.000.000.000. Selain pidana utama, Pasal 69 mengatur bahwa pelaku juga dapat dikenakan pidana tambahan berupa perampasan keuntungan atau harta kekayaan yang diperoleh dari tindak pidana tersebut, serta kewajiban membayar ganti rugi atas kerugian yang ditimbulkan.

Pasal 67 dan Pasal 68 dilakukan oleh korporasi, sanksi pidana dapat dijatuhkan kepada pengurus, pemegang kendali, pemberi perintah, pemilik manfaat, dan/atau korporasi itu sendiri. Sanksi utama bagi korporasi adalah pidana denda, yang jumlahnya dapat mencapai sepuluh kali lipat dari batas maksimal denda yang ditetapkan. Selain pidana denda, korporasi juga bisa dijatuhi hukuman tambahan, seperti perampasan keuntungan atau harta kekayaan yang diperoleh dari tindak pidana, pembekuan sebagian atau seluruh kegiatan usaha, pelarangan permanen untuk melakukan tindakan tertentu, penutupan sebagian atau seluruh tempat usaha, pemenuhan kewajiban yang terabaikan, pembayaran ganti rugi, pencabutan izin, bahkan pembubaran korporasi.

Berdasarkan ketentuan yang tercantum dalam Pasal 67 Ayat (1) dan Ayat (3) Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, pelaku pencurian data pribadi dapat dikenakan pidana penjara maksimal lima tahun dan/atau denda hingga lima miliar rupiah. Selain itu, pelaku juga bisa dikenakan pidana tambahan, seperti

perampasan keuntungan atau harta yang diperoleh dari tindak pidana dan kewajiban untuk membayar ganti rugi. Jika tindak pidana tersebut dilakukan oleh korporasi, maka sanksi tersebut bisa dijatuhkan kepada pengurus, pengendali, pemberi perintah, atau bahkan korporasi itu sendiri, dengan pidana denda sebagai sanksi utama. Korporasi yang terbukti melakukan pelanggaran juga dapat dikenakan berbagai sanksi tambahan, seperti perampasan harta, pembekuan usaha, pembatasan aktivitas tertentu, dan berbagai hukuman lainnya, termasuk pembubaran. Mengingat pentingnya data pribadi sebagai aset berharga dalam era big data dan ekonomi digital, perlindungannya bertujuan untuk mengurangi pelanggaran privasi, mencegah penyalahgunaan data, serta meningkatkan kesadaran masyarakat untuk menjaga keamanan data pribadi mereka.

Pembahasan

Kelebihan dan Kekurangan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

Undang-Undang Perlindungan Data Pribadi (UU PDP) memiliki sejumlah kelebihan yang signifikan, terutama dalam upaya melindungi hak asasi manusia, khususnya hak individu dalam mengontrol data pribadi mereka. UU PDP mengadopsi prinsip-prinsip yang sejalan dengan regulasi perlindungan data pribadi di Uni Eropa, yaitu *General Data Protection Regulation* (GDPR). Prinsip-prinsip utama yang diatur dalam GDPR, seperti pengelola data (*Data Controller*), pemrosesan data (*Data Processor*), dan hak subjek data (*Data Subject Rights*), juga diatur dalam UU PDP. Selain itu, UU PDP mewajibkan pengelola data untuk bersikap transparan mengenai pengelolaan data pribadi, di mana setiap individu berhak mengetahui jenis data yang dikumpulkan, tujuan pengumpulannya, serta pihak yang akan menerima data tersebut. Hal ini meningkatkan kepercayaan masyarakat terhadap penggunaan data pribadi dalam era digital. Undang-Undang Perlindungan Data Pribadi juga menetapkan sanksi yang tegas, baik administratif maupun pidana, untuk pelanggaran perlindungan data pribadi. Sanksi tersebut meliputi peringatan tertulis, ganti rugi, denda besar, hingga hukuman penjara bagi individu atau organisasi yang terbukti melanggar. Tujuan dari sanksi ini adalah untuk memastikan pengelola data bertanggung jawab dan serius dalam menjaga keamanan data pribadi. Penelitian oleh beberapa ahli dalam bidang hukum dan perlindungan data pribadi, seperti temuan yang menunjukkan bahwa penerapan sanksi yang tegas dapat memberikan efek jera dan meningkatkan komitmen pihak pengelola data untuk mematuhi aturan (Matheus & Thalib, 2022).

Beberapa kelemahan yang perlu diperhatikan dalam implementasi UU PDP. Salah satunya adalah pengaturan mengenai pemrosesan data pribadi anak dan penyandang disabilitas. Pasal 25 dan 26 UU PDP mengharuskan pemrosesan data pribadi anak dan penyandang disabilitas dilakukan secara khusus dengan persetujuan orang tua atau wali. Namun, pengaturan ini masih terbatas dan tidak memberikan penjelasan rinci mengenai bentuk "penyelenggaraan khusus" yang dimaksud. Akibatnya, *platform* seperti media sosial dan *platform* pendidikan kurang memiliki pedoman yang jelas dalam mengelola data pribadi anak. Hal ini juga didukung

oleh hasil penelitian yang menunjukkan bahwa banyak perusahaan teknologi yang masih kebingungan dalam menyesuaikan kebijakan privasi mereka dengan regulasi perlindungan data pribadi anak yang baru (Mamonto, 2024). Undang-Undang Perlindungan Data Pribadi juga belum menetapkan batas usia yang jelas untuk menentukan siapa yang termasuk dalam kategori anak. Perbedaan definisi usia anak dalam berbagai peraturan perundang-undangan di Indonesia, seperti UU Perlindungan Anak, UU Perkawinan, dan KUH Perdata, menciptakan ketidakjelasan yang dapat berpotensi disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab. Penelitian sebelumnya juga mengungkapkan bahwa ketidakjelasan batas usia ini dapat menyulitkan penegakan hukum dalam kasus pelanggaran data pribadi anak (Daeng et al., 2023).

Kelemahan lain yang signifikan adalah belum disahkannya peraturan pelaksana untuk UU PDP. UU ini mengamanatkan pembentukan sepuluh peraturan pemerintah yang harus diterbitkan untuk menjamin perlindungan data pribadi di Indonesia. Namun, meskipun sudah lebih dari satu tahun sejak pengesahan UU PDP, belum ada satupun peraturan pemerintah yang diterbitkan. Hal ini menciptakan ketidakpastian hukum dan kekosongan regulasi dalam perlindungan data pribadi. Ketidakjelasan ini mengarah pada potensi penafsiran yang salah terhadap UU PDP dan membuka celah bagi meningkatnya kejahatan terkait data pribadi. Penelitian terdahulu yang juga menyoroti bahwa ketidakpastian hukum ini dapat merugikan individu yang data pribadinya terlindungi dengan tidak optimal (Rafasya et al., 2023). Pasal 12 ayat (1) UU PDP memberikan hak kepada pemilik data pribadi untuk menuntut ganti rugi atau menggugat Pengendali Data yang melanggar hak mereka. Namun, UU ini belum menjelaskan secara rinci mengenai mekanisme gugatan, termasuk prosedur, tata cara, atau pengadilan yang berwenang menangani kasus terkait perlindungan data pribadi. Ketidakjelasan ini semakin parah karena peraturan pelaksana yang seharusnya mengatur hal ini belum diterbitkan. Hal ini menyebabkan kekosongan hukum dan ketidakpastian terkait prosedur ganti rugi dan pengajuan gugatan, yang pada gilirannya melemahkan perlindungan data pribadi di Indonesia. Hal ini sejalan dengan hasil penelitian yang mencatat bahwa ketidakjelasan mekanisme ini menghambat individu untuk mendapatkan keadilan (Fauzy & Shandy, 2022).

Pembentukan lembaga *independen* yang khusus menangani perlindungan data pribadi juga belum terlaksana. Pasal 58 UU PDP mengamanatkan pembentukan lembaga yang bertanggung jawab langsung kepada Presiden dan memiliki 15 wewenang terkait penyelenggaraan perlindungan data pribadi. Namun, hingga saat ini, peraturan yang mengatur tata cara pelaksanaan wewenang lembaga ini belum juga diterbitkan. Pembentukan lembaga ini sangat penting untuk memastikan perlindungan data pribadi di Indonesia sesuai dengan standar yang ditetapkan oleh undang-undang, sekaligus meningkatkan kepercayaan masyarakat terhadap keamanan penggunaan data pribadi di era digital. Penelitian sebelumnya yang menunjukkan bahwa lembaga pengawas *independen* adalah salah satu elemen kunci dalam menciptakan sistem perlindungan data pribadi yang efektif dan terpercaya (Pranata et al., 2024). Keberadaan lembaga *independen* ini sangat penting, tidak hanya untuk memenuhi kewajiban yang diatur dalam UU PDP, tetapi juga untuk memenuhi standar internasional dalam

perlindungan data pribadi. Keberadaan lembaga pengawas independen menjadi syarat utama untuk menjamin perlindungan data pribadi yang optimal. Oleh karena itu, pemerintah perlu segera mengesahkan peraturan pemerintah mengenai pembentukan lembaga ini agar lembaga tersebut dapat melaksanakan tugas dan wewenangnya secara efektif.

Bentuk Perlindungan Hukum Undang-Undang Nomor 27 Tahun 2022

Perlindungan hukum merujuk pada upaya untuk melindungi subjek hukum melalui penerapan peraturan yang berlaku, yang disertai dengan sanksi untuk memastikan kepatuhan. Subjek hukum itu sendiri mencakup baik individu maupun badan hukum. Perlindungan hukum dapat dibedakan menjadi dua kategori: preventif dan represif. Perlindungan hukum preventif dilakukan oleh pemerintah untuk mencegah terjadinya pelanggaran, yang diatur dalam peraturan perundang-undangan dengan tujuan memberikan pedoman bagi pelaksanaan kewajiban. Sementara itu, perlindungan hukum represif diterapkan setelah terjadinya pelanggaran, berupa sanksi seperti denda, hukuman penjara, atau hukuman tambahan sebagai bentuk respons terhadap pelanggaran atau sengketa yang terjadi. Undang-Undang Perlindungan Data Pribadi memberikan perlindungan hukum yang serupa dalam konteks pengelolaan dan perlindungan data pribadi.

Perlindungan Hukum Preventif

Perlindungan hukum preventif dalam konteks data pribadi mencakup berbagai langkah penting untuk memastikan bahwa data pribadi tidak disalahgunakan. Salah satu langkah pertama yang wajib dilakukan oleh pengendali data adalah memperoleh persetujuan yang sah dan eksplisit dari subjek data sebelum memproses data pribadi mereka. Persetujuan ini bertujuan untuk mencegah penggunaan data tanpa izin yang sah. Hal ini sejalan dengan prinsip dasar dalam UU PDP, yang mengharuskan transparansi dan kontrol yang jelas bagi individu terkait penggunaan data pribadi mereka (Samin, 2024). Penelitian sebelumnya menunjukkan bahwa persetujuan yang jelas dan eksplisit dari subjek data dapat mengurangi risiko penyalahgunaan data dan meningkatkan kesadaran masyarakat tentang hak mereka dalam mengontrol data pribadi (Sutarli & Kurniawan, 2023).

Undang-Undang Perlindungan Data Pribadi juga memberikan hak kepada subjek data untuk mengakses, memperbarui, menghapus, dan menarik persetujuan terkait pemrosesan data pribadi mereka. Hal ini bertujuan untuk melindungi privasi individu dan memastikan bahwa data yang diproses tetap akurat, relevan, dan tidak berlebihan. Penelitian ini relevan dengan hasil temuan yang menegaskan bahwa pemberian hak-hak ini memungkinkan individu untuk tetap mengendalikan data pribadi mereka dalam lingkungan digital yang semakin kompleks dan terbuka (Muzairroh et al., 2024).

Pengelola data juga diwajibkan untuk melaporkan setiap *insiden* kebocoran data kepada lembaga yang berwenang serta kepada subjek data yang terdampak, sebagai langkah pencegahan terhadap dampak yang lebih serius. Pemberitahuan yang cepat dan transparan dapat mencegah penyalahgunaan data lebih lanjut dan memungkinkan individu untuk mengambil tindakan yang tepat, seperti mengganti kata sandi atau mengamankan akun

mereka. Penelitian sebelumnya mengungkapkan bahwa pengelolaan kebocoran data yang tepat waktu dapat mengurangi kerugian ekonomi dan reputasi yang dapat ditimbulkan oleh kebocoran data (Kesuma et al., 2021).

Penting untuk memberikan penyuluhan dan edukasi kepada masyarakat mengenai pentingnya perlindungan data pribadi dan cara-cara menjaga keamanannya. Edukasi ini dapat dilakukan melalui berbagai saluran, seperti media massa, seminar, dan materi pendidikan yang disertakan dalam kurikulum pendidikan di sekolah. Penelitian sebelumnya yang mendukung hal ini menunjukkan bahwa tingkat pemahaman masyarakat mengenai perlindungan data pribadi masih rendah, sehingga penyuluhan yang efektif dapat meningkatkan kesadaran dan meminimalkan risiko penyalahgunaan data (Prayuti, 2024). Masyarakat yang teredukasi dengan baik lebih cenderung untuk menggunakan layanan digital dengan bijak, memahami risiko yang ada, dan melindungi informasi pribadi mereka secara lebih proaktif.

Perlindungan Hukum Represif

Perlindungan hukum represif dalam Undang-Undang Perlindungan Data Pribadi (UU PDP) mencakup pemberian sanksi administratif, pidana, dan perdata kepada pihak yang melanggar ketentuan dalam UU ini. Sanksi administratif diberlakukan kepada pengendali dan prosesor data pribadi yang melanggar aturan dalam UU PDP. Bentuk sanksi administratif ini meliputi peringatan tertulis, penghentian sementara pemrosesan data pribadi, penghapusan atau pemusnahan data pribadi, serta denda administratif yang dapat mencapai dua persen dari pendapatan tahunan atau penerimaan tahunan, tergantung pada jenis pelanggaran yang dilakukan. Penelitian terdahulu yang relevan menunjukkan bahwa pemberian sanksi administratif yang proporsional dapat mendorong pengelola data untuk lebih berhati-hati dalam pemrosesan data pribadi (Putri et al., 2024). Kasus kebocoran data pribadi, seperti yang terjadi pada *Tokopedia* dan BPJS Kesehatan, dapat dikenakan sanksi administratif sesuai ketentuan dalam UU PDP, sebagai bentuk tanggung jawab terhadap perlindungan data pribadi yang dikelola.

Undang-Undang Perlindungan Data Pribadi juga mengatur sanksi pidana bagi individu maupun korporasi yang melanggar ketentuan dalam undang-undang ini. Sanksi pidana yang dapat dijatuhkan berupa pidana penjara, denda, dan pidana tambahan berupa perampasan keuntungan atau harta kekayaan yang diperoleh melalui tindak pidana tersebut, serta pembayaran ganti rugi. Pasal 67 UU PDP dengan jelas mengatur bahwa setiap orang yang dengan sengaja memperoleh, mengungkapkan, atau menggunakan data pribadi milik orang lain secara melawan hukum dapat dijatuhi pidana penjara hingga lima tahun dan/atau denda paling banyak lima miliar rupiah. Pelanggaran yang melibatkan pengungkapan data pribadi yang bukan miliknya dapat dikenakan pidana penjara paling lama empat tahun dan/atau denda hingga empat miliar rupiah. Penelitian sebelumnya yang mengkonfirmasi bahwa penerapan sanksi pidana yang tegas dapat memberikan efek jera yang lebih besar bagi pelaku pelanggaran data pribadi (Suari & Sarjana, 2023).

Terkait dengan pidana yang dapat dijatuhkan terhadap korporasi, UU PDP mengatur bahwa sanksi pidana terbatas pada pidana denda. Besaran denda yang dikenakan kepada korporasi dapat mencapai sepuluh kali lipat dari batas maksimal denda yang diatur dalam undang-undang. Selain denda, korporasi juga bisa dijatuhi pidana tambahan berupa perampasan keuntungan atau harta kekayaan yang diperoleh melalui tindak pidana, pembekuan sebagian atau seluruh kegiatan usaha, pelarangan permanen terhadap perbuatan tertentu, penutupan sebagian atau seluruh tempat usaha, pemenuhan kewajiban yang sebelumnya diabaikan, pembayaran ganti rugi, pencabutan izin, hingga pembubaran korporasi. Salah satu contoh kasus yang terkena sanksi pidana dalam UU PDP adalah kebocoran data *SIM card*, yang melibatkan pihak ketiga yang tidak bertanggung jawab dalam penyalahgunaan data pribadi.

Pasal 12 UU PDP mengatur bahwa proses pengajuan gugatan dan pemberian ganti rugi akan diatur lebih lanjut melalui peraturan pemerintah yang hingga kini belum disahkan. Ketidakjelasan mengenai mekanisme ini mengarah pada ketidakpastian hukum bagi pihak yang merasa dirugikan. Pelanggaran perlindungan data pribadi ini dapat digugat sebagai perbuatan melawan hukum berdasarkan Pasal 1365 Kitab Undang-Undang Hukum Perdata (KUHPerdata), yang menyatakan bahwa setiap perbuatan yang melanggar hukum dan merugikan pihak lain harus diganti kerugiannya. Penelitian terdahulu yang relevan menunjukkan bahwa kelemahan dalam prosedur gugatan ini dapat menambah kesulitan dalam menegakkan hak subjek data, terutama dalam mengajukan tuntutan atas pelanggaran yang terjadi (Saputra et al., 2024). Pasal 1366 KUHPerdata juga mengatur bahwa seseorang dapat dimintai pertanggungjawaban atas kelalaian atau ketidakhati-hatian dalam melakukan tindakan yang dapat merugikan orang lain. Perbuatan melawan hukum dianggap terjadi jika memenuhi unsur adanya tindakan yang melawan hukum, kesalahan, kerugian, dan hubungan sebab-akibat antara tindakan dan kerugian. Kasus kebocoran data pribadi yang dikenakan sanksi perdata dalam UU PDP termasuk kebocoran data dari *Kredit Plus* dan Bank Syariah Indonesia, yang menunjukkan bagaimana kerugian yang dialami individu dapat berlanjut pada tuntutan perdata berdasarkan prinsip ini.

Kesimpulan

Berdasarkan pembahasan mengenai Perlindungan Data Pribadi dalam Undang-Undang Nomor 27 Tahun 2022, dapat disimpulkan bahwa kemajuan teknologi informasi di era digital telah mengubah banyak aspek kehidupan, termasuk cara pengelolaan data pribadi. Data pribadi kini menjadi aset berharga yang perlu dilindungi agar tidak disalahgunakan, yang bisa mengakibatkan dampak serius seperti penipuan dan pencurian identitas. Oleh karena itu, UU PDP disusun untuk memberikan perlindungan hukum terhadap data pribadi dengan mengatur proses pengumpulan, pengelolaan, dan penggunaan data pribadi, serta menetapkan sanksi untuk pelanggarannya. Sebelumnya, perlindungan data pribadi diatur dalam berbagai undang-undang sektoral, namun hal ini masih belum memberikan perlindungan yang optimal. Kasus kebocoran data, seperti yang terjadi di *Tokopedia* dan BPJS Kesehatan, menunjukkan

pentingnya penguatan sistem keamanan. UU PDP diharapkan dapat meningkatkan keamanan dan kepatuhan terhadap standar perlindungan data. Indonesia kini memiliki regulasi yang lebih spesifik mengenai perlindungan data pribadi yang tercantum dalam UU Nomor 27 Tahun 2022, yang berlaku sejak 17 Oktober 2022. Undang-undang ini memberikan perlindungan hukum preventif dan represif, dengan kewajiban bagi pengendali data untuk mendapatkan persetujuan, melaporkan kebocoran data, dan melakukan edukasi kepada masyarakat. Meskipun UU ini menyediakan kerangka hukum yang menyeluruh, penerapannya yang efektif masih bergantung pada pembentukan peraturan pemerintah serta lembaga independen khusus yang menangani perlindungan data pribadi. Keterbatasan dari penelitian ini adalah belum adanya evaluasi menyeluruh terhadap efektivitas implementasi UU PDP, sehingga rekomendasi untuk penelitian selanjutnya adalah untuk menganalisis dampak nyata dari penerapan UU ini terhadap tingkat pelanggaran dan kepercayaan masyarakat terhadap pengelolaan data pribadi.

Acknowledgment

-

Daftar Pustaka

- Anantama, A., & Dewantara, J. K. H. (2022). Ancaman Data Pribadi di Era Digital Dalam Perspektif Islam. *Ath-Thariq: Jurnal dakwah dan komunikasi*, 6(02). <https://doi.org/10.32332/ath-thariq.v6i2.5431>
- Annan, A. (2024). Tinjauan Yuridis Perlindungan Data Pribadi Pada Sektor Kesehatan Berdasarkan Undang-Undang No. 27 Tahun 2022. *Synergy: Jurnal Ilmiah Multidisiplin*, 1(04), 247-254.
- 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.
- Fauzy, E., & Shandy, N. A. R. (2022). Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Lex Renaissance*, 7(3), 445-461. <https://doi.org/10.20885/JLR.vol7.iss3.art1>
- Hasan, Z., Putri, S. T., Gustina, S., Satria, A. R., Ramadhani, K. O., & Satrio, M. (2024). Tanggung Jawab Hukum Dan Ekonomi Dalam Perlindungan Data Pribadi Di Era Digital. *Causa: Jurnal Hukum dan Kewarganegaraan*, 7(12), 31-40. <https://doi.org/10.3783/causa.v7i12.7183>
- Hisbulloh, M. H. (2021). Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi. *Jurnal Hukum*, 37(2), 119-133. <http://dx.doi.org/10.26532/jh.v37i2.16272>
- Kesuma, A. N. D. H., Budiarta, I. N. P., & Wesna, P. A. S. (2021). Perlindungan Hukum Terhadap Keamanan Data Pribadi Konsumen Teknologi Finansial Dalam Transaksi Elektronik. *Jurnal Preferensi Hukum*, 2(2), 411-416. <https://doi.org/10.22225/jph.2.2.3350.411-416>

- Mahuli, J. I. (2023). Perlindungan Hukum Terhadap Data Pribadi dalam Era Digital. *All Fields of Science Journal Liaison Academia and Society*, 3(4), 188-194. <https://doi.org/10.58939/afosj-las.v3i4.710>
- Mamonto, D. F. (2024). Analisis Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022. *LEX PRIVATUM*, 13(4).
- Manurung, E. A. P., & Thalib, E. F. (2022). Tinjauan Yuridis Perlindungan Data Pribadi Berdasarkan Uu Nomor 27 Tahun 2022. *Jurnal Hukum Saraswati (JHS)*, 4(2), 139-148.
- Matheus, J., & Gunadi, A. (2024). Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital: Kajian Perbandingan Dengan KPPU. *JUSTISI*, 10(1), 20-35. <https://doi.org/10.33506/jurnaljustisi.v10i1.2757>
- Muzairoh, E., Suharso, S., Noviasari, D. T., & Syafingi, H. M. (2024). Analisis Perlindungan Hukum Terhadap Privasi Data Pribadi di Era Digital dalam Prespektif Hak Asasi Manusia. *Borobudur Law and Society Journal*, 3(1), 31-36. <https://doi.org/10.31603/11824>
- Pranata, A., Juono, A. A., & Binarida, A. V. Y. (2024). 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(3), 721-730.
- Prayuti, Y. (2024). Dinamika perlindungan hukum konsumen di era digital: Analisis hukum terhadap praktik e-commerce dan perlindungan data konsumen di Indonesia. *Jurnal Interpretasi Hukum*, 5(1), 903-913. <https://doi.org/10.22225/juinhum.5.1.8482.903-913>
- Priscyllia, F. (2019). Perlindungan privasi data pribadi perspektif perbandingan hukum. *Jatiswara*, 34(3), 239-249. <https://doi.org/10.29303/jtsw.v34i3.218>
- Putri, A., Sari, N., Fajrina, P., & Aisyah, S. (2024). Keamanan Online dalam Media Sosial: Pentingnya Perlindungan Data Pribadi di Era Digital (Studi Kasus Desa Pematang Jering). *Jurnal Pengabdian Nasional (JPN) Indonesia*, 6(1), 38-52. <https://doi.org/10.35870/jpni.v6i1.1097>
- Rafasya, R., Citra, H., & Fauzi, E. (2023). Perlindungan Hukum Terhadap Konsumen Atas Pencurian Data Pribadi dalam Transaksi Elektronik. *Jurnal Ilmu Sosial, Humaniora Dan Seni*, 2(1), 29-33.
- Raihan, M. (2023). Perlindungan Data Diri Konsumen Dan Tanggungjawab Marketplace Terhadap Data Diri Konsumen (Studi Kasus: Kebocoran Data 91 Juta Akun Tokopedia). *Jurnal Inovasi Penelitian*, 3(10), 7847-7856. <https://doi.org/10.47492/jip.v3i10.2513>
- Samin, H. H. (2024). Perlindungan Hukum Terhadap Kebocoran Data Pribadi Oleh Pengendali Data Melalui Pendekatan Hukum Progresif. *Jurnal Ilmiah Research Student*, 1(3), 1-15. <https://doi.org/10.61722/jirs.v1i3.386>

- Saputra, B. A., Kurnia, E., Rahmah, M., & Sumarni, T. (2024). Penerapan Privasi Dan Etika di Era Digital dalam Perlindungan Data Pribadi. *Musytari: Neraca Manajemen, Akuntansi, dan Ekonomi*, 5(9), 55-65. <https://doi.org/10.8734/musytari.v5i9.3570>
- 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>
- Sulistianingsih, D., Ihwan, M., Setiawan, A., & Prabowo, M. S. (2023). Tata kelola perlindungan data pribadi di era metaverse (telaah yuridis undang-undang perlindungan data pribadi). *Masalah-Masalah Hukum*, 52(1), 97-106.
- Suryanto, D., & Riyanto, S. (2024). Implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dalam Industri Ritel Tinjauan terhadap Kepatuhan dan Dampaknya pada Konsumen. *VERITAS*, 10(1), 121-135. <https://doi.org/10.34005/veritas.v10i1.3711>
- Sutarli, A. F., & Kurniawan, S. (2023). Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi Phising di Indonesia. *Innovative: Journal Of Social Science Research*, 3(2), 4208-4221.
- Widigdo, Z., & Rosando, A. F. (2023). Perlindungan Negara Terhadap Privasi Data Pribadi Dalam Layanan Sim Card Di Era Digital. *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, 3(1), 679-696. <https://doi.org/10.53363/bureau.v3i1.210>
- Zahwani, S. T., & Nasution, M. I. P. (2024). Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi Di Era Digital. *Journal of Sharia Economics Scholar (JoSES)*, 2(2). <https://doi.org/10.5281/zenodo.12608751>