

Tanggung Jawab Negara Terhadap Hak Perlindungan Data Pribadi di Era Digitalisasi

Anisa Asmir¹, Sodikin²

^{1,2} Universitas Muhammadiyah Jakarta, Indonesia

E-mail: ichaasmir@gmail.com¹, sodikin.fh@umj.ac.id²

Article History:

Received: 01 Juni 2026

Revised: 15 Juli 2026

Accepted: 29 Juli 2026

Keywords *Tanggung Jawab Negara, Data Pribadi, Hak Asasi Manusia, Perlindungan.*

Abstrak: *Data pribadi mencakup informasi penting yang berkaitan dengan seseorang, sehingga keamanan data pribadi merupakan hak asasi manusia yang harus dijamin dan dihormati. Dengan meningkatnya kasus pelanggaran privasi dan penyalahgunaan data pribadi, penting bagi negara untuk memiliki peraturan perundang-undangan yang efektif untuk melindungi hak privasi warganya. Permasalahannya tentang bagaimana tanggung jawab negara dalam melindungi hak perlindungan data pribadi sesuai dengan putusan Mahkamah Konstitusi Nomor 151/PUU-XXII/2024. Metode penelitian yang digunakan adalah metode deskriptif normatif adalah pendekatan penelitian yang bertujuan untuk menggambarkan secara sistematis suatu fenomena atau keadaan saat ini. Hasil penelitian menjelaskan bahwa konstitusi dan peraturan perundang-undangan menjadi landasan hukum bagi negara dalam melindungi warga negara. Semua orang berhak untuk melindungi dirinya sendiri, keluarganya, kehormatannya, martabatnya, dan atau harta benda yang dikuasainya. Kesimpulannya yang diperoleh adalah terjadinya pergeseran paradigma hukum dari komoditas menjadi hak asasi manusia, maksudnya negara menegaskan bahwa di era digital, data pribadi bukan lagi sekadar komoditas ekonomi atau aset bisnis, melainkan eksistensi dari privasi dan martabat manusia. Negara bertanggung jawab mengintervensi pasar digital guna memastikan tidak ada eksploitasi data sepihak oleh korporasi maupun instansi publik.*

PENDAHULUAN

Era digitalisasi sekarang ini sudah tidak dapat dipungkiri lagi karena perkembangan teknologi informasi serta komunikasi telah membawa dampak perubahan besar di dalam kehidupan sehari-hari.¹ Data pribadi menjadi semakin penting karena sekarang banyak

¹ Cecep Abdul Cholik, "Perkembangan Teknologi Informasi Komunikasi/ICT Dalam Berbagai Bidang," *Jurnal Fakultas Teknik UNISA Kuningan* 2, no. 2 (2021): 39–46,

aktivitas yang dapat dilakukan secara *online*. Data pribadi mencakup informasi penting seperti nama, alamat, nomor identitas, informasi finansial, dan informasi sensitif lainnya yang berkaitan dengan seseorang atau individual. Oleh karena itu, hak perlindungan data pribadi merupakan hak konstitusional warga negara untuk mengendalikan, melindungi, dan memutuskan bagaimana informasi pribadi mereka diproses, disimpan, dan digunakan oleh pihak lain. Hal ini bertujuan menjamin keamanan diri, privasi, dan mencegah penyalahgunaan data.²

Di tengah era digitalisasi 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 mengadopsi 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 negara untuk memiliki peraturan perundang-undangan yang efektif untuk melindungi hak privasi warganya.³

Di Indonesia, dibutuhkan kesadaran akan pentingnya perlindungan data pribadi, yang sekarang semakin meningkat, terutama dalam pertumbuhan dan penggunaan internet dan aplikasi berbasis teknologi saat ini. Hak untuk membela diri merupakan salah satu hak hukum yang digariskan dalam UUD 1945. Menurut Pasal 28G Ayat (1) UUD 1945, warga negara berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta miliknya.⁴ Dengan demikian, 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. Hal ini karena berurusan dengan informasi pribadi atau identitas seseorang, hak privasi lebih sensitif dan dapat dilihat sebagai hak pribadi. Contoh kebocoran data pribadi baru-baru ini telah menjadi masalah di antaranya: (a) kasus Tokopedia, pada awal 2020, platform e-commerce besar di Indonesia, Tokopedia, dilaporkan mengalami pelanggaran keamanan yang mengakibatkan informasi pribadi dari jutaan pengguna bocor.⁵ Data yang dikompromikan meliputi nama, alamat, nomor telepon, alamat email, dan kata sandi terenkripsi; (b) kasus Bukalapak pada tahun 2021 bahwa, platform e-commerce lainnya di Indonesia, juga dilaporkan mengalami pelanggaran data pada tahun 2021. Lebih dari 13 juta akun pengguna dilaporkan terdampak, dengan data seperti nama pengguna, alamat email, nomor telepon, dan kata sandi bocor⁶; (c) kasus Pembukaan Rekening nasabah menggunakan KTP Palsu di Indonesia, dilaporkan mengalami kerugian bagi pemilik KTP asli

<https://www.neliti.com/publications/455512/perkembangan-teknologi-informasi->

² Upik Mutiara and Romi Maulana, "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi," *Indonesian Journal of Law and Policy Studies* 1, no. 1 (2020), <https://www.academia.edu/download/96517028/1629.pdf>.

³ Ridho Pakina and Mohammad Solekhan, "Pengaruh Teknologi Informasi Terhadap Hukum Privasi Dan Pengawasan di Indonesia: Keseimbangan Antara Keamanan Dan Hak Asasi Manusia," *Journal of Sciencetech Research and Development* 6, no. 1 (2024): 273–86, <https://www.idm.or.id/JSCR/index.php/JSCR/article/view/376>.

⁴ Rosihan Luthfi, "Perlindungan Data Pribadi Sebagai Perwujudan Perlindungan Hak Asasi Manusia," *Jurnal Sosial Teknologi* 2, no. 5 (2022): 431–36, <http://sostech.greenvest.co.id/index.php/sostech/article/view/336>.

⁵ Muhammad Fathur, "Tanggung Jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen," *National Conference on Law Studies (NCOLS)* 2, no. 1 (2020): 43–60, <https://conference.upnvj.ac.id/index.php/ncols/article/view/1345>.

⁶ Desy Komalawati, Maria Dewi MR, and Raiseta Dwi Kartika, "Kejutan Puluhan Miliar Tokopedia Ditengah Kasus Kebocoran Data," . 2, no. 1 (2021): 49–56, <https://jurnalsyntaxadmiration.com/index.php/jurnal/article/download/167/249>.

yang berdampak menjadi risiko operasional maupun risiko reputasi.⁷

Kebocoran data pribadi adalah masalah serius yang dapat menyebabkan kerugian finansial, identitas palsu, dan bahkan penyalahgunaan data yang lebih lanjut. Pemerintah, perusahaan, dan individu perlu meningkatkan kesadaran tentang keamanan data dan mengambil langkah-langkah pencegahan yang tepat untuk melindungi data pribadi. Penting untuk terus mengikuti berita terkini untuk memahami perkembangan terbaru tentang masalah keamanan data di Indonesia atau di negara manapun.

Pada era digitalisasi saat ini, hampir seluruh perangkat terhubung dan memiliki koneksi internet, semuanya dapat dikelola dari mana saja. Ketika orang menggunakan teknologi digital dalam kehidupan sehari-hari untuk meningkatkan efisiensi kerja, menciptakan hubungan sosial ekonomi, dan memfasilitasi aktivitas lain, konsekuensi dari periode ini sangat besar. Teknologi berbasis komputer untuk informasi dan komunikasi telah berkembang pesat di masyarakat. Kemajuan teknologi ini kemudian membantu masyarakat. Hal ini, meskipun sudah ada undang-undang, yaitu Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). UU Perlindungan Data Pribadi yang dimiliki Indonesia saat ini perlu dikaji lebih detail karena regulasinya masih perlu penyempurnaan. Setidaknya Indonesia bisa disandingkan dengan undang-undang perlindungan data pribadi negara lain, seperti di Hong Kong, Malaysia, Singapura, dan Korea Selatan. Perlindungan hukum atas data pribadi sudah dijamin oleh undang-undang khusus di beberapa negara tersebut, namun dalam penelitian ini, kami akan membandingkan undang-undang perlindungan data pribadi Malaysia dengan UU PDT Indonesia. Undang-Undang Perlindungan Data Pribadi memiliki tujuan dan manfaat yang penting dalam konteks perlindungan privasi dan penggunaan data pribadi di Indonesia, dan bertujuan untuk menciptakan lingkungan digital yang lebih aman, terpercaya, dan menghormati privasi individu, sambil tetap memungkinkan pertumbuhan ekonomi dan inovasi di era digitalisasi.

Dengan adanya variasi sistem hukum tersebut, maka asas universalitas dapat digunakan, khususnya untuk 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 di atas, maka peneliti tertarik untuk mengkaji mengenai konsep hak asasi manusia yang berkaitan dengan perlindungan data pribadi sebagaimana dijelaskan oleh Mahkamah Konstitusi dengan putusannya Nomor 151/PUU-XXII/2024 mengenai pengujian konstitusionalitas Pasal 53 ayat (1) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) terhadap Undang-Undang Dasar Negara Republik Indonesia (UUD NRI) Tahun 1945. Putusan tersebut yang lebih menekankan pada tanggung jawab dalam melindungi data pribadi setiap warga negara melalui konsep “perlindungan” (to protect). Dengan demikian, Mahkamah Konstitusi (MK) telah menegaskan bahwa data pribadi sebagai hak bagi setiap warga negara wajib untuk dilindungi secara maksimal sehingga tidak dapat dijadikan sebagai objek yang merugikan yang bertentangan dengan asas perlindungan, kehati-hatian, dan kerahasiaan demi menjaga eksklusivitas kerahasiaan data pribadi.⁸

Maksud dan tujuan dalam penulisan ini adalah dengan menjawab permasalahan tentang bagaimana tanggung jawab negara dalam melindungi hak perlindungan data pribadi sesuai dengan putusan Mahkamah Konstitusi Nomor 151/PUU-XXII/2024.

⁷ Jihan Armita, “Pembobolan Saldo Rekening Nasabah Bank Dengan Cara Pemalsuan Identitas” (PhD Thesis, Universitas Hasanuddin, 2021), <https://repository.unhas.ac.id/id/eprint/16087/>.

⁸ Ismet Hadi, “Rekonstruksi Yurisprudensi Mahkamah Konstitusi di Era Pengawasan Data,” *Jurnal Hukum Egalitaire* 3, no. 1 (2025): 83–103, <https://journal.umgo.ac.id/index.php/jhe/article/view/5484>.

METODE PENELITIAN

Metode penelitian yang digunakan adalah metode deskriptif normatif adalah pendekatan penelitian yang bertujuan untuk menggambarkan secara sistematis suatu fenomena atau keadaan saat ini, kemudian menganalisisnya berdasarkan norma, aturan, hukum, atau standar nilai yang berlaku. Karakteristik metode deskriptif normatif adalah tidak hanya berhenti pada apa yang terjadi di lapangan (fakta), tetapi juga menilai fakta tersebut berdasarkan kriteria "apa yang seharusnya" menurut aturan tertulis. Data yang digunakan sebagai jenis bahan hukum utama adalah: (a) bahan hukum primer yaitu peraturan perundang-undangan seperti Undang-Undang Dasar, dan putusan hakim; (b) bahan hukum sekunder seperti buku teks, jurnal ilmiah, hasil penelitian terdahulu, opini hukum pakar, dan laporan kasus; dan (c) bahan hukum tersier yaitu kamus hukum, ensiklopedia, atau bibliografi yang membantu menjelaskan bahan primer dan sekunder. Teknik analisis yang digunakan adalah analisis kualitatif yaitu metode yang menguraikan dan menginterpretasikan data non-angka untuk menemukan tema dan makna mendalam dari suatu fenomena. Secara sederhana, teknik ini menjawab pertanyaan "mengapa" dan "bagaimana", dan prosesnya berfokus pada kedalaman informasi.

HASIL DAN PEMBAHASAN

1. Prinsip Hak Privasi Terhadap Data Pribadi

Prinsip hak privasi terhadap data pribadi merupakan aspek kritis dalam era digital yang semakin maju ini. Setiap harinya, kita berinteraksi dengan teknologi dan memberikan data pribadi secara online. Data pribadi merujuk pada informasi apa pun yang dapat mengidentifikasi secara langsung atau tidak langsung seseorang. Teknologi saat ini memungkinkan pengumpulan dan pemanfaatan data pribadi kita secara masif dan otomatis melalui berbagai platform digital. Data ini sering kali dibagikan secara sukarela saat mendaftar aplikasi, berbelanja online, atau menggunakan media sosial. Ini termasuk, namun tidak terbatas pada, nama, alamat, nomor telepon, alamat email, tanggal lahir, nomor identifikasi, data keuangan, dan informasi medis. Namun dengan memberikan informasi ini, kita juga membuka peluang bagi potensi penyalahgunaan data dan pelanggaran privasi.⁹ Hak privasi terhadap data pribadi mencakup hak setiap individu untuk mengetahui apa yang terjadi dengan data pribadi mereka, siapa yang mengaksesnya, untuk tujuan apa data tersebut digunakan, dan bagaimana data tersebut diolah dan disimpan. Lebih dari itu, prinsip ini juga melibatkan hak untuk memberikan izin atau persetujuan atas penggunaan data pribadi tersebut, serta hak untuk meminta penghapusan data (*right to be forgotten*) atau koreksi jika data tersebut tidak akurat.

Prinsip hak privasi terhadap data pribadi bertujuan untuk melindungi hak asasi manusia dan martabat individu, serta untuk memastikan bahwa data pribadi digunakan dengan etika dan kejujuran. Hal ini tidak hanya relevan bagi perusahaan yang mengumpulkan data, tetapi juga bagi pemerintah dan entitas lain yang terlibat dalam pengumpulan, pemrosesan, dan penggunaan data pribadi. Beberapa contoh kasus hak privasi yang dilanggar atau dianggap dilanggar yang pernah ada di Indonesia adalah bocornya data pribadi pada layanan BPJS kesehatan pada tahun 2021,¹⁰ pada tahun 2020, terjadi pelanggaran data di platform e-

⁹ Ni Putu Noni Suharyanti and Ni Komang Sutrisni, "Urgensi Perlindungan Data Pribadi Dalam Menjamin Hak Privasi Masyarakat," *Prosiding Seminar Nasional Fakultas Hukum Universitas Mahasaraswati Denpasar 2020* 1, no. 1 (2021): 119–34, <https://e-journal.unmas.ac.id/index.php/psnf/article/view/2395>.

¹⁰ Marshanda Vennesa Panggabean and Annisa Fitria, "Perlindungan Hukum Data Pribadi Di Indonesia (Kasus Kebocoran Badan Penyelenggara Jaminan Sosial Kesehatan)," *Arus Jurnal Sosial Dan Humaniora* 5, no. 2

commerce Tokopedia.¹¹ Data pribadi dari puluhan juta pengguna, termasuk nama, alamat email, nomor telepon, dan informasi lainnya, dan yang hingga saat ini belum jelas kebenarannya adalah data pribadi pengguna aplikasi transportasi online seperti Gojek atau Grab telah bocor akibat pelanggaran keamanan.¹²

Hak atas privasi, terkadang dikenal sebagai hak untuk tidak diganggu, diciptakan oleh Warren dan Brandeis dan diterbitkan dalam sebuah manuskrip berjudul *The Right to Privacy* di jurnal ilmiah Harvard University Law School.¹³ Menurut Warren dan Brandeis dalam jurnal tersebut, tumbuh dan berkembangnya teknologi telah menimbulkan kesadaran masyarakat yang menimbulkan kesadaran bahwa setiap orang berhak untuk menikmati hidup. Privasi adalah hak untuk menikmati hidup dan hak untuk dibiarkan sendiri, dan perkembangan hukum ini tidak dapat dihindari dan menuntut pengakuan hukum," kata Warren dan Brandeis. Setiap orang memiliki hak untuk menikmati privasinya, yang mengharuskannya untuk dijaga. Menurut Warren dan Brandeis, seiring dengan perkembangan dan kemajuan teknologi, kesadaran masyarakat pun tumbuh sehingga menimbulkan kesadaran bahwa setiap orang berhak untuk menikmati hidup. Privasi adalah hak untuk menikmati hidup dan hak untuk dibiarkan sendiri, dan perkembangan hukum ini tidak dapat dihindari dan menuntut pengakuan hukum," kata Warren dan Brandeis. Setiap orang berhak untuk menikmati privasinya, yang mengharuskannya untuk dijaga.¹⁴

Pertama dan terpenting, menjaga hubungan dengan orang lain mengharuskan seseorang untuk menyembunyikan beberapa aspek kehidupan pribadinya untuk menjaga posisinya pada tingkat tertentu. Kedua, privasi merupakan hak yang berdiri sendiri dan tidak bergantung pada hak lainnya, namun hak ini akan hilang jika orang tersebut mengungkapkan barang-barang yang bersifat privat kepada publik. Ketiga, seseorang dalam hidupnya membutuhkan waktu untuk menyendiri, sehingga privasi dibutuhkan oleh seseorang. Keempat, hak atas privasi mencakup kemampuan seseorang untuk memelihara hubungan rumah tangga, seperti bagaimana mereka mendukung pernikahan dan memelihara keluarga mereka. Warren selanjutnya menggambarkan ini sebagai hak melawan kata. Kelima, ketidakmampuan untuk menghitung kerugian adalah alasan lain mengapa privasi membutuhkan perlindungan hukum. Karena telah mengganggu kehidupan pribadinya, kerugian yang dirasakannya jauh lebih besar dari kerugian yang sebenarnya, dan akibatnya korban harus mendapatkan ganti rugi jika terjadi kerugian.¹⁵

Konstitusi dan peraturan perundang-undangan menjadi sebuah landasan hukum Indonesia. Semua orang berhak untuk melindungi dirinya sendiri, keluarganya, kehormatannya, martabatnya, dan atau harta benda yang dikuasainya, menurut UUD 1945, serta berhak juga atas rasa aman dan tenteram dari bahaya dan ketakutan. Pasal 28 Huruf G

(2025): 1958–65, <http://www.jurnal.ardenjaya.com/index.php/ajsh/article/view/1487>.

¹¹ Upik Sri Sulistyawati, "Membangun Keunggulan Kompetitif Melalui Platform E-Commerce: Studi Kasus Tokopedia," *Jurnal Manajemen Dan Teknologi* 1, no. 1 (2024): 43–56, <http://journal.stmiki.ac.id/index.php/jmt/article/view/776>.

¹² Yulisa Laili Zahro, "Pengetahuan Hukum Masyarakat Tentang Penyelesaian Masalah Pelanggaran Atas Layanan Ojek Online Berbasis Aplikasi (Studi Pada Go-Jek Dan Grab di Wilayah Kabupaten Cilacap)" (PhD Thesis, Universitas Islam Indonesia, 2019), <https://dspace.uui.ac.id/handle/123456789/19795>.

¹³ Ben Bratman, "Brandeis and Warren's The Right to Privacy and the Birth of the Right to Privacy," *Tenn. L. Rev.* 69 (2001): 623, https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/tenn69§ion=27.

¹⁴ Erwin Chemerinsky, "Rediscovering Brandeis's Right to Privacy," *Brandeis LJ* 45 (2006): 643, https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/branlaj45§ion=28.

¹⁵ Chemerinsky, "Rediscovering Brandeis's Right to Privacy."

Ayat (1) UUDNRI Tahun 1945 khususnya mengatur bahwa “Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan dilindungi dari ancaman ketakutan akan kejahatan.”¹⁶ Gagasan perlindungan data melindungi kebebasan orang untuk memilih apakah akan mengungkapkan atau menukar data pribadi mereka atau tidak. Selain itu, orang berhak memilih persyaratan untuk transfer data pribadi tersebut. Untuk membuat hak untuk melindungi data pribadi, hak privasi telah berkembang.

Setiap individu dapat memilih untuk melakukan privasi terhadap data yang dimiliki atau membagikannya, kebebasan tersebut di dilindungi oleh undang-undang yang berlaku di Indonesia. Berdasarkan landasan hukum tersebut, penduduk Indonesia memiliki hak konstitusional atas perlindungan hak privasinya, yang meliputi hak atas privasi atas informasi pribadinya. Negara diwajibkan berdasarkan hak konstitusionalnya untuk memberikan perlindungan hukum bagi berbagai aspek kehidupan warga negara Indonesia. Tujuan hukum untuk hak konstitusional harus mencakup keuntungan hukum, keadilan dan kejelasan.¹⁷ Berkaitan dengan perlindungan data pribadi, beberapa tindakan atau upaya yang telah dilakukan oleh Pemerintah Indonesia seperti yang terdapat dalam peraturan berikut ini: Undang-Undang Nomor 11 Tahun 2020 tentang Informasi dan Transaksi Elektronik (UU ITE), undang-undang ini meskipun lebih fokus pada transaksi elektronik dan keamanan informasi, tetapi memiliki ketentuan terkait perlindungan data pribadi dalam sistem elektronik. UU ini mewajibkan pengelola data untuk melindungi data pribadi dan memberikan sanksi bagi pelanggaran yang merugikan hak privasi. Pemerintah Indonesia telah merancang undang-undang yang secara khusus mengatur perlindungan data pribadi. UU ini merupakan langkah untuk menunjukkan upaya pemerintah dalam mengatasi perlindungan data pribadi dengan lebih komprehensif. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, peraturan ini mengatur perlindungan data pribadi dalam sistem elektronik dan memberikan pedoman tentang praktik yang benar dalam pengelolaan data pribadi. Pengaturan perlindungan data pribadi dalam sectoral, seperti beberapa sektor seperti perbankan, kesehatan, dan telekomunikasi, memiliki regulasi atau pedoman sendiri terkait perlindungan data pribadi. Contohnya, Bank Indonesia memiliki peraturan mengenai perlindungan data pribadi nasabah. Adanya pengawasan dan sanksi, sehingga pemerintah juga memiliki peran dalam mengawasi entitas yang mengelola data pribadi. Apabila terjadi pelanggaran, mereka dapat memberikan sanksi kepada pelaku yang melanggar ketentuan perlindungan data.

Upaya yang dilakukan oleh pemerintah adalah Pemerintah juga telah melakukan kampanye untuk meningkatkan kesadaran publik mengenai pentingnya melindungi data pribadi dan praktik yang aman dalam berbagi informasi pribadi. Pemerintah telah berusaha untuk mengembangkan kerangka kerja keamanan data yang membantu organisasi dan perusahaan dalam melindungi data pribadi yang mereka kelola. Pemerintah Indonesia juga terlibat dalam kerja sama internasional dalam bidang perlindungan data pribadi, termasuk mematuhi standar internasional yang diakui. Adapun upaya teknis yang dilakukan pemerintah hingga saat ini dalam perlindungan data pribadi warganegaranya diantara adalah Pemerintah dapat

¹⁶ Sekaring Ayumeida Kusnadi, “Perlindungan Hukum Data Pribadi Sebagai Hak Privasi,” *AL WASATH Jurnal Ilmu Hukum* 2, no. 1 (2021): 9–16, <https://journal.unusia.ac.id/alwasath/article/view/127>.

¹⁷ Hikmal Yusuf Argiansyah and M. Rizki Yudha Prawira, “Perlindungan Hukum Hak Atas Privasi Dan Perlindungan Data Pribadi Berdasarkan Perspektif Hak Asasi Manusia,” *Jurnal Hukum Pelita* 5, no. 1 (2024): 61–75, <https://www.researchgate.net/profile/M-Rizki-Yudha-Prawira/publication/381112415>.

menerapkan standar keamanan tinggi pada sistem dan infrastruktur yang mengelola data pribadi. Ini termasuk penggunaan enkripsi data, perlindungan terhadap serangan siber, dan penerapan *firewall* yang kuat. Pemerintah dapat menggunakan alat pemantauan untuk mendeteksi aktivitas anomali yang mencurigakan pada sistem atau jaringan. Ini bisa membantu mendeteksi upaya peretasan atau akses yang tidak sah. Pemerintah dapat mengeluarkan sertifikasi keamanan bagi organisasi atau layanan yang mengelola data pribadi, setelah mereka terbukti memenuhi standar keamanan tertentu. Pemerintah dapat mempekerjakan atau melibatkan auditor keamanan independen untuk melakukan audit rutin terhadap sistem dan praktik yang berkaitan dengan perlindungan data pribadi. Pemerintah dapat mengharuskan organisasi untuk melaporkan pelanggaran data pribadi secara segera kepada otoritas yang berwenang, sehingga tindakan cepat dapat diambil untuk meminimalkan dampaknya. Pemerintah dapat mendorong organisasi untuk memberikan pelatihan kepada karyawan mengenai praktik keamanan data, seperti cara mengenali *phishing* atau mengamankan kata sandi. Pemerintah dapat mendorong implementasi mekanisme otentikasi ganda atau akses terbatas untuk menghindari akses yang tidak sah ke data pribadi. Pemerintah dapat mendorong penggunaan enkripsi selama data dalam perjalanan antara pengirim dan penerima, misalnya melalui protokol HTTPS. Pemerintah dapat memberikan pedoman bagi organisasi tentang bagaimana data yang tidak lagi diperlukan harus dihapus atau dihancurkan secara aman. Pemerintah dapat mendorong organisasi untuk secara teratur melakukan pengujian keamanan, seperti uji penetrasi, untuk mengidentifikasi kerentanannya. Pemerintah dapat bekerja sama dengan perusahaan dan peneliti keamanan siber untuk memahami tren ancaman terbaru dan menerapkan langkah-langkah pencegahan yang sesuai.¹⁸

2. Tanggung Jawab Negara Terhadap Data Pribadi sebagai Hak Privasi Melalui Peraturan Undang-Undang

Tanggung jawab pemerintah Indonesia terhadap data pribadi sebagai hak privasi dapat dibandingkan dengan perlindungan terhadap data pribadi yang telah dilakukan oleh beberapa negara lainnya misalnya yang dilakukan oleh Singapura, Malaysia, Hong Kong, dan Korea Selatan. Undang-Undang Perlindungan Data Pribadi No. 26 Tahun 2012 Singapura (PDPA 2012) memberikan perlindungan hukum atas data pribadi di Singapura. Beberapa prinsip panduan untuk perlindungan hukum atas data pribadi diuraikan dalam PDPA Singapura 2012. Konsep "persetujuan yang dianggap", atau persetujuan yang diberikan secara eksplisit untuk digunakan untuk tujuan tertentu, diakui oleh peraturan tersebut. PDPA 2012 milik Singapura juga mengatur konsekuensi perdata dan pidana, termasuk denda hingga USD 790.000 dan/atau penjara hingga 3 (tiga) tahun.¹⁹ Selanjutnya Undang-Undang Perlindungan Data Pribadi No. 709 Tahun 2010 (PDPA Malaysia) adalah salah satu undang-undang dan peraturan yang melindungi data pribadi yang sudah ada di Malaysia. Untuk melindungi kepentingan subjek data, Personal Data Protection Act tahun 2010 mengatur bagaimana data pribadi diproses oleh pengguna data dalam rangka transaksi komersial.²⁰ Hal ini dilakukan dengan memastikan

¹⁸ N. Salsabila Nainggolan and P. Nasution, "Pentingnya Keamanan Big Data Dalam Lembaga Pemerintahan Di Era Digital," *Jurnal Jurnal Sains Dan Teknologi (JSIT)* 3, no. 2 (2023): 253, <https://pdfs.semanticscholar.org/6d84/4139b8d460f1542861aeeb9fde0ae3e6b7fe.pdf>.

¹⁹ Muhammad Afdan Rojabi, *Mengenal PDPA Singapura 2012: Dasar-Dasar Perlindungan Data Pribadi* (Afdan Rojabi Publisher, 2025).

²⁰ Hasventhran Baskaran et al., "Blockchain and the Personal Data Protection Act 2010 (PDPA) in Malaysia," *2020 8th International Conference on Information Technology and Multimedia (ICIMU)*, 2020, 189–93, <https://ieeexplore.ieee.org/abstract/document/9243493/>.

bahwa persetujuan subjek data diperoleh sebelum data pribadi apa pun diproses dan dengan memberi mereka kemampuan untuk melihat, memperbarui, dan mengelola pemrosesan data pribadi mereka. Komite Penasihat Perlindungan Data Pribadi didirikan di Malaysia berdasarkan Undang-Undang Perlindungan Data Pribadi 2010 dengan tanggung jawab menerima informasi mengenai ancaman dan transfer data pribadi yang tidak sah. PDPA Malaysia memiliki prinsip-prinsip berikut untuk perlindungan hukum atas data pribadi di Bagian 5 hingga 12:²¹ (1) Prinsip Umum Pemrosesan Berbasis Otorisasi (Pasal 6), yang melarang pengguna data memproses data pribadi tanpa izin pemilik data; (2) Pembatasan umum atas pemrosesan data pribadi diatur dengan kriteria “keabsahan, kebutuhan, dan tidak melebihi” (Pasal 6 Ayat 3); (3) Prinsip pengumpulan dan pemberitahuan, pemilik data harus mengetahui dan memberikan persetujuan untuk perolehan data pribadi, dan pengguna data harus memberi tahu pengguna data secara tertulis tentang alasan pengumpulan data pribadi; (4) Panduan penggunaan dan pengungkapan (paragraf 3 dari Bagian 6), apabila digunakan dan diproses untuk tujuan hukum, tujuan terkait data pengguna, dan tujuan pengumpulan dan pemrosesan data yang terhubung, data pribadi dapat digunakan dan diproses; (5) Data pribadi yang sensitif mencakup informasi tentang kesehatan individu, kondisi mental, keyakinan agama, klaim kesalahan, preferensi politik, dan topik spesifik lainnya; (6) Setiap pengguna data harus mematuhi konsep ini sesuai dengan aturan yang ditetapkan oleh Komisioner untuk perlindungan data pribadi; (7) Prinsip Retensi Data dan Hak Memblokir Pemrosesan karena data pengguna harus mematuhi pedoman penyimpanan Komisioner untuk Perlindungan Data Pribadi, ia harus memverifikasi bahwa data pribadi telah dihancurkan sepenuhnya setelah tujuan yang dimaksud terpenuhi; (8) Prinsip Integritas Data menyatakan Pengguna data pribadi dapat memastikan bahwa data tersebut benar, terkini, dan tidak mungkin diakses dengan mengambil tindakan pencegahan yang wajar; (9) Prinsip akses dan koreksi. Pemilik data pribadi berhak memperbarui dan mengubah informasi pribadi yang sudah usang, tidak benar, atau tidak lengkap.²²

Di Indonesia, dalam melakukan proses data pribadi berdasarkan sejumlah prinsip menurut peraturan perundang-undangan, sebagai dasar perlindungan data pribadi yaitu: *pertama*, Undang – Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan. Undang-undang ini menjelaskan bahwa frasa "rahasia bank" diartikan sebagai "segala sesuatu yang berkaitan dengan penabung dan simpanannya" dalam Pasal 1 Ayat (28) UUD. Ini mengklarifikasi bahwa setiap informasi terkait pelanggan di bank adalah masalah yang sensitif dan pribadi. Kecuali dalam keadaan sebagaimana dimaksud dalam Pasal 41, 41A, 42, 44, dan 44A, bank diharapkan menjaga kerahasiaan informasi yang disimpan nasabah penyimpan dan simpanannya, sesuai dengan Pasal 40 Ayat (1). Menurut pasal ini, bank wajib mengamankan semua data nasabah. Pihak Perbankan dalam melakukan pembukaan rekening dan atau melakukan transaksi perbankan harus memastikan bahwa identitas dalam hal ini KTP milik nasabah adalah identitas yang asli sesuai dengan sistem dukcapil. Hal ini jg sesuai dengan menjaga Rahasia Bank agar nasabah tidak menggunakan identitas yang palsu.²³

²¹ Kamal Halili Hassan, “Personal Data Protection in Employment: New Legal Challenges for Malaysia,” *Computer Law & Security Review* 28, no. 6 (2012): 696–703, <https://www.sciencedirect.com/science/article/pii/S0267364912001422>.

²² Edwin Lee Yong Cieh, “Personal Data Protection and Privacy Law in Malaysia,” in *Beyond Data Protection*, ed. Noriswadi Ismail and Edwin Lee Yong Cieh (Berlin, Heidelberg: Springer Berlin Heidelberg, 2013), 5–29, https://doi.org/10.1007/978-3-642-33081-0_2.

²³ Vicky Katiandagho, Diana Darmayanti Putong, and Isye Junita Melo, “Undang–Undang Perlindungan Data Pribadi Memperkuat Undang–Undang Perbankan Dalam Menjaga Rahasia Data Nasabah Dan Untuk

Kedua, Undang – Undang Nomor 36 Tahun 1999 tentang Telekomunikasi yang menjelaskan bahwa perlindungan data pribadi secara umum diatur oleh Undang-Undang Telekomunikasi, meskipun tidak secara khusus terkait dengan data pribadi. “Penyelenggara jasa telekomunikasi wajib merahasiakan informasi yang dikirim dan/atau diterima oleh pelanggan jasa telekomunikasi melalui jaringan telekomunikasi dan/atau jasa telekomunikasi yang diselenggarakannya,” bunyi Pasal 42 ayat 1 UU Telekomunikasi. Hal ini menjadi dasar kewajiban penyelenggara jasa untuk menjamin keamanan setiap data yang akan dikirim melalui jaringan telekomunikasi atau diterima melalui jasa telekomunikasi. Untuk keperluan proses peradilan pidana, penyelenggara jasa telekomunikasi dapat merekam informasi yang dikirim dan atau diterima oleh penyelenggara jasa telekomunikasi dan dapat memberikan informasi yang diperlukan atas: (a) permintaan tertulis dari Kejaksaan Agung dan/atau Kepala Kepolisian Negara Republik Indonesia. Republik Indonesia untuk tindak pidana tertentu; (b) permintaan tertulis dari Jaksa Agung dan/atau Kepala Kepolisian Republik Indonesia. Menurut Pasal 57 UU Telekomunikasi, “Penyelenggara jasa telekomunikasi yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 42 ayat (1) dipidana dengan pidana penjara paling lama 2 (dua) tahun dan atau denda paling banyak Rp200.000.000,00 (dua ratus juta rupiah).” Undang-Undang Telekomunikasi juga mengatur tentang sanksi mengenai tindak pidana terhadap keamanan informasi tersebut.²⁴

Ketiga, Undang – Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia (UU HAM). Hal ini karena setiap orang berhak untuk berkomunikasi dan mengakses pengetahuan yang diperlukan untuk mengembangkan kepribadian dan lingkungan sosialnya, sesuai dengan Pasal 14 Ayat 1 UUD. Pasal ini menegaskan bahwa setiap orang berhak untuk mengakses pengetahuan yang mereka butuhkan untuk kehidupan sehari-hari guna memajukan pertumbuhan mereka sendiri dan kualitas lingkungan tempat mereka tinggal. Dalam Pasal 29 Ayat (1) UU HAM disebutkan bahwa “Setiap orang berhak melindungi diri sendiri, keluarga, kehormatan, martabat, dan hak milik”. Pasal ini mengatur tentang hak atas perlindungan pribadi yang dijamin oleh Pasal 28 Huruf G Ayat (1) UUDNRI 1945. Menurut Pasal 32 UU HAM, yang menyatakan bahwa “Kemerdekaan dan kerahasiaan dalam hubungan korespondensi, termasuk hubungan komunikasi dengan sarana elektronik, tidak boleh diganggu, kecuali atas perintah hakim atau pejabat lain yang sah sesuai dengan ketentuan Undang-undang Hak Asasi Manusia. undang-undang,” ada juga tambahan baru pada undang-undang yang berkaitan dengan perlindungan data pribadi.²⁵

Keempat, Undang – Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Dalam undang-undang ini bahwa satu-satunya pasal yang secara tegas menjamin perlindungan data pribadi setelah diproses adalah Pasal 26 ayat (1), tetapi kemudian pengaturannya secara khususnya diatur Pasal 27 hingga 37, yang mengatur kegiatan ilegal di bidang informasi elektronik yang tidak secara khusus berkaitan dengan data pribadi. Pasal-pasal tersebut pada umumnya melarang perbuatan yang melanggar hak dan penyalahgunaan informasi elektronik dengan sengaja

Melindungi Data Pribadi Masyarakat Indonesia,” *Jurnal Hukum To-Ra: Hukum Untuk Mengatur Dan Melindungi Masyarakat* 9, no. 1 (2023): 106–14, <https://www.ejournal.fhuki.id/index.php/tora/article/view/212>.

²⁴ Three Boy and Ariawan Ariawan, “Peran Undang-Undang Perlindungan Data Pribadi Dan Hukum Telekomunikasi Dalam SPBE Di Indonesia,” *UNES Law Review* 6, no. 2 (2023): 5533–38, <https://review-unes.com/index.php/law/article/view/1379>.

²⁵ Nela mardiana Parihin, “Urgensi Perlindungan Data Pribadi Dalam Perpektif Hak Asasi Manusia,” *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia* 5, no. 1 (2023): 16–23, <https://rechten.nusaputra.ac.id/article/view/108>.

yang dapat merugikan orang lain, terutama pemilik informasi. Menyusul beberapa kasus peretasan, undang-undang PDP tampaknya menjadi solusi bagi warga Indonesia.²⁶ Penyelesaian sektor komersial organisasi pemerintah, dan masyarakat merupakan masalah terbesar pemerintah dalam mewujudkan UU PDP. Pemerintah harus memastikan bahwa setiap organisasi bisnis dan pemerintahan di Indonesia mampu mematuhi UU PDP. Rumah sakit, aplikasi layanan publik, perbankan industri, dan bisnis yang bergerak di bidang keuangan hanyalah beberapa di antaranya. Karena sangat mungkin mereka yang tidak memahami UU PDP kemudian melakukan pelanggaran tanpa disadari, melatih masyarakat untuk menaati UU tersebut menjadi tantangan tersendiri. UU PDP secara khusus mengatur proses privasi data bagi anak dan penyandang disabilitas. Namun, ada kecenderungan semua informasi tentang anak dan orang dewasa penyandang disabilitas disalahgunakan. Proses 'khusus' yang disebutkan dalam UU PDP belum diatur secara tegas, dan tidak ada batasan usia anak yang dianggap demikian. Indonesia memiliki Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang juga mencakup aspek perlindungan data pribadi. Namun, undang-undang ini dianggap belum cukup kuat dalam melindungi data pribadi. Pada November 2020, Indonesia mengesahkan Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) untuk meningkatkan perlindungan ini.

3. Maksud Putusan Mahkamah Konstitusi

Perlindungan data pribadi merupakan bagian yang tidak terpisahkan dari hak atas perlindungan diri pribadi sebagaimana dimaksud dalam Pasal 28G ayat (1) UUD NRI Tahun 1945. Perlindungan data pribadi adalah hak dasar setiap orang untuk mengendalikan informasi tentang diri mereka agar tidak disalahgunakan.²⁷ Di Indonesia, payung hukum utama yang mengatur hal ini adalah Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Jenis data pribadi adalah: (a) Data Umum, seperti nama lengkap, jenis kelamin, kewarganegaraan, agama, dan data yang dikombinasikan untuk mengidentifikasi seseorang; (b) Data Spesifik seperti data kesehatan, biometrik, genetika, kehidupan/orientasi seksual, pandangan politik, catatan kejahatan, data anak, dan data keuangan pribadi. Setiap orang berhak atas kerahasiaan data pribadinya, sehingga hak sebagai pemilik data adalah: hak mengakses (mengetahui jenis data apa saja yang dikumpulkan oleh perusahaan atau instansi; hak memperbaiki (meminta koreksi atas data yang salah atau tidak akurat); hak menghapus (meminta data untuk dihapus/hak untuk dilupakan, jika sudah tidak relevan atau kontrak selesai); hak menarik persetujuan (membatalkan izin penggunaan data yang pernah Anda berikan sebelumnya); hak mengajukan keberatan (menolak data untuk digunakan dalam pemasaran langsung atau pengambilan keputusan otomatis berbasis kecerdasan buatan /AI profiling).

Melalui uji materi Pasal 53 ayat (1) huruf b UU PDP yang diajukan karena penggunaan kata "dan" di akhir ayat tersebut dinilai mempersempit ruang lingkup perlindungan data. Kata hubung ini membuat syarat penunjukan Petugas Pelindungan Data Pribadi (PPDP) atau *Data Protection Officer* (DPO) bersifat kumulatif (semua kriteria harus terpenuhi sekaligus). Pasal 53 ayat (1) UU PDP selengkapanya berbunyi, "*Pengendali Data Pribadi dan Prosesor Data Pribadi*

²⁶ Muhammad Gustryan and Zainal Arifin Hoesein, "Peran Undang-Undang ITE Dan Undang-Undang Perlindungan Data Pribadi Dalam Perlindungan Data Dan Privasi Di Era Ekonomi Digital," *Jurnal Minfo Polgan* 14, no. 2 (2025): 3333–43, <https://jurnal.polgan.ac.id/index.php/jmp/article/view/15746>.

²⁷ Putra Wijaya and H. B. Gusliana, "Relevansi Hak Privasi Dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dengan Pasal 28 G Ayat 1 Undang-Undang Dasar Negara Republik Indonesia Tahun 1945," *Jurnal Ilmiah Wahana Pendidikan* 10, no. 22 (2024): 662–72, <http://www.jurnal.peneliti.net/index.php/JIWP/article/view/11126>.

*wajib menunjuk pejabat atau petugas yang melaksanakan fungsi Pelindungan Data Pribadi dalam hal: (a) pemrosesan Data Pribadi untuk kepentingan pelayanan publik; (b) kegiatan inti Pengendali Data Pribadi memiliki sifat, ruang lingkup, dan/atau tujuan yang memerlukan pemantauan secara teratur dan sistematis atas Data Pribadi dengan skala besar; dan (c) kegiatan inti Pengendali Data Pribadi terdiri dari pemrosesan Data Pribadi dalam skala besar untuk Data Pribadi yang bersifat spesifik dan/atau Data Pribadi yang berkaitan dengan tindak pidana”.*²⁸

Dirumuskannya kata “dan” sebagai kata penghubung dalam Pasal 53 ayat (1) huruf b UU PDP setelah akhir kalimat “*kegiatan inti Pengendali Data Pribadi memiliki sifat, ruang lingkup, dan/atau tujuan yang memerlukan pemantauan secara teratur dan sistematis atas Data Pribadi dengan skala besar.*” Hal ini dikhawatirkan bahwa pengendali data pribadi dan prosesor data pribadi dalam melaksanakan kegiatan pemrosesan data pribadi baru wajib menunjuk Petugas atau Pejabat Pelindungan Data Pribadi (PPDP) apabila unsur/kriteria pada huruf a, huruf b, dan huruf c ketiganya terpenuhi semua. Hal demikian terjadi karena rumusan kata “dan” tersebut mengandung makna kumulatif. Sementara sesuai dengan maksud pembentuk undang-undang dalam merumuskan huruf a, huruf b, dan huruf c dalam norma Pasal 53 ayat (1) UU PDP dimaksudkan sebagai kriteria mandiri/independen, yang jika terpenuhi salah satu, dua, atau keseluruhan kriteria persyaratan oleh pengendali data pribadi atau prosesor data pribadi, maka wajib baginya menunjuk PPDP. Dengan demikian, Maksud Mahkamah Konstitusi, bahwa rumusan yang tepat adalah bersifat alternatif kumulatif yaitu menggunakan frasa “dan/atau” yang lazim digunakan dalam perumusan suatu peraturan perundang-undangan sebagaimana diatur dalam angka 90 Lampiran II UU Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan. Hal demikian sesungguhnya telah menjawab kekhawatiran subjek data dikarenakan adanya aktivitas pemrosesan data pribadi yang berisiko tinggi (*high risk data processing activities*) sehingga perlindungan dan jaminan terhadap hak-hak konstitusional subjek data benar-benar terlindungi sedemikian rupa. Oleh karena itu, perlindungan data pribadi merupakan bagian yang tidak terpisahkan dari hak atas perlindungan data pribadi sebagaimana dimaksud Pasal 28G ayat (1) UUD NRI 1945.²⁹

Alasan tersebut menjadikan dalam Pasal 53 ayat (1) huruf b Undang-Undang Nomor 27 Tahun 2022 haruslah dinyatakan inkonstitusional. Dengan demikian melalui putusan Nomor 151/PUU-XXII/2024, maka Mahkamah Konstitusi menyatakan kata “dan” dalam Pasal 53 ayat (1) huruf b UU 27 Tahun 2022 tentang PDP bertentangan dengan UUD NRI Tahun 1945, mengubah kata “dan” menjadi “dan/atau”. Mahkamah Konstitusi menegaskan bahwa negara wajib memberikan perlindungan maksimal terhadap data pribadi warganya. Melalui pertimbangan hukum dalam putusan Nomor 151/PUU-XXII/2024,³⁰ Mahkamah Konstitusi menegaskan kembali bahwa data pribadi adalah hak asasi yang melekat pada privasi warga negara. Oleh karena itu, data tersebut tidak boleh dijadikan komoditas ekonomi atau objek yang merugikan tanpa adanya perlindungan hukum yang maksimal. Kewajiban negara memberikan perlindungan maksimal terhadap data pribadi warganya merupakan amanat konstitusi yang tertuang dalam Pasal 28G ayat

²⁸ Zico Junius Fernando, Ahmad Wali, and Desi Hafizah, “Konstitusionalisme Digital Di Indonesia: Pembatasan Kekuasaan Negara Dan Platform Dalam Perlindungan Hak Konstitusional Warga Di Ruang Siber,” *Konferensi Nasional Asosiasi Pengajar Hukum Tata Negara Dan Hukum Administrasi Negara* 3, no. 1 (2025): 429–50, <https://proceedingaphtnhan.id/index.php/paphtnhan/article/view/268>.

²⁹ Mediodecci Lustrini, “Kepastian Hukum Pelindungan Data Pribadi Pasca Pengesahan UU Nomor 27 Tahun 2022,” *Kementerian Komunikasi Dan Informatika*, 2022, https://jdih.komdigi.go.id/storage/file-artikel-hukum/1729219695-Kepastian_Hukum_PDP.pdf.

³⁰ Emillia Isni Maulidina, “Urgensi Uji Kebutuhan Dan Proporsionalitas Dalam Pengecualian Hak-Hak Subjek Data Pribadi Di Indonesia,” *Jurnal Analisis Hukum* 7, no. 2 (2024): 143–59, <https://journal.undiknas.ac.id/index.php/JAH/article/view/5464>.

(1) UUD NRI 1945. Pasal tersebut menjamin hak setiap orang atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya.

KESIMPULAN

Tanggung jawab negara terhadap hak perlindungan data pribadi di era digitalisasi adalah kewajiban konstitusional yang bersifat mutlak dan tidak dapat ditawar. Hal ini berdasarkan amanat Pasal 28G ayat (1) UUD 1945 dan arah hukum pasca Putusan MK Nomor 151/PUU-XXII/2024. Dengan demikian dapat disimpulkan bahwa terjadinya pergeseran paradigma hukum dari komoditas menjadi hak asasi manusia, maksudnya negara menegaskan bahwa di era digital, data pribadi bukan lagi sekadar komoditas ekonomi atau aset bisnis, melainkan eksistensi dari privasi dan martabat manusia. Oleh karena itu, negara bertanggung jawab mengintervensi pasar digital guna memastikan tidak ada eksploitasi data sepihak oleh korporasi maupun instansi publik. Adanya kewajiban proaktif melalui regulasi tanpa celah, yaitu negara tidak boleh pasif atau sekadar menjadi pemadam kebakaran saat terjadi kebocoran data. Lewat instrumen hukum seperti UU PDP, negara wajib menutup setiap celah hukum yang melemahkan keamanan data masyarakat yang salah satunya dengan memperketat kewajiban penunjukan Petugas Pelindungan Data Pribadi (PPDP) di berbagai sektor. Tanggung jawab negara baru dianggap tuntas dan nyata jika regulasi di atas kertas diikuti oleh tindakan konkret. Hal ini meliputi dua aspek utama yaitu penegakan sanksi, maksudnya menindak tegas dan menjatuhkan sanksi kepada pengendali data yang lalai; dan kelembagaan independent, dengan segera mengoperasikan Otoritas Perlindungan Data Pribadi yang independent agar pengawasan tidak tumpah tindih dengan kepentingan politik atau birokrasi pemerintah. Selain itu, sebagai saran, bahwa Pemerintah (Presiden) harus melompati hambatan birokrasi dan segera menetapkan Peraturan Presiden (Perpres) pembentukan Otoritas Perlindungan Data Pribadi yang independen agar tidak terjadi kekosongan penegakan hukum.

DAFTAR REFERENSI

- Argiansyah, Hikmal Yusuf, and M. Rizki Yudha Prawira. "Perlindungan Hukum Hak Atas Privasi Dan Perlindungan Data Pribadi Berdasarkan Perspektif Hak Asasi Manusia." *Jurnal Hukum Pelita* 5, no. 1 (2024): 61–75. <https://www.researchgate.net/profile/M-Rizki-Yudha-Prawira/publication/381112415>
- Armita, Jihan. "Pembobolan Saldo Rekening Nasabah Bank Dengan Cara Pemalsuan Identitas." PhD Thesis, Universitas Hasanuddin, 2021. <https://repository.unhas.ac.id/id/eprint/16087/>.
- Baskaran, Hasventhran, Salman Yussof, Fiza Abdul Rahim, and Asmidar Abu Bakar. "Blockchain and the Personal Data Protection Act 2010 (PDPA) in Malaysia." *2020 8th International Conference on Information Technology and Multimedia (ICIMU)*, 2020, 189–93. <https://ieeexplore.ieee.org/abstract/document/9243493/>.
- Boy, Three, and Ariawan Ariawan. "Peran Undang-Undang Perlindungan Data Pribadi Dan Hukum Telekomunikasi Dalam SPBE Di Indonesia." *UNES Law Review* 6, no. 2 (2023): 5533–38. <https://review-unes.com/index.php/law/article/view/1379>.
- Bratman, Ben. "Brandeis and Warren's The Right to Privacy and the Birth of the Right to Privacy." *Tenn. L. Rev.* 69 (2001): 623. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/tenn69§ion=27.
- Chemerinsky, Erwin. "Rediscovering Brandeis's Right to Privacy." *Brandeis LJ* 45 (2006): 643. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/branlaj45§ion=28.
- Cholik, Cecep Abdul. "Perkembangan Teknologi Informasi Komunikasi/ICT Dalam Berbagai

-
- Bidang.” *Jurnal Fakultas Teknik UNISA Kuningan* 2, no. 2 (2021): 39–46.
<https://www.neliti.com/publications/455512/perkembangan-teknologi-informasi->
- Cieh, Edwin Lee Yong. “Personal Data Protection and Privacy Law in Malaysia.” In *Beyond Data Protection*, edited by Noriswadi Ismail and Edwin Lee Yong Cieh, 5–29. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013. https://doi.org/10.1007/978-3-642-33081-0_2.
- Fathur, Muhammad. “Tanggung Jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen.” *National Conference on Law Studies (NCOLS)* 2, no. 1 (2020): 43–60.
<https://conference.upnvj.ac.id/index.php/ncols/article/view/1345>.
- Fernando, Zico Junius, Ahmad Wali, and Desi Hafizah. “Konstitusionalisme Digital Di Indonesia: Pembatasan Kekuasaan Negara Dan Platform Dalam Perlindungan Hak Konstitusional Warga Di Ruang Siber.” *Konferensi Nasional Asosiasi Pengajar Hukum Tata Negara Dan Hukum Administrasi Negara* 3, no. 1 (2025): 429–50.
<https://proceedingaphtnhan.id/index.php/paphtnhan/article/view/268>.
- Gustryan, Muhammad, and Zainal Arifin Hoesein. “Peran Undang-Undang ITE Dan Undang-Undang Perlindungan Data Pribadi Dalam Perlindungan Data Dan Privasi Di Era Ekonomi Digital.” *Jurnal Minfo Polgan* 14, no. 2 (2025): 3333–43.
<https://jurnal.polgan.ac.id/index.php/jmp/article/view/15746>.
- Hadi, Ismet. “Rekonstruksi Yurisprudensi Mahkamah Konstitusi Di Era Pengawasan Data.” *Jurnal Hukum Egalitaire* 3, no. 1 (2025): 83–103.
<https://journal.umgo.ac.id/index.php/jhe/article/view/5484>.
- Hassan, Kamal Halili. “Personal Data Protection in Employment: New Legal Challenges for Malaysia.” *Computer Law & Security Review* 28, no. 6 (2012): 696–703.
<https://www.sciencedirect.com/science/article/pii/S0267364912001422>.
- Katiandagho, Vicky, Diana Darmayanti Putong, and Isye Junita Melo. “Undang–Undang Perlindungan Data Pribadi Memperkuat Undang–Undang Perbankan Dalam Menjaga Rahasia Data Nasabah Dan Untuk Melindungi Data Pribadi Masyarakat Indonesia.” *Jurnal Hukum To-Ra: Hukum Untuk Mengatur Dan Melindungi Masyarakat* 9, no. 1 (2023): 106–14. <https://www.ejournal.fhuki.id/index.php/tora/article/view/212>.
- Komalawati, Desy, Maria Dewi MR, and Raiseta Dwi Kartika. “Kejutan Puluhan Miliar Tokopedia Ditengah Kasus Kebocoran Data.” . 2, no. 1 (2021): 49–56.
<https://jurnalsyntaxadmiration.com/index.php/jurnal/article/download/167/249>.
- Kusnadi, Sekaring Ayumeida. “Perlindungan Hukum Data Pribadi Sebagai Hak Privasi.” *AL WASATH Jurnal Ilmu Hukum* 2, no. 1 (2021): 9–16.
<https://journal.unusia.ac.id/alwasath/article/view/127>.
- Lustarini, Mediodecci. “Kepastian Hukum Pelindungan Data Pribadi Pasca Pengesahan UU Nomor 27 Tahun 2022.” *Kementerian Komunikasi Dan Informatika*, 2022.
https://jdih.komdigi.go.id/storage/file-artikel-hukum/1729219695-Kepastian_Hukum_PDP.pdf.
- Luthfi, Rosihan. “Perlindungan Data Pribadi Sebagai Perwujudan Perlindungan Hak Asasi Manusia.” *Jurnal Sosial Teknologi* 2, no. 5 (2022): 431–36.
<http://sostech.greenvest.co.id/index.php/sostech/article/view/336>.
- Maulidina, Emillia Isni. “Urgensi Uji Kebutuhan Dan Proporsionalitas Dalam Pengecualian Hak-Hak Subjek Data Pribadi Di Indonesia.” *Jurnal Analisis Hukum* 7, no. 2 (2024): 143–59.
<https://journal.undiknas.ac.id/index.php/JAH/article/view/5464>.
- Mutiara, Upik, and Romi Maulana. “Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi.” *Indonesian Journal of Law and Policy Studies* 1,

- no. 1 (2020). <https://www.academia.edu/download/96517028/1629.pdf>.
- Nainggolan, N. Salsabila, and P. Nasution. "Pentingnya Keamanan Big Data Dalam Lembaga Pemerintahan Di Era Digital." *Jurnal Jurnal Sains Dan Teknologi (JSIT)* 3, no. 2 (2023): 253. <https://pdfs.semanticscholar.org/6d84/4139b8d460f1542861aeeb9fde0ae3e6b7fe.pdf>.
- Pakina, Ridho, and Mohammad Solekhan. "Pengaruh Teknologi Informasi Terhadap Hukum Privasi Dan Pengawasan di Indonesia: Keseimbangan Antara Keamanan dan Hak Asasi Manusia." *Journal of Scientech Research and Development* 6, no. 1 (2024): 273–86. <https://www.idm.or.id/JSCR/index.php/JSCR/article/view/376>.
- Panggabean, Marshanda Vennesa, and Annisa Fitria. "Perlindungan Hukun Data Pribadi Di Indonesia (Kasus Kebocoran Badan Penyelenggara Jaminan Sosial Kesehatan)." *Arus Jurnal Sosial Dan Humaniora* 5, no. 2 (2025): 1958–65. <http://www.jurnal.ardenjaya.com/index.php/ajsh/article/view/1487>.
- Parihin, Nela mardiana. "Urgensi Perlindungan Data Pribadi Dalam Perpektif Hak Asasi Manusia." *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia* 5, no. 1 (2023): 16–23. <https://rechten.nusaputra.ac.id/article/view/108>.
- Rojabi, Muhammad Afdan. *Mengenal PDPA Singapura 2012: Dasar-Dasar Perlindungan Data Pribadi*. Afdan Rojabi Publisher, 2025. <https://www.google.com/books?>
- Suharyanti, Ni Putu Noni, and Ni Komang Sutrisni. "Urgensi Perlindungan Data Pribadi Dalam Menjamin Hak Privasi Masyarakat." *Prosiding Seminar Nasional Fakultas Hukum Universitas Mahasaraswati Denpasar 2020* 1, no. 1 (2021): 119–34. <https://e-journal.unmas.ac.id/index.php/psnfh/article/view/2395>.
- Sulistyawati, Upik Sri. "Membangun Keunggulan Kompetitif Melalui Platform E-Commerce: Studi Kasus Tokopedia." *Jurnal Manajemen Dan Teknologi* 1, no. 1 (2024): 43–56. <http://journal.stmiki.ac.id/index.php/jmt/article/view/776>.
- Wijaya, Putra, and H. B. Gusliana. "Relevansi Hak Privasi Dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dengan Pasal 28 G Ayat 1 Undang-Undang Dasar Negara Republik Indonesia Tahun 1945." *Jurnal Ilmiah Wahana Pendidikan* 10, no. 22 (2024): 662–72. <http://www.jurnal.peneliti.net/index.php/JIWP/article/view/11126>.
- Zahro, Yulisa Laili. "Pengetahuan Hukum Masyarakat Tentang Penyelesaian Masalah Pelanggaran Atas Layanan Ojek Online Berbasis Aplikasi (Studi Pada Go-Jek Dan Grab Di Wilayah Kabupaten Cilacap)." PhD Thesis, Universitas Islam Indonesia, 2019. <https://dspace.uui.ac.id/handle/123456789/19795>.