Jurnal Legal Dialogica
Volume I Issue 2 Tahun 2026

TINJAUAN YURIDIS TINDAK PIDANA PELANGGARAN PRIVASI DATA PRIBADI DALAM ERA DIGITAL

Nursyahrani Sabila Elake[1], Mulyati Pawennei[2], Salle Salle[3]

[123]Fakultas Hukum, Universitas Muslim Indonesia

Email Koresponden : mulyatipawennai.fh@umi.ac.id

Abstrak: Penelitian ini bertujuan untuk mengetahui pengaturan hukum tindak pidana pelanggaran privasi data pribadi dalam era digital, serta mengetahui pertanggungjawaban pidana terhadap pelaku tindak pidana pelanggaran privasi data pribadi. Penelitian ini menggunakan metode penelitian hukum normatif. Pendekatan penelitian dengan melakukan pendekatan perundang undangan pendekatan konseptual dan pendekatan kasus. Jenis dan sumber data yang digunakan berupa bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Teknik pengumpulan bahan hukum yaitu Studi kepustakaan. Hasil analisis tersebut akan penulis hubungkan dengan permasalahan dalam penelitian ini untuk menghasilkan suatu penelitian obyektif untuk menjawab permasalahan dalam penelitian. Hasil penelitian ini menunjukan bahwa: 1. Pengaturan hukum tindak pidana pelanggaran privasi data pribadi dalam era digital di Indonesia diatur melalui peraturan mengenai perlindungan data pribadi dan sistem elektronik, yang menjadi dasar hukum dalam melindungi data pribadi serta menindak penggunaan, akses, dan penyalahgunaan data tanpa izin. 2. Pertanggungjawaban pidana terhadap pelaku pelanggaran privasi data pribadi dikenakan kepada setiap orang yang dengan sengaja dan melawan hukum memperoleh, menggunakan, mengungkapkan, atau memalsukan data pribadi orang lain, yang dapat dijatuhi sanksi pidana berupa penjara dan/atau denda sebagai bentuk penegakan hukum dan perlindungan hak privasi. Penelitian ini merekomendasikan, Pemerintah perlu memperkuat pelaksanaan perlindungan data pribadi melalui penyempurnaan dan perpaduan pengaturan antara Undang-Undang Perlindungan Data Pribadi dan Undang-Undang Informasi dan Transaksi Elektronik agar tidak terjadi tumpang tindih dalam penegakan hukum, memperepat pembentukan lembaga pengawas yang independen, peningkatan kapasitas aparat penegak hukum di bidang keamanan siber, serta peningkatan edukasi kepada masyarakat guna mencegah penyalahgunaan data pribadi di era digital.

Kata Kunci: Tindak Pidana, Pelanggaran, Data Pribadi, Era Digital.

Abstract: *This research aims to determine the legal regulations for criminal acts of violation of personal data privacy in the digital era, as well as to determine the criminal liability of perpetrators of criminal acts of violation of personal data privacy. This research uses a normative legal research method. The research approach uses a regulatory approach, a contextual approach, and a case approach. The types and sources of data used include primary legal materials, secondary legal materials, and tertiary legal materials. The legal material collection technique is literature study. The author will connect the results of this analysis with the research problem to produce an objective study to answer the research questions. The results of this study indicate that: 1. The legal provisions for criminal violations of personal data privacy in Indonesia in the digital era are regulated*

through regulations concerning personal data protection and electronic systems, which serve as the legal basis for protecting personal data and prosecuting unauthorized use, access, and chipping of data. 2. Criminal liability for perpetrators of personal data privacy violations applies to anyone who intentionally and unlawfully obtains, uses, discloses, or falsifies another person's personal data, and is subject to imprisonment and/or fines as a form of law enforcement and protection of privacy rights. This study recommends that the government strengthen the implementation of personal data protection by improving and integrating regulations between the Personal Data Protection Law and the Information and Electronic Transactions Law to prevent overlapping law enforcement, expediting the establishment of independent supervisory bodies, increasing the capacity of law enforcement officers in cybersecurity, and increasing public education to prevent personal data violations in the digital era.
Keywords: Criminal Acts, Violations, Personal Data, Digital Era.

PENDAHULUAN

Dalam era digital, perkembangan teknologi informasi dan komunikasi telah membawa perubahan besar dalam kehidupan manusia. Dalam prosesnya, data pribadi menjadi semakin penting dan sensitif karena banyak aktivitas yang dilakukan secara online. Data pribadi mencakup informasi seperti nama, alamat, nomor identitas, informasi finansial, riwayat kesehatan, dan informasi sensitif lainnya yang berkaitan dengan individu.

Di tengah era digital yang pesat, data pribadi individu semakin rentan terhadap potensi penyalahgunaan dan pelanggaran privasi. Keamanan data pribadi merupakan hak asasi manusia yang harus dijamin dan dihormati. Indonesia, sebagai negara berkembang dengan adopsi teknologi yang pesat, memiliki tanggung jawab untuk melindungi data pribadi sebagai hak privasi. Dalam konteks ini, hak privasi menjadi isu yang mendesak untuk diatasi. Hak privasi adalah hak asasi setiap individu untuk menjaga kerahasiaan dan keamanan data pribadi mereka. Dengan meningkatnya kasus pelanggaran privasi dan penyalahgunaan data pribadi, penting bagi setiap negara untuk memiliki peraturan perundang-undangan yang efektif untuk melindungi hak privasi warganya.

Di Indonesia, kesadaran akan perlunya perlindungan data pribadi telah semakin meningkat, terutama seiring dengan pertumbuhan penggunaan internet dan aplikasi berbasis teknologi. Hak membela diri merupakan salah satu hak hukum yang digariskan dalam UUD 1945. Menurut Pasal 28G Ayat (1), warga negara berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta miliknya. Namun demikian, dengan kemajuan teknologi informasi dan komunikasi, hak pribadi seharusnya tidak

hanya dipahami sebagai hak milik sebagaimana diatur dalam pasal tersebut. Hak privasi harus menjadi salah satu yang mendasar. Karena berurusan dengan informasi pribadi atau identitas seseorang, hak privasi lebih sensitif dan dapat dilihat sebagai hak pribadi. [1]

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan perlindungan hukum yang lebih kuat bagi individu terkait pengumpulan, penggunaan, dan penyebaran data pribadi mereka. Undang-undang ini juga mengatur mekanisme pengawasan dan penegakan hukum melalui pembentukan lembaga pengawas independen. Dalam konteks hukum pidana, undang undang ini mengatur sanksi terhadap pelanggaran data pribadi, seperti pencurian dan penyalahgunaan data. Perlindungan data pribadi menjadi semakin relevan dengan meningkatnya transaksi ecommerce dan perkembangan teknologi informasi. Namun, risiko kebocoran data pribadi juga meningkat, seperti kasus kebocoran data Tokopedia dan Facebook. Oleh karena itu, perlindungan hukum yang efektif dan regulasi yang kuat diperlukan untuk melindungi data pribadi dan hak privasi individu. Undang-Undang Nomor 27 Tahun 2022 menjadi landasan penting untuk mengatur perlindungan data pribadi di Indonesia, memastikan bahwa data pribadi dihormati dan dilindungi sesuai dengan kemajuan teknologi dan kebutuhan masyarakat. [2]

Namun demikian, dengan kemanjuan teknologi informasi dan komunikasi, hak pribadi seharusnya tidak hanya dipahami sebagai hak milik sebagaimana yang diatur dalam pasal tersebut. Hak Privasi harus menjadi salah satu yang mendasar Dengan demikian, dapat disimpulkan bahwa pengaturan perlindungan data pribadi di Indonesia masih bersifat sektoral. Perlu pengaturan perlindungan data pribadi pada tingkat hukum karena perlindungan data pribadi sebagai bagian dari privasi adalah hak asasi manusia. [3]

Tetapi contoh kebocoran data pribadi baru-baru ini menjadi masalah yang parah. Kebocoran data pribadi adalah masalah yang serius yang dapat menyebabkan kerugian finansial. Pada era sekarang hampir seluruh perangkat terhubung dan memiliki koneksi internet, semuanya dapat dikelola dari mana saja. Teknologi berbasi komputer untuk informasi dan komunikasi berkembang pesat di masa sekarang dalam kehidupan masyarakat. Kemajuan ini sangat membantu masyarakat. Meskipuin tersebar berbagai undang undang, perlindungan-perlindungan data pribadi di Indonesia. RUU

Perlindungan Data Pribadi (RUU PDT) yang dimiliki Indonesia saat ini perlu dikasi regulasinya masih perlu penyempurnaan. Supaya RUU PDT dapat disandingkan dengan undang-undang perlindungan data yang dimiliki oleh negara luar seperti Malaysia, Singapura, dan Korea Selatan. Perlindungan hukum atas data pribadi sudah dijamin oleh undang-undang khusus di beberapa negara tersebut. RUU PDT memiliki tujuan dan manfaat yang penting dalam konteks perlindunga privasi dan penggunaan data pribadi di Indonesia, dan bertujuan menciptakan lingkungan digital yang aman, terpercaya sambil tetap memungkinkan pertumbuhan ekonomi dan inovasi di era digital.

Indonesia mengalami peningkatan signifikan kasus pelanggaran privasi data pribadi dari 2020 hingga 2025.

1. 2020 (Tokopedia & KPU): Kebocoran 91 juta data pengguna Tokopedia (Mei 2020) dan 2,3 juta data pemilih Komisi Pemilihan Umum (KPU).
2. 2021 (BPJS Kesehatan): Dugaan kebocoran 279 juta data penduduk Indonesia, dengan 100.002 data terkonfirmasi bocor dan dijual di forum online.
3. 2022-2023 (Bjorka & Dukcapil): Serangkaian kebocoran data yang diklaim oleh peretas "Bjorka", termasuk data surat-menyurat negara. Terjadi juga dugaan kebocoran data 34 juta data paspor dan data Dukcapil.
4. 2023 (KPU): Dugaan kebocoran 204 juta data Daftar Pemilih Tetap (DPT) KPU.
5. 2024 (Pusat Data Nasional/PDN): Serangan ransomware pada PDN Sementara (PDNS 2) di Surabaya pada Juni 2024 yang melumpuhkan 282 layanan publik.
6. 2025 (Nasional & Daerah): Pada awal 2025, dilaporkan 210 instansi mengalami kebocoran data. Selain itu, terdapat kasus peretasan 4,5 juta data warga Jawa Barat oleh Digital Ghost.

Hal ini menekankan larangan untuk menjaga privasi orang lain, seperti tidak mencari-cari kesalahan (tajassus) atau mengganggu urusan pribadi. yang merupakan bentuk pelanggaran privasi. ini bisa dihubungkan dengan pelanggaran privasi data, di mana pencurian atau penyalahgunaan data pribadi mirip dengan bentuk tajassus modern. Prinsip ini mendukung perlindungan hukum pidana sebagai bentuk menjaga keadilan dan hak asasi, sesuai dengan era digital di Indonesia.

Dengan adanya variasi sistem hukum tersebut, maka asas universalitas dapat digunakan, khususnya untuk kepentingan 6 kepentingan global yang didasarkan pada anggapan bahwa setiap bangsa di dunia wajib ikut serta dalam melaksanakan sistem

hukum global tersebut. Berdasarkan Fenomena dan penyalahgunaan data privasi diatas, maka peneliti tertarik untuk mengkaji mengenai Bagaimana Prinsip Hak Privasi Terhadap Data Pribadi dan apakah Tanggung Jawab Indonesia Terhadap Data Pribadi sebagai Hak Privasi Melalui Peraturan Undang-Undangan. [4]

METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif. Penelitian hukum normatif adalah penelitian yang berfokus pada kajian terhadap norma-norma hukum positif, baik yang tertulis dalam peraturan perundang-undangan maupun yang terdapat dalam putusan pengadilan, doktrin, dan asas-asas hukum. Dalam konteks penelitian ini, pendekatan normatif digunakan untuk menganalisis pengaturan hukum pidana yang berkaitan dengan perlindungan terhadap pelanggaran privasi data pribadi di Indonesia, khususnya dalam menghadapi perkembangan era digital yang menimbulkan berbagai bentuk kejahatan siber (cybercrime).

PEMBAHASAN

1. **Pengaturan Hukum Tindak Pidana Pelanggaran Privasi Data Pribadi Dalam Era Digital**

   Di Indonesia saat ini telah disahkan peraturan yang mengatur tentang perlindungan data pribadi warga negara Indonesia yang tertuang dalam Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi dimana tercantum: Pasal 1 ayat (1) Data Pribadi, didefinisikan sebagai “Data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik” sedangkan pada Pasal 2 menjelaskan bahwa “Perlindungan Data Pribadi adalah keseluruhan Upaya untuk melindungi data pibadi dalam rangkaian pemrosesan data pribadi guna menjamin hak konstitusional subjek data pribadi”. Di dalam kedua pasal tersebut telah menegaskan bahwa data pribadi dilindungi oleh hukum sebagai jaminan hak dasar warga negara. [5]

   Selama bertahun-tahun, perlindungan data pribadi di Indonesia tidak memiliki landasan hukum yang kuat dan khusus. Sebelum disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), berbagai ketentuan mengenai perlindungan data terfragmentasi dalam sejumlah peraturan. Beberapa di antaranya adalah Undang-Undang Informasi dan Transaksi Elektronik

(UU ITE), Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta peraturan sektoral lainnya. Kondisi fragmentasi regulasi ini berujung pada inkonsistensi dalam penerapan hukum, ketidakjelasan mengenai kewenangan, dan lemahnya mekanisme penegakan hukum terhadap pelanggaran data pribadi.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), muncul sebagai langkah signifikan dalam sistem hukum Indonesia, bertujuan untuk menyediakan kerangka hukum yang lebih menyeluruh dan terpusat dalam mengatur hak-hak subjek data, kewajiban pengendali dan prosesor data, serta sanksi terhadap pelanggaran data pribadi. Undang-undang ini mengadopsi berbagai prinsip dari General Data Protection Regulation (GDPR) yang diterapkan di Uni Eropa, termasuk prinsip keabsahan pemrosesan data, hak untuk mengakses dan menghapus data, serta kewajiban untuk melaporkan kebocoran data. Namun, pelaksanaan UU PDP masih dihadapkan pada beberapa tantangan, seperti rendahnya kesadaran masyarakat mengenai hak-hak mereka, kurangnya kesiapan dari institusi pengendali data, serta 51 keterbatasan infrastruktur dan sumber daya manusia dalam bidang keamanan siber. [6]

Dalam konteks hukum, perlindungan data pribadi mencakup dua aspek penting: perlindungan terhadap privasi sebagai hak asasi manusia dan perlindungan terhadap data yang merupakan aset rentan terhadap penyalahgunaan. Hak atas privasi telah diakui secara konstitusional melalui Pasal 28G ayat (1) UUD 1945, yang menegaskan bahwa setiap individu berhak mendapatkan perlindungan terkait diri pribadi, keluarga, kehormatan, martabat, serta harta benda yang berada di bawah penguasaan mereka. Oleh karena itu, negara memiliki tanggung jawab untuk memastikan bahwa proses pengumpulan, penyimpanan, pengolahan, dan distribusi data pribadi dilakukan dengan cara yang sah, adil, dan transparan. [7]

Undang-undang Informasi dan Transaksi Elektronik selanjutnya disebut ITE memang belum memuat aturan perlindungan data pribadi secara khusus. Namun secara implisit undang-undang ini memunculkan pemahaman baru mengenai perlindungan terhadap keberadaan suatu data atau informasi elektronik baik yang bersifat umum maupun pribadi. Perlindungan data pribadi dalam sebuah sistem elektronik meliputi perlindungan dari penggunaan tanpa izin, perlindungan oleh

penyelenggara sistem elektronik, dan perlindungan dari akses dan interfensi illegal. Terkait dengan perlindungan data pribadi dari penggunaan tanpa izin, pasal 26 undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik mensyaratkan bahwa penggunaan setiap data pribadi dalam sebuah media elektronik harus mendapat persetujuan dari pemilik data bersangkutan. Setiap orang yang melanggar ketentuan ini dapat digugat atas kerugian yang ditimbulkan. Bunyi pasal 26 undang-undang ITE sebagai berikut: "Kecuali ditentukan lain oleh peraturan perundang undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan" sedangkan pada ayat (2) menjelaskan bahwa: "Setiap orang yang dilanggar haknya sebagaimana dimaksut pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan undang-undang ini". Pasal 26 ayat (1) menyatakan kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan. Ayat (2) kemudian menyatakan setiap orang yang dilanggar haknya sebagaimana dimaksut pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan undang-undang ini. Penjelasan pasal 26 ayat (1) menerangkan bahwa dalam pemanfaatan teknologi informasi, perlindungan data pibadi merupakan salah satu bagian dari hak pribadi (privasi right). Hak pribadi mengandung pengertian sebagai berikut: [8]

1) Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan;
2) Hak pribadi merupakan hak untuk dapat berkomunikasi dengan orang lain tanpa tindakan memata-matai;
3) Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.

Secara tegas undang-undang ITE melarang adanya akses secara melawan hukum kepada data milik orang lain melalui sistem elektronik untuk memperoleh informasi dengan cara menerobos sistem pengaman. Secara tegas undang-undang ITE menyatakan bahwa penyadapan (interception) adalah termasuk perbuatan yang dilarang kecuali dilakukan oleh pihak yang memiliki kewenangan untuk itu dalam

rangka upaya hukum. Berdasarkan undang-undang ITE ini juga, setiap orang dilarang dengan cara apapun untuk membuka informasi milik orang lain dengan tujuan apapun bahkan jika data yang sifatnya rahasia sampai dapat terbuka kepada publik. [9]

Perlindungan hukum merupakan langkah yang bertujuan untuk menjamin hak-hak subjek hukum melalui penerapan peraturan perundang-undangan yang berlaku, serta disertai dengan sanksi untuk memastikan kepatuhan terhadap ketentuan hukum tersebut. Subjek hukum yang dimaksud mencakup baik individu maupun badan hukum. [10] Dalam praktiknya, perlindungan hukum terbagi menjadi dua bentuk, yaitu preventif dan represif. Perlindungan hukum preventif bertujuan untuk mencegah terjadinya pelanggaran hukum. Bentuk ini umumnya dilakukan melalui penyusunan regulasi oleh pemerintah yang memberi pedoman dan rambu-rambu dalam menjalankan hak dan kewajiban hukum.

Sementara itu, perlindungan hukum represif diberikan setelah terjadinya pelanggaran atau sengketa, sebagai bentuk penegakan hukum yang dapat berupa pemberian sanksi administratif, denda, hukuman pidana, atau sanksi tambahan lainnya. Dalam konteks data pribadi, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi hadir sebagai dasar hukum yang memberikan jaminan perlindungan terhadap individu sebagai pemilik data. Undang undang ini tidak hanya mengatur hak dan kewajiban para pihak dalam pengelolaan data pribadi, tetapi juga menetapkan mekanisme preventif untuk mencegah kebocoran dan penyalahgunaan data, serta menyediakan jalur represif melalui sanksi hukum terhadap pelanggaran yang terjadi. [11]

1) Perlindungan Preventif Perlindungan hukum preventif dalam pengelolaan data pribadi mencakup serangkaian tindakan strategis untuk mencegah terjadinya penyalahgunaan data. Salah satu langkah utama yang harus dilakukan oleh pihak pengendali data adalah memperoleh persetujuan yang sah, eksplisit, dan berdasarkan kesadaran dari pemilik data sebelum data pribadi tersebut diproses. Persetujuan ini berfungsi sebagai bentuk perlindungan awal agar data tidak digunakan secara tidak sah atau tanpa sepengetahuan subjek data. Ketentuan ini sejalan dengan prinsip-prinsip fundamental yang tercantum dalam Undang Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, yang menekankan

pentingnya transparansi serta memberikan kendali penuh kepada individu atas data pribadi yang mereka miliki.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi memberikan sejumlah hak penting kepada subjek data, termasuk hak untuk mengakses, memperbarui, menghapus, serta menarik persetujuan atas pemrosesan data pribadi mereka. Pemberian hak-hak ini dimaksudkan untuk menjaga privasi individu dan memastikan bahwa data yang dikelola tetap akurat, sesuai kebutuhan, dan tidak berlebihan. Hal ini menunjukkan bahwa adanya hak tersebut memungkinkan setiap individu untuk tetap memiliki kendali atas informasi pribadinya, terutama di tengah perkembangan teknologi digital yang semakin kompleks dan terbuka. [12]

Pemberian edukasi dan penyuluhan kepada masyarakat mengenai pentingnya perlindungan data pribadi serta langkah - langkah untuk menjaga keamanannya merupakan hal yang sangat krusial. Upaya edukatif ini dapat dilakukan melalui berbagai media, seperti media massa, kegiatan seminar, maupun melalui integrasi materi perlindungan data pribadi dalam kurikulum pendidikan di sekolah. Penyuluhan yang terarah dan efektif dapat berperan besar dalam meningkatkan kesadaran publik dan mengurangi potensi penyalahgunaan data. Masyarakat yang memiliki pemahaman yang baik cenderung lebih berhati-hati dalam menggunakan layanan digital, memahami potensi risiko, serta mampu menjaga data pribadinya secara lebih aktif dan bertanggung jawab.

2) Perlindungan Represif

Perlindungan hukum secara represif dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi mencakup penerapan sanksi administratif, pidana, dan perdata terhadap pihak-pihak yang terbukti melanggar ketentuan dalam undang undang tersebut. [13] Sanksi administratif ditujukan kepada pengendali maupun prosesor data pribadi yang tidak mematuhi aturan, dengan bentuk sanksi yang bervariasi, seperti teguran tertulis, penghentian sementara aktivitas pemrosesan data, kewajiban untuk menghapus atau memusnahkan data pribadi, hingga denda administratif yang nilainya bisa mencapai dua persen dari total pendapatan atau penerimaan tahunan, tergantung pada jenis pelanggaran yang dilakukan. [14]

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi juga menetapkan ketentuan pidana terhadap perorangan maupun badan hukum yang melakukan pelanggaran terhadap isi undang-undang tersebut. Jenis sanksi pidana yang dapat dikenakan mencakup hukuman penjara, denda, serta pidana tambahan seperti penyitaan keuntungan atau aset yang diperoleh dari tindak pidana, dan kewajiban membayar ganti rugi kepada pihak yang dirugikan.[15] Dalam Pasal 67, dijelaskan bahwa setiap individu yang dengan sengaja mengakses, menyebarluaskan, atau menggunakan data pribadi milik orang lain secara melanggar hukum, dapat dijatuhi hukuman penjara hingga lima tahun atau dikenakan denda maksimal sebesar lima miliar rupiah.[16] Sementara itu, bagi pelaku yang membocorkan data pribadi milik orang lain tanpa hak, ancaman pidana yang dikenakan dapat berupa penjara paling lama empat tahun atau denda hingga empat miliar rupiah. Penerapan sanksi pidana secara tegas mampu memberikan efek jera yang signifikan bagi para pelanggar dan berkontribusi dalam memperkuat sistem perlindungan data pribadi di Indonesia.

Terkait penerapan sanksi pidana terhadap korporasi, Undang Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menetapkan bahwa hukuman yang dikenakan terbatas pada pidana denda. Nilai denda yang dapat dijatuhkan kepada korporasi bisa mencapai hingga sepuluh kali dari batas maksimum denda yang diatur dalam undang-undang tersebut. Selain pidana denda, korporasi juga dapat dikenakan sanksi tambahan, seperti penyitaan keuntungan atau aset yang diperoleh dari tindak pidana, pembekuan sebagian atau seluruh kegiatan usaha, pelarangan permanen terhadap aktivitas tertentu, penutupan tempat usaha secara sebagian atau menyeluruh, kewajiban untuk memenuhi tanggung jawab yang sebelumnya diabaikan, pembayaran kompensasi kepada pihak yang dirugikan, pencabutan izin operasional, hingga pembubaran perusahaan. [17]

2. **Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Pelanggaran Privasi Data Pribadi**

Pertanggungjawaban pidana berarti bahwa setiap individu yang melakukan kejahatan atau pelanggaran yang dijelaskan dalam hukum harus menanggung konsekuensi dari tindakan tersebut sesuai dengan kesalahannya. Dengan kata lain. individu yang terlibat dalam kriminalitas harus dihadapkan pada sanksi jika

terbukti bersalah. Seseorang dinyatakan bersalah jika saat melakukan tindakan, menurut pandangan masyarakat. mencerminkan pandangan norma tentang kesalahan yang diperbuat oleh individu tersebut. pada Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi. setiap individu yang dengan sengaja dan ilegal memperoleh atau mengumpulkan data pribadi milik orang lain dapat dikenakan hukuman penjara hingga lima tahun dan/atau denda maksimum sebesar Rp 5 miliar. Sementara itu, individu yang dengan sengaja dan tanpa izin mengungkapkan data pribadi yang bukan miliknya dapat menghadapi hukuman penjara hingga empat tahun dan/atau denda maksimal Rp 4 miliar.

Bagi individu yang dengan sengaja dan melanggar hukum menggunakan data pribadi milik orang lain, hukuman penjara yang diterapkan dapat mencapai lima tahun dan/atau denda maksimum Rp 5 miliar. Selain itu, sanksi juga berlaku bagi mereka yang dengan sengaja memalsukan data pribadi demi keuntungan pribadi atau orang lain yang dapat mendatangkan kerugian bagi pihak lain. 61 Pelanggar yang melakukan tindakan tersebut dapat dipenjara hingga enam tahun dan/atau denda paling tinggi Rp 6 miliar. Selain mendapat sanksi pidana ini, pelaku juga mungkin akan dikenakan hukuman tambahan yang berupa pengambilan keuntungan dan/atau aset yang diperoleh dari tindakan ilegal serta pembayaran kompensasi. Apabila tindakan ini dilakukan oleh suatu perusahaan, maka sanksi dapat dikenakan kepada manajer, pemegang kontrol, pihak yang memberi instruksi. pemilik manfaat, dan/atau perusahaan tersebut. Sanksi yang bisa diterima oleh perusahaan hanya berupa denda, yang jumlahnya tidak boleh lebih dari sepuluh kali lipat dari denda maksimum yang terancam.

Ada empat kesalahan yang bisa mendapat hukuman pidana menurut Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi:

1) Mengungkapkan informasi pribadi milik orang lain atau doxing. Tindakannya dapat berujung pada hukuman penjara dengan maksimal empat tahun dan denda hingga Rp4 miliar.
2) Mengumpulkan informasi pribadi dengan cara yang tidak sah. Pelanggar dapat dijatuhi hukuman penjara maksimum lima tahun dan denda maksimal Rp5 miliar.

3) Memanfaatkan informasi pribadi orang lain. Salah satu contoh tindakan ini adalah mendaftar kartu SIM dengan menggunakan 62 identitas orang lain. Pelakunya menghadapi ancaman penjara maksimal lima tahun dan denda hingga Rp5 miliar.
4) Membuat informasi pribadi yang tidak valid atau memalsukan data pribadi. Pelakunya akan dihukum penjara dengan maksimal enam tahun dan denda sebesar Rp6 miliar. [18]

Berdasarkan sanksi diatas bisa dilihat contoh kasus Bjorka yang merupakan seorang peretas yang telah menjadi sorotan publik sejak pertengahan 2022, dikenal karena serangkaian aksi peretasan dan kebocoran data pribadi yang melibatkan jutaan warga negara Indonesia, termasuk data dari berbagai instansi pemerintah dan lembaga strategis. Kasus ini tidak hanya menimbulkan keresahan publik yang luar biasa, tetapi juga mengekspos kerentanan sistem keamanan siber nasional yang mendesak untuk diperbaiki. Pengenaan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dengan ancaman pidana maksimal 12 tahun penjara dan denda hingga Rp12 miliar menunjukkan keseriusan negara dalam menangani kejahatan siber yang mengancam kedaulatan data dan privasi warga negara.

Tindak pidana pertama yang dilakukan Bjorka adalah akses ilegal ke sistem elektronik, yang merupakan inti dari seluruh rangkaian kejahatannya. Bjorka diduga melakukan penetrasi tidak sah ke berbagai basis data pemerintah dan swasta, termasuk sistem Direktorat Jenderal Imigrasi, Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan, dan berbagai instansi lainnya. Modus operandi yang digunakan kemungkinan melibatkan teknik hacking canggih seperti SQL injection, phishing, atau eksploitasi kerentanan keamanan (vulnerability exploitation) pada sistem yang ditargetkan. Tindakan tersebut telah secara tegas ditentukan dalam Pasal 46 ayat (1) UU ITE, yang menyatakan bahwa setiap orang yang dengan sengaja serta tanpa hak atau secara melanggar hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 30 ayat (1) yaitu melakukan akses terhadap komputer dan/atau sistem elektronik milik orang lain dengan metode apa pun dapat dijatuhi hukuman pidana. Kritik yang muncul adalah bahwa meskipun undang-undang ini telah ada, implementasi sistem keamanan siber di Indonesia masih sangat lemah, sehingga

memudahkan peretas seperti Bjorka untuk melancarkan aksinya tanpa hambatan berarti selama bertahun-tahun.

Setelah berhasil mengakses sistem elektronik, Bjorka kemudian melakukan pencurian data dalam skala masif yang mencakup informasi pribadi jutaan warga negara Indonesia. Data yang dicuri meliputi Nomor Induk Kependudukan (NIK), informasi paspor, data kesehatan dari BPJS, hingga data registrasi kartu SIM yang sangat sensitif. Perbuatan pencurian data ini dikategorikan sebagai tindak pidana berdasarkan Pasal 32 ayat (1) UU ITE melarang setiap orang untuk dengan sengaja dan tanpa hak atau secara melawan hukum melakukan tindakan apa pun yang berupa mengubah, menambah, mengurangi, mentransmisikan, merusak, menghapus, memindahkan, atau menyembunyikan informasi elektronik dan/atau dokumen elektronik milik pihak lain maupun milik publik. Pencurian data dalam konteks ini bukansekadar perbuatan kriminal biasa, melainkan adalah salah satu bentuk pelanggaran terhadap hak asasi manusia terkait hak atas privasi sebagaimana dijamin dalam UUD 1945 Pasal 28G ayat (1), sehingga dampaknya melampaui kerugian material dan menciptakan ancaman jangka panjang terhadap keamanan personal korban.

Tindakan Bjorka tidak berhenti pada pencurian data, tetapi berlanjut dengan penyebarluasan data pribadi tersebut melalui berbagai platform internet, termasuk forum-forum dark web dan media sosial. Bjorka secara terbuka membagikan sampel data curian sebagai bentuk "pembuktian" atas keberhasilannya meretas sistem-sistem Indonesia, bahkan menawarkan data tersebut untuk dijual kepada pihak-pihak yang berkepentingan. Perbuatan ini secara eksplisit melanggar Pasal 26 UU ITE tentang perlindungan data pribadi, yang kemudian diperkuat dengan ketentuan dalam UU PDP. Penyebarluasan data ini menimbulkan efek domino yang sangat berbahaya: korban menjadi rentan terhadap berbagai bentuk kejahatan lanjutan seperti pencurian identitas (identity theft), penipuan (fraud), pemerasan, hingga ancaman keamanan fisik. Dari perspektif kritis, kasus ini mengungkapkan kegagalan sistemik dalam penegakan hukum perlindungan data di Indonesia, di mana sanksi yang ada belum memberikan efek jera yang memadai, dan mekanisme perlindungan preventif masih sangat terbatas.

Aksi Bjorka juga menimbulkan gangguan signifikan terhadap operasional sistem elektronik berbagai instansi yang diretas, meskipun tidak ada laporan tentang kerusakan permanen pada sistem tersebut. Gangguan ini mencakup keharusan melakukan investigasi forensik digital, pemulihan sistem, peningkatan protokol keamanan darurat, dan upaya mitigasi dampak kebocoran data yang memerlukan sumber daya besar dan mengganggu pelayanan publik. Tindakan tersebut dapat digolongkan sebagai bentuk pelanggaran terhadap Pasal 33 UU ITE mengatur mengenai perbuatan yang dilakukan dengan sengaja dan tanpa hak atau secara melawan hukum yang menyebabkan terganggunya sistem elektronik dan/atau membuat sistem tersebut tidak berfungsi sebagaimana mestinya. Kritik yang perlu diajukan adalah bahwa pemerintah dan lembaga-lembaga yang menjadi korban seharusnya juga memikul tanggung jawab atas kelalaian dalam mengamankan data publik yang dipercayakan kepada mereka, sehingga penanganan kasus ini tidak boleh hanya fokus pada penghukuman pelaku tetapi juga pada reformasi tata kelola keamanan siber nasional.

Kasus Bjorka merepresentasikan kompleksitas kejahatan siber modern yang melibatkan multiple layers of criminality, mulai dari akses ilegal, pencurian data, penyebarluasan informasi pribadi, pemerasan, hingga gangguan terhadap kepentingan umum. Pengenaan UU ITE dengan ancaman pidana maksimal 12 tahun penjara dan denda Rp12 miliar menunjukkan bahwa hukum Indonesia telah mengantisipasi keseriusan kejahatan siber, namun efektivitas penegakan hukum ini sangat bergantung pada kemampuan aparat dalam melakukan investigasi digitaldan menghadirkan bukti-bukti forensik yang kuat di pengadilan. Secara kritis, kasus ini seharusnya menjadi momentum bagi Indonesia untuk melakukan reformasi menyeluruh dalam sistem keamanan siber nasional, termasuk peningkatan investasi pada infrastruktur keamanan, capacity building bagi aparat penegak hukum, harmonisasi regulasi perlindungan data, dan pembangunan kesadaran literasi digital masyarakat. Tanpa langkah-langkah komprehensif menjadi tersebut, penangkapan Bjorka hanya akan kemenangan simbolis tanpa dampak preventif terhadap ancaman kejahatan siber di masa depan. 68

Penanganan kasus Bjorka menghadirkan kompleksitas yuridis yang unik karena melibatkan penerapan dua instrumen hukum utama secara bersamaan, yaitu

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). UU ITE lebih menekankan pada aspek teknis kejahatan siber seperti akses ilegal, interferensi sistem, dan penyalahgunaan teknologi informasi, sementara UU PDP secara spesifik mengatur tentang perlindungan hak privasi individu atas data pribadinya. Dalam konteks kasus Bjorka, penerapan kedua undang-undang ini secara kumulatif memberikan landasan hukum yang komprehensif untuk menjerat pelaku dengan berbagai pasal yang relevan, mulai dari tindakan peretasan sistem hingga pencurian dan penyebarluasan data pribadi jutaan warga negara. Namun, penerapan kerangka hukum ganda ini juga menimbulkan pertanyaan kritis mengenai potensi tumpang tindih pengaturan dan bagaimana aparat penegak hukum harus mengonstruksi dakwaan yang tepat untuk menghindari gugurnya dakwaan karena obscuur libel atau dakwaan yang tidak jelas.

Undang-Undang Nomor 1 Tahun 2024 sebagai perubahan terbaru dari UU ITE memberikan instrumen hukum yang kuat untuk menjerat Bjorka atas tindakan peretasan dan akses ilegal yang dilakukannya. Pasal 30 ayat (1) jo. Pasal 46 ayat (1) UU ITE secara tegas melarang akses ke komputer dan/atau sistem elektronik milik orang lain tanpa hak, dengan ancaman pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp600 juta. Dalam kasus Bjorka yang melibatkan penetrasi ke multiple systems seperti basis data Direktorat Jenderal Imigrasi, BPJS Kesehatan, dan sistem registrasi SIM, penerapan pasal ini dapat dilakukan secara berlapis karena setiap akses ilegal ke sistem yang berbeda merupakan tindak pidana tersendiri. Pasal 32 ayat (1) jo. Pasal 48 ayat (1) UU ITE yang mengatur tentang pemindahan atau pentransferan informasi elektronik dengan ancaman pidana penjara paling lama 8 tahun dan/atau denda paling banyak Rp2 miliar, juga sangat relevan mengingat Bjorka tidak hanya mengakses tetapi juga mengekstraksi data dalam jumlah masif. Kritik yang perlu dikedepankan adalah ancaman pidana yang ada masih belumsebanding dengan dampak masif yang ditimbulkan, sehingga perlu ada diskursus mengenai pemberatan hukuman khususnya untuk kejahatan siber yang berdampak pada keamanan nasional.

Penerapan UU ITE dan UU PDP dalam kasus Sanksi terhadap Bjorka tidak hanya mencakup hukuman pokok berupa pidana penjara dan denda, tetapi juga membuka peluang penjatuhan pidana tambahan yang memberikan efek jera lebih besar dan keadilan restoratif bagi korban. Pasal 69 Undang-Undang Perlindungan Data Pribadi menetapkan adanya pidana tambahan berupa: penyitaan keuntungan dan/atau kekayaan yang diperoleh dari tindak pidana; penyitaan aset yang digunakan untuk melakukan tindak pidana; serta kewajiban membayar ganti rugi kepada korban. UU ITE juga memuat ketentuan mengenai pidana tambahan berupa pengumuman putusan pengadilan sebagaimana tercantum dalam Pasal 52, yang bertujuan memberikan efek pencegahan umum (general deterrence). Hakim juga dapat memerintahkan pemusnahan data curian yang masih dikuasai terpidana atau pihak ketiga, serta pemblokiran akses terhadap konten atau platform yang digunakan untuk menyebarkan data curian. Kritik yang muncul adalah implementasi pidana tambahan di lapangan masih menghadapi kendala, terutama mekanisme eksekusi ganti kerugian kepada korban yang jumlahnya masif dan tersebar, serta kompleksitas melacak dan merampas aset hasil kejahatan yang telah dikonversi ke berbagai bentuk termasuk cryptocurrency. [19]

Menurut penulis, Masih terdapat berbagai kelemahan mendasar dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana diubah dengan Undang-Undang Nomor 1 Tahun 2024, sehingga penegakan hukum terhadap pelanggaran privasi data pribadi di era digital belum berjalan secara efektif. Permasalahan tersebut tidak hanya disebabkan oleh ketidaksesuaian antar ketentuan, norma hukum yang belum dirumuskan secara jelas, serta lambatnya pembentukan lembaga pendukung, tetapi juga karena kedua undang-undang tersebut belum sepenuhnya mampu menghadapi kejahatan siber lintas negara, sebagaimana terlihat dalam kasus kebocoran data yang dikenal sebagai kasus Bjorka.

Sebagai contoh, Pasal 67 UU PDP mengatur ancaman pidana penjara paling lama lima tahun atau denda paling banyak Rp5 miliar bagi setiap orang yang mengakses data pribadi secara tidak sah. Meskipun ketentuan ini tampak tegas, penggunaan frasa “melawan hukum” masih membuka peluang arti yang berbeda-beda. Selain itu,

ketentuan tersebut belum mengatur perbedaan sanksi berdasarkan tingkat kerugian yang ditimbulkan. Dalam kasus kebocoran data dalam skala besar, seperti kebocoran jutaan Nomor Induk Kependudukan dan data peserta BPJS, ancaman pidana yang diterapkan sama dengan pelanggaran yang berdampak kecil. Akibatnya, sanksi yang dijatuhkan sering kali tidak sebanding dengan kerugian yang dialami korban, yang jumlahnya banyak dan sulit memperoleh ganti kerugian. Oleh karena itu, diperlukan perbaikan pengaturan pidana yang lebih berorientasi pada kepentingan korban, antara lain melalui pengaturan yang lebih tegas mengenai gugatan kelompok serta penguatan sanksi tambahan berupa kewajiban pembayaran ganti rugi secara bersama-sama.

Selain itu, terdapat tumpang tindih pengaturan antara UU PDP dan UU ITE. Misalnya, Pasal 30 jo. Pasal 46 UU ITE mengatur tindak pidana akses ilegal terhadap sistem elektronik dengan ancaman pidana penjara antara enam hingga dua belas tahun, sedangkan Pasal 65 UU PDP mengatur pengumpulan data pribadi secara ilegal. Tumpang tindih ini berpotensi menimbulkan dakwaan ganda atau dakwaan yang tidak jelas, sehingga berisiko melanggar asas ne bis in idem (larangan menghukum seseorang dua kali atas perbuatan yang sama). Kondisi tersebut terlihat dalam kasus Bjorka, di mana aparat penegak hukum mengalami kesulitan menentukan undang-undang yang paling tepat untuk diterapkan. Oleh sebab itu, diperlukan penyesuaian pengaturan melalui ketentuan penghubung yang menegaskan bahwa UU PDP digunakan sebagai dasar utama untuk pelanggaran yang secara langsung menyangkut data pribadi, sedangkan UU ITE diterapkan untuk perbuatan yang berkaitan dengan gangguan teknis terhadap sistem elektronik. Selain itu, perlu dipertimbangkan pengaturan mengenai kejahatan siber gabungan dengan ancaman pidana yang lebih berat untuk kasus pelanggaran yang bersifat kompleks dan berlapis.

Permasalahan paling serius terletak pada keterlambatan pembentukan Dewan Perlindungan Data Pribadi (DPDP) sebagaimana diatur dalam pasal 49 UU PDP Hingga awal tahun 2026, lembaga ini belum terbentuk secara efektif akibat kendala politik dan anggaran. Akibatnya, tidak terdapat lembaga independen yang berwenang melakukan pengawasan preventif, seperti pemeriksaan kepatuhan Penyelenggara Sistem Elektronik serta penjatuhan sanksi administratif. Tanpa

kehadiran DPDP, fungsi pengawasan masih dibebankan kepada kementerian atau aparat penegak hukum yang tidak memiliki spesialisasi di bidang perlindungan data pribadi. Oleh karena itu, diperlukan percepatan pembentukan peraturan pelaksana yang memperkuat kedudukan DPDP sebagai lembaga independen dengan kewenangan penyelidikan dan pendanaan yang memadai.

UU PDP dan UU ITE juga dinilai belum mampu mengikuti perkembangan teknologi terbaru, seperti penggunaan kecerdasan buatan dalam peretasan, penyalahgunaan data melalui teknologi deepfake, serta pemanfaatan blockchain untuk menyamarkan identitas pelaku. Definisi data pribadi dalam Pasal 1 UU PDP masih bersifat umum dan belum membedakan antara data pribadi biasa dan data pribadi sensitif, seperti data biometrik dan pola perilaku digital, yang seharusnya mendapatkan perlindungan lebih ketat. Sementara itu, Pasal 32 UU ITE masih terbatas pada pengaturan pemindahan atau perubahan data, tanpa menyesuaikan bentuk serangan siber modern seperti eksploitasi celah keamanan dan serangan ransomware. Oleh karena itu, diperlukan perubahan untuk memperluas definisi data pribadi, mewajibkan standar keamanan sistem yang lebih ketat, serta mewajibkan pelaporan kebocoran data dalam jangka waktu tertentu. Selain itu, kerja sama internasional perlu diperkuat melalui partisipasi aktif dalam konvensi internasional tentang kejahatan siber.

Pengaturan sanksi terhadap korporasi dalam Pasal 68 UU PDP masih belum sebanding dengan potensi kerugian negara dan masyarakat akibat kebocoran data berskala besar. Denda maksimal yang diatur belum memberikan efek jera yang memadai, terutama bagi korporasi besar. Selain itu, belum terdapat pengaturan mengenai pertanggungjawaban pidana korporasi dalam kasus pelanggaran data yang menimbulkan dampak serius terhadap keselamatan atau kehidupan manusia. Oleh karena itu, diperlukan revisi regulasi dengan pendekatan berbasis risiko, yang mengatur tingkat sanksi berdasarkan berat ringannya pelanggaran, sekaligus mendorong kepatuhan melalui insentif bagi penyelenggara sistem elektronik yang telah memenuhi standar keamanan tinggi. Dengan demikian, sistem perlindungan data pribadi di Indonesia dapat bertransformasi dari pendekatan yang bersifat reaktif menjadi sistem yang lebih preventif dan adaptif terhadap ancaman kejahatan siber di era digital.

KESIMPULAN

Pengaturan tindak pidana pelanggaran privasi data pribadi di indonesia diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan Undang Undang Informasi dan Transaksi Elektronik (UU ITE). UU PDP mengatur bentuk pelanggaran serta sanksinya, dan UU ITE mengatur tentang pengamanan data di sistem elektronik, penggunaan tanpa izin, akses tanpa hak, dan penyadapan. Kedua peraturan tersebut menjadi dasar hukum untuk memberikan perlindungan dan penegakan hukum terhadap pelanggaran data pribadi di Indonesia.

Pertanggungjawaban pidana atas pelanggaran data pribadi dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan Undang-Undang Informasi dan Transaksi Elektronik menegaskan bahwa setiap orang yang secara sengaja dan melawan hukum memperoleh, menggunakan, mengungkapkan, atau memalsukan data pribadi orang lain dapat dikenai sanksi pidana berupa penjara dan/atau denda sebagai bentuk penegakan hukum dan perlindungan hak privasi.

REFERENSI

[1] Suari, Kadek Rima Anggen, and I. Made Sarjana. "Menjaga privasi di era digital: Perlindungan data pribadi di Indonesia." Jurnal Analisis Hukum 6.1, hlm. 133-134, 2023.

[2] Mamonto, Dewi Fortuna. "Analisis Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022." LEX PRIVATUM 13.4, Hlm.1, 2024.

[3] Muhammad Rifqi Adil Nur, Muhammad Fachri Said, Mursyid, Analisis Hukum tentang Tanggung Jawab Pidana Pelaku Pornografi Balas Dendam dalam Perlindungan Data Pribadi Korban, Horizon Public Legal Studies. Vol. 1, No. 2, Hlm 133-134 2025.

[4] Dade, L. L., Waha, C. J., & Nachrawy, N., Kajian yuridis tentang tindak pidana penyebaran data pribadi melalui internet (doxing) di Indonesia. Lex Privatum, 13(3), 2024.

[5] Alexander Kennedy, Perlindungan Data Pribadi Dalam Dunia Siber Di Indonesia Ditinjau Berdasarkan Hukum Tata Negara. Hukum Dinamika Ekselensia, 6(2): 82–98, 2024.

[6] Salsabila, S., & Wiraguna, S. A., Pertanggungjawaban hukum atas pelanggaran data pribadi dalam perspektif Undang-Undang Pelindungan Data Pribadi Indonesia. Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi, 2(2), 145-157, 2025.

[7] Erlina Maria Christin Sinaga dan Mery Christian Putri, Formulasi Perlindungan Data Pribadi dalam Revolusi Industri, Jurnal Hukum Media Pembinaan Hukum Nasional, Volume 9 No. 9, agustus 2020.

[8] Fauzy, E., & Shandy, N. A. R., Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. Lex Renaissance, 7(3) 52, 2022.

[9] Pelindungan Privacy dan Personal Data, Diakses dari https://www.dpr.go.id/dokakd/dokumen/K1-RJ-20210422 090703-5599.pdf pada 3 Desember 2025

[10] Judhari Sawan, Pengantar Hukum Telekomunikasi, PT. Raja Grafindo Persada: Jakarta, 2009.

[11] Islamy, Imam Teguh, et al. "Pentingnya memahami penerapan privasi di era teknologi informasi." Jurnal Pendidikan 11 (2), 2018.

[12] Alfitri, N. A., Rahmawati, R., & Firmansyah, F., Perlindungan Terhadap Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022. Journal Social Society, 4(2), 92-111, 2024.

[13] Disemadi, H. S., Sudirman, L., Girsang, J., & Aninda, A. M., Perlindungan Data Pribadi di Era Digital: Mengapa Kita Perlu Peduli?. Sang Sewagati Journal, 1(2), 66-90, 2023.

[14] Kusuma, S. C. B., Tinjauan Normatif Konsep Perlindungan Hukum Hak Privat Warga Negara Dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, 2023.

[15] Suryanto, D., & Riyanto, S., Implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data pribadi dalam Industri Ritel Tinjauan terhadap Kepatuhan dan Dampaknya pada Konsumen. Veritas, 10(1), 2024.

[16] Sianturi, C. G. P., Nababan, R., & Siregar, R. J., Peran Hukum Dalam Melindungi Data Pribadi. Innovative: Journal Of Social Science Research, 4(5), 2024.

[17] Satria, M., & Handoyo, S., Perlindungan Hukum Terhadap Data Pribadi Pengguna Layanan Pinjaman Online Dalam Aplikasi Kreditpedia. Journal de Facto, 8(2), 2022.

[18] Soesanto, E., Romadhon, A., Mardika, B. D., & Setiawan, M. F., Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File. Sammajiva: Jurnal Penelitian Bisnis dan Manajemen, 1(2) 2023.

[19] Inggria, D., Bella, W. G. O., & Hosnah, A. U., Penegakan hukum terhadap tindak pidana cybercrime dalam kasus peretasan dan pelanggaran data pribadi oleh hacker Bjorka. Jurnal Review Pendidikan dan Pengajaran, 8(4), 8284–8292, 2025.