Jurnal Pemuliaan Hukum – ISSN: 2654-2722 (p) 2829-8640 (e)
Vol. 6, No. 2 (April 2024), pp. 147-162, doi: 10.30999/ ph.v6i2.3430
Faculty of Law, Nusantara Islamic University (UNINUS) Bandung, Indonesia
Jl. Soekarno Hatta No. 530, Sekejati, Kec. Buahbatu, Bandung City, West Java 40286, Indonesia

Menilik Ketiadaan Regulasi Mengenai Perlindungan Data Pribadi Konsumen di Ruang Maya

Irpan Maulana[1], Ishma yunisa Nurhasanah[2], Ahmad Irfan Abdul Majid[3]
[1]Fakultas Hukum Universitas Islam Nusantara, Indonesia
Correspondence: *irpanmlna031@gmail.com*

Artikel

Keywords:
consumer legal protection; personal data; digital platform.

Artikel History:
Submission: 2024-08-22
Accepted: 2024-08-26
Published: 2024-08-27

DOI:
10.30999/ ph.v6i2.3430

Abstract

This research examines the legal protection of consumer personal data in cyberspace, particularly in transactions through digital platforms. With the increase in digital transactions, the issue of consumer personal data security is becoming increasingly urgent, requiring strict and comprehensive regulations. This research uses a normative method with a statutory approach and juridical analysis of the applicable regulations. The research findings show that although there are several regulations regarding personal data protection in Indonesia, these regulations have not been fully effective in protecting consumers from potential data misuse. Therefore, it is necessary to accelerate the ratification of a more comprehensive Personal Data Protection Law to strengthen consumer protection in the digital era.

Kata kunci: perlindungan hukum konsumen; data pribadi; platform digital.

Abstrak

Penelitian ini mengkaji perlindungan hukum data pribadi konsumen di ruang maya, khususnya dalam transaksi melalui platform digital. Dengan meningkatnya transaksi digital, isu keamanan data pribadi konsumen menjadi semakin mendesak, membutuhkan regulasi yang tegas dan komprehensif. Penelitian ini menggunakan metode normatif dengan pendekatan perundang-undangan serta analisis yuridis terhadap regulasi yang berlaku. Temuan penelitian menunjukkan bahwa meskipun terdapat beberapa regulasi mengenai perlindungan data pribadi di Indonesia, aturan tersebut belum sepenuhnya efektif dalam melindungi konsumen dari potensi penyalahgunaan data. Oleh karena itu,

diperlukan percepatan pengesahan Undang-Undang Perlindungan Data Pribadi yang lebih komprehensif guna memperkuat perlindungan konsumen di era digital.

Pendahuluan

Saat ini, dunia telah memasuki era postmodern, di mana perkembangan pesat dalam berbagai aspek kehidupan, termasuk sosial dan sumber informasi, telah mengubah cara manusia mengelola data secara digital. Revolusi digital telah menghasilkan penemuan baru dalam pengumpulan, penyimpanan, perubahan, dan pengiriman volume data yang luas dan kompleks secara real-time. Hal ini membuat revolusi digital dan revolusi data kerap dianggap sama. Seiring dengan perkembangan ini, pengumpulan berbagai jenis data meningkat pesat, dan baik sektor swasta maupun pemerintah berlomba-lomba meningkatkan kapasitas penyimpanan data. Data menjadi aset berharga layaknya aset berwujud lainnya karena memiliki nilai baru yang dapat dieksplorasi, menandai munculnya era Big Data dalam manajemen data.[1]

Di Indonesia, Undang-Undang Dasar Republik Indonesia Tahun 1945 menjadi fondasi hukum yang menjamin perlindungan data pribadi, terutama berakar pada hak-hak asasi manusia. Pasal 28F UUD 1945 memberikan hak kepada individu untuk berkomunikasi dan mendapatkan informasi, serta untuk menyimpan, mengolah, dan mengkomunikasikan informasi melalui berbagai saluran.[2] Pasal 28G ayat 1 dari Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 menegaskan bahwa setiap individu memiliki hak untuk melindungi diri sendiri, keluarga, kehormatan, martabat, dan properti yang mereka miliki. Mereka juga berhak merasa aman dan terlindungi dari segala bentuk ancaman yang dapat menghalangi mereka untuk melakukan atau tidak melakukan tindakan yang merupakan hak dasar mereka.[3] Dalam Konstitusi Republik Indonesia, terdapat beberapa regulasi yang mengatur tentang perlindungan data pribadi. Ini termasuk Undang-Undang Hak Asasi Manusia No. 39/1999, Undang-Undang Telekomunikasi No. 36/1999, Undang-Undang Keterbukaan Informasi Publik No. 14/2008, Undang-Undang Informasi dan Transaksi Elektronik No. 11/2008, Undang-Undang Administrasi Kependudukan No. 23/2014, Undang-Undang Perbankan No. 10/1998,

[1] Piyush Malik, "Governing Big Data: Principles and Practices," *IBM Journal of Research and Development* 57, no. 3/4 (2013): 1–1.

[2] Andi Muhammad Asrun, "Hak Asasi Manusia Dalam Kerangka Negara Hukum: Catatan Perjuangan Di Mahkamah Konstitusi," *Jurnal Cita Hukum* 4, no. 1 (2016).

[3] Loura Hardjaloka and Varida Megawati Simarmata, "E-Voting: Kebutuhan vs. Kesiapan (Menyongsong) e-D *Jurnal Konstitusi* 8, no. 4 (2011): 579–604.

Undang-Undang Perlindungan Konsumen No. 8/1999, Peraturan Menteri Komunikasi dan Informatika No. 20/2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, serta Rancangan Undang-Undang Perlindungan Data Pribadi.[4]

Sementara itu, Pasal 8 dari Konvensi Eropa merupakan landasan utama dari hak perlindungan data, yang ditujukan untuk melindungi individu di zaman masyarakat informasi ini. Di Eropa, perlindungan atas data pribadi telah mengalami perkembangan, terutama melalui sistem hukum common law. Jerman menjadi negara pertama yang menerapkan undang-undang perlindungan data pada tahun 1970, disusul oleh Inggris, Swedia, Perancis, Swiss, dan Austria. Sementara di Amerika Serikat, Fair Credit Reporting Act yang dikeluarkan pada tahun yang sama, juga memberikan perlindungan data serupa.[5] Berdasarkan latar belakang ini, masalah yang akan dibahas adalah perlindungan hukum bagi konsumen terhadap data pribadi di platform digital. Hal ini disebabkan oleh tidak adanya undang-undang khusus di Indonesia yang mengatur tentang perlindungan data pribadi, yang menyebabkan kekosongan hukum. Oleh karena itu, jurnal dengan judul Perlindungan Hukum Konsumen atas Data Pribadi di Platform Digital menjadi fokus penulis.

Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah metode penelitian hukum normatif. Penelitian hukum normatif berfokus pada hukum sebagai standar dan norma untuk menganalisis perkembangan sistem hukum. Sistem norma yang dianalisis mencakup berbagai sumber hukum, seperti aturan perundang-undangan, prinsip-prinsip hukum, perjanjian internasional, doktrin atau ajaran hukum, serta putusan pengadilan. Dalam penelitian ini, penulis melakukan analisis terkait ketiadaan regulasi mengenai perlindungan data pribadi konsumen di ruang maya dengan mengacu pada norma-norma hukum yang berlaku, termasuk undang-undang yang relevan serta prinsip-prinsip hukum yang diakui. Selain itu, penelitian ini mencakup kajian doktrin hukum dan putusan pengadilan yang dapat memberikan landasan hukum terhadap isu yang diangkat. Data dalam penelitian ini diperoleh dari studi pustaka, yang mencakup bahan hukum primer dan sekunder. Bahan hukum primer terdiri dari perundang-undangan yang relevan, sedangkan bahan hukum sekunder mencakup literatur hukum, doktrin, dan kajian akademis yang membahas topik serupa. Proses pengumpulan data dilakukan dengan menelusuri literatur hukum yang berkaitan dengan perlindungan data pribadi dan ketidakadaan regulasi khusus di ruang maya. Analisis data dilakukan dengan menggunakan metode deduktif, di mana

[4] Siti Yuniarti, "Perlindungan Hukum Data Pribadi Di Indonesia," *Business Economic, Communication, and Social Sciences Journal (BECOSS)* 1, no. 1 (2019): 147–54.
[5] Fanny Priscyllia, "Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum," *Jatiswara* 34, no. 3 (2019): 239–49.

penulis memulai dengan prinsip-prinsip hukum yang bersifat umum dalam sistem hukum yang berlaku. Prinsip-prinsip ini kemudian diterapkan untuk menganalisis kasus konkret mengenai ketiadaan regulasi perlindungan data pribadi di ruang maya. Pendekatan ini memungkinkan penulis untuk mengkaji apakah norma-norma yang ada cukup memadai untuk memberikan perlindungan terhadap konsumen di era digital atau memerlukan pembaruan regulasi.[6]

Hasil dan Pembahasan

Perlindungan Data Pribadi Konsumen di Platform Digital

Putusan hakim sebelumnya, yang didasarkan pada yurisprudensi, menunjukkan bahwa sistem *common law* di Eropa melindungi data pribadi konsumen. Hukum umum dibuat oleh hakim. Ini adalah jumlah total kasus yang telah diselesaikan oleh pengadilan banding negara bagian tersebut. Semua kasus yang diputuskan oleh pengadilan banding *Illinois* terdiri dari hukum umum *Illinois*. Hampir semua hukum dua abad yang lalu adalah hukum umum. Saat ini, *common law* masih sangat penting dalam hukum gugatan, kontrak, dan keagenan, serta sangat penting dalam properti, pekerjaan, dan bidang lainnya. Di Indonesia, istilah perlindungan data pribadi digunakan dengan cara yang berbeda. Di Amerika Serikat, Kanada, dan Australia, istilah PII digunakan. antara sistem hukum sipil dan common law. Meskipun *common law* tidak memiliki alat khusus yang dapat secara ketat menafsirkan arti data pribadi, ada tiga cara untuk menjelaskan istilah tersebut: pendekatan tautologis (*tautological approach*), pendekatan non-publik (*non-public approach*), dan pendekatan khusus (*specific type approach*).[7]

Sebagai contoh, di Amerika Serikat yang menganut sistem hukum common law, telah ada kebijakan yang melindungi privasi, seperti Privacy Act 1974 yang disahkan oleh Kongres. Namun, tidak ada satu undang-undang nasional pun yang mengatur secara komprehensif tentang pengelolaan dan penggunaan data pribadi. Konsep perlindungan privasi telah termasuk dalam berbagai regulasi federal yang sering kali memiliki persilangan, kesamaan, atau kontradiksi. Regulasi-regulasi ini hanya mengatur pembatasan dalam pengumpulan dan penggunaan informasi pribadi oleh lembaga federal sehubungan dengan Privacy Act 1974, dan tidak berlaku untuk entitas swasta atau badan pemerintah lainnya. Pada dasarnya, undang-undang ini melarang pembukaan data pribadi oleh perusahaan atau lembaga pemerintah tanpa persetujuan dari pemilik data, kecuali dalam situasi tertentu yang membutuhkan pemeriksaan hukum.

Perubahan besar dalam regulasi perlindungan data di Eropa dihasilkan oleh Meski telah ada undang-undang seperti UU ITE dan UU Administrasi Kependudukan, perlindungan data pribadi belum diatur secara komprehensif. Hal ini menciptakan celah hukum yang bisa dimanfaatkan oleh pihak-pihak yang

[6] Benito Asdhie Kodiyat, "Fungsi Partai Politik Dalam Meningkatkan Partsipasi Pemilih Pada Pemilihan Umum Kepala Daerah Di Kota Medan," *EduTech: Jurnal Ilmu Pendidikan Dan Ilmu Sosial* 5, no. 1 (2019).
[7] HS Salim, *Hukum Kontrak: Teori Dan Teknik Penyusunan Kontrak* (Bandung: Sinar Grafika, 2021).

tidak bertanggung jawab, baik di dalam negeri maupun dari luar negeri, untuk mengakses dan memanfaatkan data pribadi secara ilegal. Seiring dengan meningkatnya penggunaan layanan digital oleh konsumen dan pelaku usaha, penting bagi Indonesia untuk mengadopsi regulasi yang lebih ketat dan jelas, seperti General Data Protection Regulation (GDPR) di Uni Eropa, yang terbukti efektif dalam melindungi data pribadi. Tantangan hukum dalam menegakkan perlindungan data di Indonesia mencakup kesulitan pembuktian pelanggaran data di pengadilan, seperti kasus Facebook-Cambridge Analytica yang menunjukkan kelemahan sistem hukum Indonesia dalam memberikan solusi bagi pelanggaran data. Selain itu, ketidakkonsistenan regulasi antara UU ITE, UU Pers, dan UU Keterbukaan Informasi Publik (KIP) juga menambah tantangan dalam implementasi hukum, terutama terkait hak untuk dilupakan yang diadopsi dari GDPR. Ketidakpastian dalam regulasi ini juga berpengaruh pada kepercayaan konsumen terhadap layanan digital dan berdampak negatif pada pertumbuhan ekonomi digital. Beberapa kasus besar seperti kebocoran data di Tokopedia dan Bukalapak telah memperburuk situasi ini. Dari perspektif ekonomi, kepercayaan konsumen yang menurun juga mengurangi daya saing Indonesia di pasar global, di mana harmonisasi regulasi dengan standar internasional seperti GDPR menjadi penting untuk menarik investasi teknologi global. Selain itu, peran otoritas perlindungan data yang independen dan bertanggung jawab dalam mengawasi pelaksanaan peraturan serta memberi panduan dan sanksi terhadap pelanggaran sangatlah krusial. Pengendali data juga perlu bertanggung jawab dalam memastikan keamanan data melalui audit, pelatihan, dan penerapan kebijakan perlindungan data yang kuat. Analisis yang lebih kritis menunjukkan bahwa ketidakjelasan regulasi perlindungan data pribadi tidak hanya berdampak pada aspek hukum, tetapi juga memengaruhi kepercayaan konsumen dan perkembangan ekonomi digital. Indonesia perlu segera melakukan harmonisasi regulasi dengan standar internasional dan memastikan penegakan hukum yang efektif untuk melindungi hak konsumen di era digital. Pada Januari 2018, legislasi perlindungan data telah diadopsi sebagai undang-undang nasional di lebih dari seratus negara.

Secara umum, struktur undang-undang perlindungan data terdiri dari beberapa elemen kunci yang berfungsi untuk melindungi data pribadi dalam berbagai konteks. *Pertama*, perlindungan data mencakup pengendali dan pemroses data, serta mengatur tentang wilayah dan yurisdiksi yang relevan dalam proses pengelolaan data. *Kedua*, undang-undang ini mendefinisikan jenis-jenis data pribadi yang dilindungi dan memberikan definisi yang jelas tentang apa yang dimaksud dengan data pribadi. *Ketiga*, konsep yang mendukung perlindungan data juga diatur dalam undang-undang ini, termasuk alasan yang sah untuk pemrosesan data, seperti persetujuan dari pemilik data atau subjek data, kepentingan publik, dan kewajiban hukum. *Keempat*, pengendali dan pemroses

data memiliki tanggung jawab tertentu, termasuk memastikan data diproses dengan cara yang sah, adil, dan transparan, serta menjaga keamanannya. *Kelima*, undang-undang perlindungan data juga menetapkan hak-hak pemilik data atau subjek data, seperti hak untuk mengakses data mereka, hak untuk memperbaiki atau menghapus data yang tidak akurat, dan hak untuk menolak pemrosesan data dalam kondisi tertentu. *Keenam*, terdapat pengawas independen, yang juga dikenal sebagai otoritas perlindungan data, yang bertanggung jawab atas pengawasan dan penegakan hukum terkait perlindungan data pribadi. Otoritas ini berfungsi untuk memastikan kepatuhan terhadap undang-undang perlindungan data dan mengambil tindakan terhadap pelanggaran yang terjadi.[8]

Perlindungan data secara umum adalah kumpulan prosedur dan peraturan yang dirancang untuk menjaga keamanan informasi pribadi serta memberikan kontrol kepada pihak yang mengelolanya. Hal ini memungkinkan pemilik data untuk menentukan pilihan terkait dengan pembagian informasi, akses, durasi akses, tujuan penggunaan informasi, serta kemungkinan modifikasi informasi tersebut. Sementara itu, definisi data pribadi menurut GDPR Uni Eropa adalah informasi yang berkaitan dengan individu yang bisa diidentifikasi, baik secara langsung maupun tidak langsung, melalui pengenal seperti nama, nomor identifikasi, atau faktor lain yang berkaitan dengan identitas fisik, mental, atau sosial individu tersebut.[9]

Untuk memperluas analisis terkait implikasi hukum dari ketiadaan regulasi perlindungan data pribadi konsumen di ruang maya, beberapa poin kritis perlu ditambahkan. Meskipun pembahasan awal telah menguraikan perlindungan data di beberapa negara dan komparasi dengan Indonesia, terdapat celah yang signifikan terkait dampak ketidakjelasan regulasi perlindungan data pribadi. Ketidakjelasan regulasi perlindungan data pribadi di Indonesia memunculkan risiko serius bagi konsumen, terutama di era digital yang semakin kompleks di mana data pribadi dapat diakses dan digunakan tanpa persetujuan jelas. Hal ini memberikan celah bagi pelanggaran privasi, baik oleh entitas komersial maupun pihak ketiga, yang dapat menyalahgunakan data untuk tujuan ilegal. Tanpa perlindungan hukum yang komprehensif, konsumen sering kali tidak memiliki jalur hukum yang efektif untuk menuntut pelanggaran privasi mereka, sebagaimana terlihat pada kasus kebocoran data Cambridge Analytica. Perbandingan dengan GDPR Uni Eropa menunjukkan bahwa Indonesia belum memiliki regulasi yang setara, yang dapat berdampak pada rendahnya rasa aman masyarakat dalam menggunakan layanan digital serta menurunkan kepercayaan terhadap platform online. Ketiadaan regulasi yang jelas juga menimbulkan ketidakpastian bagi pelaku usaha terkait penanganan data pribadi, meningkatkan risiko litigasi di masa depan. Pandangan ahli hukum seperti Alan Westin yang

[8] Theddy Hendrawan Nasution and others, "Perlindungan Hukum Data Pribadi Nasabah Dalam Penggunaan Big Data Oleh Perbankan Di Indonesia (Studi Komparatif Penggunaan Data Pribadi Nasabah Di Uni Eropa)," 2020.
[9] Erlina Maria Christin Sinaga and Mery Christian Putri, "Formulasi Legislasi Perlindungan Data Pribadi Dalam Revolusi Industri 4.0," *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional* 9, no. 2 (2020): 237.

mengedepankan privasi sebagai hak fundamental, serta studi kasus kebocoran data Tokopedia atau Bukalapak, semakin memperkuat argumen bahwa konsumen Indonesia berisiko lebih tinggi terhadap pelanggaran data. Selain implikasi hukum, ketidakjelasan regulasi juga berdampak pada aspek ekonomi dan sosial, di mana kepercayaan konsumen menurun, mengganggu perkembangan ekonomi digital, serta menimbulkan rasa ketidakamanan di masyarakat. Indonesia juga perlu mempertimbangkan harmonisasi regulasi dengan standar internasional seperti GDPR, mengingat data bergerak lintas batas negara. Hal ini penting untuk meningkatkan daya saing Indonesia di pasar global.

Data otomatis dan pemrosesannya, serta format terstruktur yang disimpan secara manual (sistem pengarsipan), harus dilindungi oleh undang-undang. Dengan kata lain, undang-undang tersebut harus mencakup semua pemrosesan data yang terjadi di komputer, telepon, perangkat IoT, dan catatan kertas. Selain itu, ia mencakup institusi swasta dan publik. Namun, umumnya diketahui bahwa pemrosesan untuk tujuan individu atau rumah tangga dikecualikan dari pemberlakuan hukum. Secara keseluruhan, undang-undang perlindungan data juga memperhatikan bahwa data dapat berpindah antarnegara, yang sering menimbulkan masalah yurisdiksi, termasuk potensi konflik dengan hukum nasional yang berlaku. Hukuman harus difokuskan pada individu, dengan memastikan bahwa data pribadi tetap terlindungi, baik saat diproses di dalam maupun di luar wilayah asal. Dengan pendekatan ini, data pribadi hanya dapat ditransfer ke pihak luar negeri jika tingkat perlindungan data yang diterapkan oleh penerima setidaknya setara dengan peraturan yang berlaku di negara asal.

Sementara itu, pengendali dan pengolah data biasanya bertanggung jawab untuk memastikan bahwa pemrosesan data mereka sesuai dengan hukum melalui tindakan organisasi dan teknis. Mereka biasanya bertanggung jawab atas hal-hal berikut: Sebagai peneliti, Anda memiliki tanggung jawab untuk memastikan keamanan data. Berikut ini adalah ringkasan dari kebijakan dan prosedur perlindungan data yang Anda perlu implementasikan: melakukan audit data secara berkala; mengadopsi pendekatan privasi yang komprehensif mulai dari desain hingga default; menunjuk Petugas Perlindungan Data (DPO); mengembangkan prosedur yang transparan untuk pemilik data; melakukan penilaian berkala terhadap pemilik data; meningkatkan keahlian staf dalam hal keamanan data; mengimplementasikan langkah keamanan yang kuat; serta mendirikan prosedur yang jelas untuk menghadapi, mencatat, dan melaporkan pelanggaran data. Selain itu, Anda harus memastikan bahwa semua hak subjek data dipenuhi, termasuk hak untuk mendapatkan informasi, mengakses, memperbaiki, memblokir, dan menghapus data; hak untuk menolak pemrosesan data; hak portabilitas data; hak terhadap profil dan pengambilan keputusan otomatis; serta hak untuk mendapatkan kompensasi dan pengakuan tanggung jawab atas pelanggaran yang terjadi.

Tinjauan Hukum tentang Perlindungan Data Pribadi di Era Digital

Indonesia telah mengadopsi undang-undang yang menjamin perlindungan data pribadi penggunanya. Seiring dengan perubahan zaman, hak atas privasi, termasuk perlindungan data pribadi, semakin diakui sebagai hak konstitusional oleh UUD 1945 setelah beberapa kali amandemen. Hak ini termasuk dalam bab baru tentang hak asasi manusia, yaitu Bab XA Pasal 28A-J. Pasal 28G ayat (1) secara khusus menjamin bahwa setiap individu berhak melindungi diri, keluarga, kehormatan, martabat, dan properti mereka serta memiliki hak untuk merasa aman dan terlindungi dari segala bentuk ancaman.[10] Selain adanya jaminan perlindungan konstitusi, keikutsertaan Indonesia sebagai negara pihak juga menambah perlindungan dalam hal data pribadi. Ini dilakukan sesuai dengan Undang-Undang No. 39/1999 tentang Hak Asasi Manusia, yang antara lain melalui Pasal 14(2), Pasal 29(1), dan Pasal 31, mengamankan hak warga negara terhadap privasi. Khususnya, Pasal 29 ayat pertama menyatakan hak setiap individu untuk menjaga diri, keluarga, kehormatan, martabat, dan kepemilikannya, melindungi data pribadi dan hubungan. Sementara itu, Pasal 14 ayat 2 menyebutkan bahwa hak untuk mencari, mengumpulkan, menyimpan, mengolah, dan menyebarkan informasi adalah bagian dari hak mengembangkan diri. Terkait dengan ini, Pasal 31 dalam UU HAM menegaskan bahwa kerahasiaan komunikasi elektronik harus dilindungi, kecuali bila dibutuhkan oleh hakim atau otoritas yang berwenang menurut hukum yang berlaku.

Secara lebih spesifik, terdapat berbagai undang-undang dan peraturan yang mengatur tentang perlindungan, pengumpulan, pemrosesan, penggunaan, dan pengungkapan data pribadi. Undang-undang ini mencakup berbagai sektor, antara lain: (i) telekomunikasi dan informatika; (ii) kependudukan dan kearsipan; (iii) keuangan, perbankan, dan perpajakan; (iv) perdagangan dan industri; (v) layanan kesehatan; dan (vi) penegakan hukum dan keamanan. Berdasarkan UU No. 36 Tahun 1999 tentang Telekomunikasi, hak atas privasi dalam sektor telekomunikasi dan informatika terbatas pada kerahasiaan informasi dan komunikasi pribadi. Undang-undang ini juga memberi kewenangan kepada penyelenggara telekomunikasi untuk merekam komunikasi sebagai bukti pemakaian fasilitas telekomunikasi atas permintaan pelanggan. Selanjutnya, UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menegaskan kebutuhan perlindungan data pribadi dalam pengoperasian sistem elektronik. Transfer data pribadi harus mendapat izin dari pemilik data sesuai dengan ketentuan dalam Pasal 26 ayat (1) UU ITE.

Berdasarkan Pasal 26 ayat 2, penerima data pribadi memiliki hak untuk mengajukan gugatan ganti rugi di pengadilan. Namun, pemilik data sering menghadapi kesulitan dalam menuntut dugaan kebocoran data pribadinya secara hukum karena tantangan dalam pembuktian di pengadilan perdata Indonesia.

[10] Indonesia, *Constitution of the Republic of Indonesia* (Information Division, Embassy of Indonesia, 1945).

Hingga tahun 2018, hanya satu gugatan warga negara (citizen lawsuit/CLS) yang diajukan ke pengadilan. Sebagai contoh, dalam kasus Cambridge Analytica, sekelompok pengguna Facebook Indonesia menggugat perusahaan tersebut karena diduga membocorkan data mereka. Selain itu, setelah putusan Mario Costeja di Pengadilan Eropa (CJEU) pada tahun 2014 yang menetapkan klausul hak untuk dilupakan, perubahan UU ITE pada tahun 2016 juga membawa dampak. Dalam revisi UU tersebut, para legislator mengusulkan agar Indonesia turut mengadopsi prinsip "hak untuk dilupakan". Pasal 26 ayat (3) dari UU No. 19 Tahun 2016, yang merupakan amandemen dari UU No. 11 Tahun 2008 tentang ITE, mengatur bahwa setiap pengelola sistem elektronik wajib menghapus informasi atau dokumen elektronik yang tidak lagi relevan jika diminta oleh individu yang bersangkutan, sesuai dengan putusan pengadilan.

Regulasi pemerintah akan memberikan ketentuan lebih detail tentang penghapusan informasi yang tidak relevan, seperti disebutkan dalam Pasal 26 ayat 4. Rumusan tersebut hanya menyinggung penghapusan Dokumen Elektronik dan Informasi Elektronik yang dianggap tidak relevan tanpa memberikan definisi spesifik mengenai apa yang termasuk "tidak relevan". Ketiadaan penjelasan ini dapat menyebabkan konflik dalam implementasinya, bertentangan dengan peraturan lain yang melindungi hak publik untuk informasi dan kebebasan berbicara. Sebagai contoh, konflik potensial bisa terjadi dengan UU No. 40 Tahun 1999 tentang Pers dan UU No. 14 Tahun 2008 tentang Keterbukaan Informasi Publik. Namun, Pasal 6 ayat (3) huruf (c) UU KIP membatasi badan publik dalam memberikan informasi publik yang berkaitan dengan hak pribadi. Lebih lanjut, Pasal 17 huruf (g) dan (h) mengatur bahwa informasi pribadi seperti detil yang sangat pribadi, keinginan terakhir atau wasiat, serta rahasia pribadi tidak boleh diungkapkan, termasuk informasi tentang riwayat kesehatan fisik dan mental, kondisi finansial, pendapatan, rekening bank, serta pendidikan formal dan nonformal seseorang.

Selanjutnya, pemerintah memiliki kewajiban untuk mengelola dan menjaga keamanan data pribadi warganya sesuai dengan Undang-Undang Administrasi Kependudukan (UU No. 23/2006). Sehubungan dengan ini, Peraturan Presiden No. 67 Tahun 2011 tentang Implementasi Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan secara Nasional menguraikan tata cara lebih detail mengenai bagaimana pejabat yang berhak mengakses data tersebut dan institusi yang bertugas mengumpulkan data harus menjaga keamanan data tersebut. Kemudian, Pasal 85 Administrasi Kependudukan menetapkan bahwa negara bertanggung jawab untuk menyimpan dan melindungi data pribadi penduduk tersebut. Pasal 79 juga mencantumkan hal ini, yang mewajibkan negara untuk melindunginya dan menunjuk menteri untuk bertanggung jawab atas akses ke data pribadi penduduk. Ketika data kependudukan dikategorikan sebagai "wajib dilindungi/dirahasiakan", muncul masalah. Sangat banyak perbedaan antara UU

No. 23/2006 dan perubahannya, UU No. 24 Tahun 2013. Situasi ini terjadi karena kategorisasi data pribadi di Indonesia tidak jelas.

Namun, dalam konteks kearsipan, sangat terkait dengan proses penyelenggaraan negara, salah satunya berkaitan dengan pengoperasian sistem kearsipan oleh pemerintah. Dalam konteks ini, kearsipan tidak memasukkan data atau informasi pribadi seperti data kependudukan atau informasi tentang mahasiswa dan staf akademik. Tujuan kearsipan, seperti yang dinyatakan dalam Pasal 3 huruf (f) Nomor 43 Tahun 2009 tentang Kearsipan, adalah untuk menjaga keamanan dan keselamatan arsip sebagai bukti pertanggungjawaban dalam kehidupan berbangsa, negara, dan masyarakat. Undang-undang ini juga mengatur waktu penyimpanan data dan informasi yang berkisar antara sepuluh hingga dua puluh lima tahun. Setelah 25 tahun, arsip (data atau informasi) yang dapat dipertahankan dapat dimusnahkan atau dibuka untuk umum, dengan ketentuan bahwa tidak ada yang mengungkapkan data rahasia atau data pribadi. Berikut ini adalah beberapa kasus data pribadi di Indonesia. Yang pertama adalah kasus hilangnya tabungan Winda Earl, seorang atlet eSports Maybank Indonesia, yang sempat mengejutkan industri keuangan nasional. Kepala Cabang Maybank Cipulir telah ditetapkan sebagai tersangka karena kehilangan uang tersebut. Menurut polisi, tersangka mengambil uang Winda tanpa sepengetahuan korban. Untuk mendapatkan keuntungan, uang ditransfer ke rekening temannya. Ini menunjukkan bahwa dia tidak memperhatikan data pribadi dalam kasus ini, di mana seseorang dapat menyalahgunakan data nasabah Maybank.

Selain itu, ada kasus lain yang melibatkan Eric Priyo Prasetyo (43), seorang dokter gigi, yang kehilangan uang sebesar 400 juta rupiah karena rekening banknya dibobol setelah dia menutup nomor ponselnya, yang kemudian dibobol oleh operator ponsel. Dalam kasus-kasus tersebut, operator telepon seluler diminta untuk membayar kerugian. Beberapa contoh kasus tersebut menunjukkan bahwa perlindungan data pribadi konsumen masih lemah di Indonesia, memungkinkan orang-orang yang berwenang menyalahgunakan data konsumen. Akibatnya, perlu ada undang-undang yang melindungi peristiwa hukum yang telah diuraikan. Kasus ketiga adalah kasus Ayu (35), seorang wanita yang tinggal di Malang, yang kehilangan ratusan juta di Tabugan miliknya pada Minggu, 22 November 2020. Ayu menerima telepon dari seseorang yang mengaku dari Bank BUMN pada hari itu. Dia memberi tahu Ayu bahwa dia mendapatkan pulsa seratus ribu. Setelah diselidiki, terbukti Pulsa itu benar-benar dikirim ke nomor ponselnya. Selanjutnya, seseorang yang mengaku berasal dari bank BUMN tersebut meminta kode satu kali akses ke handphone Ayu. Setelah beberapa kali dan telepon berakhir, Ayu baru menyadari bahwa yang terjadi adalah penipuan. Tidak lama kemudian, pesan yang dikirim ke handphonenya menyatakan bahwa ada uang sebesar Rp. 49 miliar dolar dari rekeningnya. Hal ini terbukti oleh kelemahan perlindungan data pribadi saat ini.

Berdasarkan kejadian-kejadian yang telah lalu, tampak jelas bahwa terdapat kekurangan dalam melindungi data pribadi pada platform digital oleh perusahaan

swasta maupun BUMN, yang seharusnya menjaga data tersebut dengan lebih ketat. Dalam konteks ini, Peraturan Menteri Komunikasi dan Informatika Republik Indonesia No. 20 Tahun 2016 menekankan perlindungan menyeluruh atas data pribadi dalam sistem elektronik, yang mencakup semua aspek dari pengumpulan hingga pemusnahan data. Peraturan tersebut juga mengharuskan masyarakat sipil dan lembaga non-pemerintah untuk melindungi kerahasiaan data mereka sesuai dengan Pasal 26 huruf a, sementara Pasal 27 huruf a menuntut pihak bisnis untuk memelihara kerahasiaan data pengguna. Namun, aturan tersebut belum sepenuhnya mampu menghukum pelaku yang menyalahgunakan data pribadi.

Di sini terdapat ketidakpastian hukum, ketidakpastian, atau ketidakpastian. Kekosongan hukum dapat didefinisikan sebagai "keadaan kosong atau tidak adanya peraturan perundang-undangan (hukum yang mengatur tatanan (tertentu) dalam masyarakat", menurut Kamus Besar Bahasa Indonesia, "kekosongan adalah hal (keadaan, sifat, dan sebagainya) kosong atau hampa", yang diterjemahkan atau diartikan sama dengan "kosong atau hampa." Ketika hukum dapat mengatur kehidupan, hukum tidak ada. Hukum tetap tidak berfungsi ketika potensi tersebut tidak diaktifkan atau digunakan. Tidak ada hukum yang ditetapkan dan tidak dimaksudkan untuk digunakan untuk mengendalikan atau menciptakan ketertiban. Hukum yang belum ditetapkan belum memenuhi tiga tujuan hukum: keadilan, ketertiban, dan kepastian. Selain itu, tujuan hukum tersebut menjadi gaya gravitasi untuk mengikat hukum pada situasi sosial. Hukum menggunakan situasi sosial sebagai platform untuk menunjukkan betapa bermanfaatnya untuk mencapai tujuan hukum.[11]

Untuk mengisi kekosongan hukum terkait perlindungan data pribadi di ruang maya, perlu dibuat undang-undang yang efektif yang dapat memberikan perlindungan optimal bagi konsumen. Keberhasilan undang-undang tersebut dapat dinilai berdasarkan beberapa kriteria penting. Pertama, undang-undang harus memberikan deskripsi yang sangat baik tentang keadaan yang dihadapi, sehingga masalah yang ingin diselesaikan menjadi jelas. Kedua, perlu menggabungkan penilaian-penilaian ini ke dalam rangkaian hirarki, yang membantu menentukan apakah penerapan regulasi ini memberikan efek positif atau tidak lebih buruk dari masalah yang ada, layaknya konsep manfaat penggunaan obat yang harus lebih besar daripada efek sampingnya. Ketiga, verifikasi hipotesis diperlukan untuk memastikan bahwa tujuan yang diharapkan dapat tercapai, dengan menguji secara empiris efektivitas dari peraturan yang diterapkan. Keempat, pengukuran dampak dari peraturan tersebut juga perlu dilakukan untuk mengetahui sejauh mana aturan tersebut berpengaruh terhadap perlindungan data pribadi konsumen. Terakhir, identifikasi komponen yang dapat

[11] Muhammad Syukri Albani Nasution, Syukuri Albani, and others, "Hukum Dalam Pendekatan Filsafat," *Kencana, Jakarta* 63 (2016).

mengurangi efek negatif dari aturan yang diwajibkan juga penting, guna memastikan bahwa peraturan tersebut dapat diterima dan efektif dalam masyarakat, sekaligus mencapai tujuan reformasi hukum yang diinginkan.[12]

Kepastian hukum dan kemanfaatan hukum adalah tujuan hukum yang lebih realistis. Fungsionalisme mengutamakan keuntungan hukum, sedangkan positivisme menekankan kepastian hukum. Menurut teori ini, "summum ius, summa unjuria, summa lex, summa crux" berarti bahwa hukum yang keras dapat mencederakan seseorang kecuali jika keadilan dapat membantunya, sehingga meskipun keadilan bukan satu-satunya tujuan hukum, namun tujuan hukum yang paling substantif adalah keadilan.34 Sehubungan dengan teori ini, dalam hal ini telah diuraikan bahwa Peraturan Perbankan (UU No. 10/1998), antara lain, mengatur kerahasiaan bank. Berdasarkan asas kerahasiaan, bank diharuskan untuk merahasiakan semua data dan informasi mengenai nasabah, termasuk keadaan keuangan dan pribadi mereka. Rahasia bank didefinisikan dalam Pasal 1 ayat 28 UU Perbankan sebagai segala sesuatu yang berkaitan dengan data dan simpanan nasabah penyimpan. Oleh karena itu, prinsip kepercayaan dan kerahasiaan yang menjadi dasar kinerja institusi keuangan juga diterapkan pada hubungan yang terjadi antara bank dan klien mereka. Data pribadi pelanggan harus diberikan kepada bank saat mereka membeli atau menggunakan produk bank lainnya.

Dalam konteks perdagangan, sejumlah peraturan seperti UU No. 8 Tahun 1997 tentang Dokumen Perusahaan, UU No. 8 Tahun 1999 tentang Perlindungan Konsumen, dan UU No.7 Tahun 2014 tentang Perdagangan sangat penting dalam konteks perlindungan data pribadi. Hal ini dikarenakan transaksi elektronik diatur oleh UU ITE dan PP PSTE. Namun, UU Perlindungan Konsumen tidak secara eksplisit menyebutkan hak-hak konsumen yang seharusnya dilindungi oleh pelaku usaha. Undang-undang tersebut menekankan pentingnya pelaku usaha memberikan informasi yang akurat mengenai produk dan jasa mereka kepada konsumen. Sementara itu, UU Perdagangan tidak menjelaskan secara spesifik tentang perlindungan data konsumen. Akan tetapi, Pasal 65 ayat (3) dari UU tersebut menyatakan bahwa pelaku usaha dalam e-commerce harus mematuhi ketentuan UU ITE. Ini berarti bahwa aspek-aspek yang berkaitan dengan perlindungan data pribadi juga tercakup dalam transaksi elektronik. Undang-undang yang mengatur e-commerce, sebagaimana diamanatkan oleh Pasal 66 UU Perdagangan, seharusnya mencakup perlindungan data pribadi konsumen dengan merujuk pada UU ITE dan UU Perlindungan Konsumen. Di samping itu, Indonesia sedang merancang RUU Perlindungan Data Pribadi yang akan mengadopsi prinsip-prinsip dari GDPR Uni Eropa, mencakup berbagai aspek terkait data pribadi seperti jenis data, kepemilikan, pengolahan, larangan

[12] Arfi Azhari, "Legal Review of Consumer Law Protection on Personal Data on Digital Platform," *Indonesia Private Law Review* 2, no. 1 (2021): 59–72.

penggunaan, serta kerangka kerja internasional dan nasional dalam mengatasi masalah terkait data pribadi.

Data pribadi didefinisikan sebagai: "setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara individual maupun yang digabungkan dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau non-elektronik", menurut definisi yang diberikan dalam RUU ini.[13] Data pribadi terdiri dari dua kategori: data pribadi umum dan data pribadi khusus. Sayangnya, rancangan ini tidak menjelaskan secara rinci jenis data pribadi yang masuk ke dalam kualifikasi sensitif atau khusus; hanya disebutkan bahwa ini akan ditentukan oleh peraturan perundang-undangan. Prinsip yurisdiksi ekstra-teritorial akan diterapkan dalam pelaksanaan undang-undang ini. Pemindahan data dapat dilakukan baik di dalam maupun di luar wilayah hukum Indonesia, dengan ketentuan berikut: "Undang-undang ini berlaku bagi setiap orang, badan publik, pelaku usaha, dan organisasi/lembaga yang melakukan perbuatan hukum sebagaimana diatur dalam undang-undang ini, baik yang berada di dalam maupun di luar wilayah hukum Indonesia, yang mempunyai akibat hukum di dalam maupun di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia." Pengendali dan pengolah data di seluruh negara harus memastikan perlindungan data pribadi sesuai dengan peraturan perundang-undangan. Misalkan data dikirim ke luar Indonesia untuk saat ini. Dalam hal ini, pengendali data perlu mendapatkan persetujuan tertulis dari pemilik data sebelum memindahkan data tersebut kepada pihak ketiga yang berada di luar yurisdiksi Indonesia.

Selain itu, pengiriman data pribadi ke negara lain tidak diperbolehkan jika negara atau organisasi internasional tersebut tidak memiliki perlindungan data pribadi yang sebanding dengan ketentuan yang diatur dalam Undang-Undang ini. Namun, terdapat pengecualian, seperti adanya kontrak antara Pengontrol Data Pribadi dengan pihak ketiga di luar Indonesia yang berkaitan dengan perlindungan Data Pribadi atau berdasarkan perjanjian internasional.[14] Rancangan Undang-Undang ini juga menetapkan beberapa pengecualian untuk perlindungan data pribadi, antara lain untuk kepentingan keamanan dan pertahanan negara, kepentingan proses peradilan sesuai dengan ketentuan peraturan perundang-undangan, kepentingan negara dan masyarakat umum, terutama dalam bidang ekonomi atau keuangan, serta untuk menjaga etika profesional. Selain itu, diperlukan pengukuran dampak dari peraturan ini dan identifikasi komponen yang akan mengurangi efek negatif dari aturan yang diwajibkan, guna menciptakan peraturan yang efektif di masyarakat untuk mencapai tujuan reformasi hukum. Untuk data agregat yang digunakan dalam

[13] Diah Puspitasari et al., "Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Mengatasi Masalah Keamanan Data Penduduk," *Journal Of Administrative And Social Science* 4, no. 2 (2023): 195–205.
[14] Wahyudi Djafar, "Hukum Perlindungan Data Pribadi Di Indonesia: Lanskap, Urgensi Dan Kebutuhan Pembaruan," in *Seminar Hukum Dalam Era Analisis Big Data, Program Pasca Sarjana Fakultas Hukum UGM*, vol. 26, 2019.

penelitian statistik dan ilmiah, tidak dijelaskan secara rinci mengenai batasan dan prosedur pengecualian. Selain itu, tidak ada aturan teknis yang spesifik mengatur hal tersebut. Dalam hal ini, hanya disebutkan bahwa pengecualian hanya dilakukan sesuai dengan hukum atau perjanjian internasional yang berlaku dan telah disahkan.[15]

RUU tersebut tidak mengusulkan pembuatan lembaga pengawas independen untuk melindungi data pribadi. Sebaliknya, pengawasan atas perlindungan data diserahkan kepada berbagai kementerian sesuai dengan bidangnya. Data kependudukan akan diawasi oleh Kementerian Dalam Negeri, data finansial dan perbankan oleh OJK, rekam medis oleh Kementerian Kesehatan, serta data paspor dan hukum oleh Kementerian Hukum dan HAM, semuanya bekerja sama dengan Menteri Komunikasi dan Informatika.

Kesimpulan

Penelitian ini menggarisbawahi pentingnya regulasi yang lebih spesifik terkait perlindungan data pribadi di Indonesia, terutama untuk platform digital. Walaupun terdapat beberapa peraturan yang relevan seperti Peraturan Privasi No. 20 Tahun 2016, aturan tersebut dinilai masih terlalu umum dan belum mencakup perlindungan data pribadi secara mendalam. Selain itu, Peraturan Presiden No. 74 Tahun 2017 tentang Peta Jalan Sistem Perdagangan Nasional Berbasis Elektronik menunjukkan bahwa perlindungan data pribadi adalah bagian dari upaya perlindungan konsumen, namun masih membutuhkan regulasi yang lebih khusus dan rinci. Rancangan Undang-Undang Perlindungan Data Pribadi yang sedang disusun oleh pemerintah merupakan langkah krusial untuk memberikan dasar hukum yang jelas dan spesifik dalam melindungi data pribadi konsumen. Regulasi ini harus mencakup penegakan sanksi pidana bagi pelaku penyalahgunaan dan penyebaran data secara ilegal. Untuk itu, disarankan agar pemerintah mempercepat proses penyusunan undang-undang ini dengan mempertimbangkan perkembangan teknologi digital yang cepat dan memberikan perlindungan yang efektif bagi konsumen. Dengan demikian, penelitian ini berkontribusi pada pengembangan ilmu hukum dengan menyoroti kebutuhan mendesak akan regulasi yang lebih komprehensif dan adaptif terhadap dinamika teknologi.

Daftar Pustaka

Asrun, Andi Muhammad. "Hak Asasi Manusia Dalam Kerangka Negara Hukum: Catatan Perjuangan Di Mahkamah Konstitusi." *Jurnal Cita Hukum* 4, no. 1 (2016).

Azhari, Arfi. "Legal Review of Consumer Law Protection on Personal Data on

[15] Sekaring Ayumeida Kusnadi and Andy Usmina Wijaya, "Perlindungan Hukum Data Pribadi Sebagai Hak Privasi," *AL WASATH Jurnal Ilmu Hukum* 2, no. 1 (2021): 9–16.

Digital Platform." *Indonesia Private Law Review* 2, no. 1 (2021): 59–72.

Djafar, Wahyudi. "Hukum Perlindungan Data Pribadi Di Indonesia: Lanskap, Urgensi Dan Kebutuhan Pembaruan." In *Seminar Hukum Dalam Era Analisis Big Data, Program Pasca Sarjana Fakultas Hukum UGM*, Vol. 26, 2019.

Hardjaloka, Loura, and Varida Megawati Simarmata. "E-Voting: Kebutuhan vs. Kesiapan (Menyongsong) e-Demokrasi." *Jurnal Konstitusi* 8, no. 4 (2011): 579–604.

Indonesia. *Constitution of the Republic of Indonesia*. Information Division, Embassy of Indonesia, 1945.

Kodiyat, Benito Asdhie. "Fungsi Partai Politik Dalam Meningkatkan Partsipasi Pemilih Pada Pemilihan Umum Kepala Daerah Di Kota Medan." *EduTech: Jurnal Ilmu Pendidikan Dan Ilmu Sosial* 5, no. 1 (2019).

Kusnadi, Sekaring Ayumeida, and Andy Usmina Wijaya. "Perlindungan Hukum Data Pribadi Sebagai Hak Privasi." *AL WASATH Jurnal Ilmu Hukum* 2, no. 1 (2021): 9–16.

Malik, Piyush. "Governing Big Data: Principles and Practices." *IBM Journal of Research and Development* 57, no. 3/4 (2013): 1–1.

Nasution, Muhammad Syukri Albani, Syukuri Albani, and others. "Hukum Dalam Pendekatan Filsafat." *Kencana, Jakarta* 63 (2016).

Nasution, Theddy Hendrawan and others. "Perlindungan Hukum Data Pribadi Nasabah Dalam Penggunaan Big Data Oleh Perbankan Di Indonesia (Studi Komparatif Penggunaan Data Pribadi Nasabah Di Uni Eropa)," 2020.

Priscyllia, Fanny. "Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum." *Jatiswara* 34, no. 3 (2019): 239–49.

Puspitasari, Diah, Izzatusholekha Izzatusholekha, Sintia Kartini Haniandaresta, and Dalila Afif. "Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Mengatasi Masalah Keamanan Data Penduduk." *Journal Of Administrative And Social Science* 4, no. 2 (2023): 195–205.

Salim, HS. *Hukum Kontrak: Teori Dan Teknik Penyusunan Kontrak*. Bandung: Sinar Grafika, 2021.

Sinaga, Erlina Maria Christin, and Mery Christian Putri. "Formulasi Legislasi Perlindungan Data Pribadi Dalam Revolusi Industri 4.0." *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional* 9, no. 2 (2020): 237.

Yuniarti, Siti. "Perlindungan Hukum Data Pribadi Di Indonesia." *Business Economic, Communication, and Social Sciences Journal (BECOSS)* 1, no. 1 (2019): 147–54.