

PERLINDUNGAN HUKUM TERHADAP DATAPRIVASI KONSUMEN E-COMMERCE YANG MENJADI KORBAN KEJAHATAN SIBER

¹Immanuel Christian Pontorondo, ²Misael Aldo Walangitan, ³Bervie Fransel Rondonuwu
Politeknik Negeri Manado
Corresponding-mail: immanuelpontorondo@gmail.com

Copyright © 2025 The Author



This is an open access article

Under the Creative Commons Attribution Share A like 4.0 International License

DOI:10.53866/jimi.v5i2.794

Abstract

Technology has become a vital part of Indonesian business activities. Currently in Indonesia, regulations regarding e-commerce are regulated in Law Number 11 of 2008 which has been amended to Law Number 19 of 2016 concerning Electronic Information and Transactions, Law Number 7 of 2014 concerning Trade and Government Regulation Number 80 of 2019 concerning Trade through Electronic Systems. In this research, the method used is normative research method, which in its construction includes analyzing problems by managing data obtained from laws and regulations (statue approach) as the basis of research. Seeing the rapid progressiveness of technology, e-commerce transactions have become an integral part of people's lives. This progress can be seen in transaction tools that only use electronic goods through financial applications which have now become a platform for conducting trading activities. In conclusion, consumers as data subjects are also given significant legal rights. In Articles 7-13 of the Personal Data Protection Law, various data subject rights are mentioned, including the right to obtain information regarding the clarity of the identity of the party requesting the data, the right to access and correct the data, the right to erasure, and the right to withdraw consent. The exercise of these rights becomes a juridical instrument to control the use of the data.

Keywords: Protection, E-Commerce, Cyber

Abstrak

Teknologi sudah menjadi bagian yang vital dalam kegiatan bisnis masyarakat Indonesia. Saat ini di Indonesia, pengaturan mengenai e-commerce sudah diatur dalam Undang-Undang Nomor 11 Tahun 2008 yang sudah di ubah menjadi Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 7 Tahun 2014 Tentang Perdagangan dan Peraturan Pemerintah Nomor 80 Tahun 2019 Tentang Perdagangan Melalui Sistem Elektronik. Dalam penelitian ini metode yang digunakan adalah metode penelitian normatif, yang dalam konstruksinya meliputi analisis permasalahan dengan mengelola data yang diperoleh dari peraturan perundang-undangan (statue approach) sebagai landasan penelitian. Melihat progresifitas teknologi yang semakin pesat, transaksi e-commerce telah menjadi bagian integral dalam kehidupan masyarakat. Kemajuan ini terlihat dalam alat – alat transaksi yang hanya menggunakan barang elektronik melalui aplikasi keuangan yang saat ini sudah menjadi platform untuk melakukan kegiatan perdagangan. Kesimpulannya konsumen sebagai subjek data juga diberikan hak-hak hukum yang signifikan. Dalam Pasal 7–13 Undang-Undang Perlindungan Data Pribadi, disebutkan berbagai hak subjek data, antara lain hak untuk mendapatkan informasi mengenai kejelasan identitas pihak yang meminta data, hak untuk mengakses dan memperbaiki data, hak untuk menghapus data (right to erasure), hingga hak untuk menarik kembali persetujuan. Pelaksanaan hak ini menjadi instrumen yuridis untuk mengontrol penggunaan data pribadi oleh penyedia layanan e-commerce.

KataKunci: Perlindungan, E-Commerce, Siber

1. Pendahuluan

Industri perdagangan telah memasuki era disrupsi industri yang cepat melalui perkembangan teknologi yang canggih dan modern. Dalam perkembangan sejarahnya, prosedur perdagangan hanya dilakukan melalui proses tukar menukar (*barter*) antara pihak-pihak yang bertatap muka langsung untuk melakukan transaksi jual beli. Melalui barter sistem pembayaran dalam kegiatan dagang menjadi prosedur yang dilakukan secara terus menerus (Dwi Mayasari & Gde Rudy, 2021). Dengan adanya kemajuan teknologi, sistem transaksi dagang ini pun berkembang secara inovatif.

Teknologi sudah menjadi bagian yang vital dalam kegiatan bisnis masyarakat Indonesia. Dalam perkembangannya teknologi memberikan sumbangsi melalui sistem yang bekerja secara cepat, tepat dan tidak menguras biaya. Munculnya teknologi dalam setiap lini kegiatan masyarakat yang dalam hal ini kegiatan bisnis, membuat masyarakat pun harus beradaptasi mengikuti perkembangan teknologi dalam proses berbisnis (Fransisco, 2020). Di tahun 2020 dengan adanya pandemi *covid-19* membuat pemerintah mengeluarkan instruksi melalui Peraturan Pemerintah Nomor 21 Tahun 2020 tentang Wabah Penyakit Menular. Hal ini pun mempengaruhi seluruh kegiatan bisnis yang mengalami disrupsi dari kegiatan bisnis secara konvensional menjadi kegiatan bisnis yang modern.

Pemanfaatan teknologi modern saat ini menjadi pemicu untuk pertumbuhan bisnis di Indonesia, karena terbukanya ruang informasi yang sudah sangat canggih, transparan dan massive sehingga dapat dilakukan dari jarak jauh dan berdampak pada penghematan biaya (Lukito, 2017). Hal ini pun menjadi trigger positif untuk pengusaha di Indonesia yang melakukan kegiatan bisnis yang berkecimpung di bidang *e-commerce* dalam menjalankan bisnis yang lebih efektif dan efisien. Dilihat dari perkembangannya *e-commerce* pun menjadi bisnis yang menjanjikan di era modern ini. *E-commerce* juga merupakan bagian dari *e-business* yang kegiatannya dilakukan melalui modernisasi teknologi. *E-commerce* adalah segala bentuk transaksi perdagangan (bisnis) yang dalam prosesnya menggunakan media elektronik. Perkembangan *e-commerce* di Indonesia telah mengalami transformasi yang signifikan seiring dengan kemajuan teknologi informasi dan komunikasi. Namun perkembangan ini juga menimbulkan berbagai tantangan hukum yang perlu diatasi untuk menciptakan ekosistem *e-commerce* yang aman dan adil.

Merujuk pada data Asosiasi Penyelenggara Jasa Internet Indonesia jumlah pengguna internet di Indonesia tahun 2024 telah mencapai 221.563.479 jiwa dari total populasi 278.696.200 jiwa penduduk Indonesia tahun 2023. Terlihat dari hasil survei penetrasi internet Indonesia 2024 yang dirilis APJII, menyentuh angka 79,5%. Dibandingkan dengan periode sebelumnya, maka ada peningkatan sebesar 1,4%. Berdasarkan hasil survei diatas, menunjukkan bahwa aktifitas masyarakat Indonesia sudah menggunakan teknologi internet sebagai sarana kegiatan sehari-hari. Melihat euphoria masyarakat Indonesia terlebih khusus kaum muda seperti generasi milenial dan gen-z yang dalam pola gaya hidupnya cenderung bersifat konsumtif dan hedonistik, memberikan pengaruh signifikan dalam kegiatan perekonomian seperti *e-commerce*. Kegiatan tersebut di support dengan kemajuan teknologi yang canggih sehingga masyarakat Indonesia dapat mengakses, membeli dan melakukan transaksi secara cepat dimana pun dan kapan pun.

Saat ini di Indonesia, pengaturan mengenai *e-commerce* sudah diatur dalam Undang-Undang Nomor 11 Tahun 2008 yang sudah di ubah menjadi Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 7 Tahun 2014 Tentang Perdagangan dan Peraturan Pemerintah Nomor 80 Tahun 2019 Tentang Perdagangan Melalui Sistem Elektronik. Namun, pengaturan tersebut masih belum efektif untuk memberikan perlindungan hukum bagi para konsumen. Salah satu aspek penting adalah perlindungan konsumen dalam transaksi online. Meskipun *e-commerce* menawarkan kemudahan dan efisiensi dalam bertransaksi, konsumen seringkali menghadapi resiko seperti penipuan, produk yang tidak sesuai dengan deskripsi, serta kurangnya jaminan perlindungan data pribadi konsumen. Dilansir dari media Kompas, sudah ada Penipuan mengatasnamakan pihak Shopee yang digunakan untuk mengajukan pinjaman ke layanan pinjaman online SPinjam. Hal ini pun menjadi ancaman terhadap masyarakat yang telah menjadi konsumen *e-commerce*.

Dalam penelusuran yang dilakukan dalam penelitian ini, adapun penelitian terdahulu yang membahas tentang kejahatan siber dalam transaksi melalui *e-commerce*. Yang pertama ada Kevin Yoga Prestyo dengan penelitian yang berjudul Pengaruh E-Commerce Terhadap Tindak Kejahatan Siber Di Era Milenium untuk Generasi Milenial. Menurut Kevin, kejahatan penipuan *scamming* dan *phising* dapat berpengaruh pada tingkat kepercayaan konsumen yang melakukan kegiatan bisnis melalui platform

commerce (Pramita & Suganda, 2023). Selain Kevin, adapun pendapat dari hasil penelitian Marta Rustam yang mengarah pada langkah preventive pengguna platform *e-commerce*. Menurut Prasetya, konsumen juga harus memiliki sikap preventif yakni dengan tidak menyebarluaskan data pribadi ke sosial media atau platform manapun. Dengan sikap preventif tersebut, konsumen dapat meminimalisir dampak yang dilakukan oleh oknum penipuan (*scamming*) dalam kegiatan bisnis melalui platform *e-commerce* (Prasetya, 2023). Perbedaan dengan beberapa penelitian di atas, dalam penelitian ini memfokuskan pada pengaturan yang lebih progresif untuk mencegah terjadinya penipuan melalui perlindungan data pribadi melalui penguatan sumber daya dan penegakan hukum terhadap korban-korban yang terdampak dalam kejahatan *scamming* dan *phising* melalui platform *e-commerce*.

Dengan adanya kemajuan teknologi melalui platform sosial media seperti Instagram, Facebook dan Tiktok, memberikan kemudahan dalam melakukan kegiatan bisnis *e-commerce*. Akan tetapi dengan kemajuan teknologi yang signifikan, adapun permasalahan yang dihadapi oleh konsumen. Menurut data Direktorat Jenderal Perlindungan Konsumen dan Tertib Niaga (PTKN) Kementerian Perdagangan mencatat pada semester I tahun 2021 sebanyak 95 persen atau 4.855 konsumen membuat pengaduan di sektor niaga elektronik (*e-commerce*). Hal ini perlu menjadi evaluasi perihal pengaturan prosedur transaksi *e-commerce* dalam kegiatan ekonomi yang di atur dalam Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Penelitian ini bertujuan untuk mengkaji dan menganalisis tentang perlindungan dan penegakan hukum terhadap data privasi konsumen dalam transaksi elektronik melalui platform *e-commerce* untuk mendeteksi jenis penipuan berupa *scamming* dan *phising* yang dapat menimbulkan kerugian terhadap pihak-pihak yang melakukan kegiatan bisnis melalui transaksi elektronik. Pada akhirnya, penelitian ini dapat memberikan pemahaman dalam melindungi data privasi pada saat melakukan kegiatan transaksi melalui platform *e-commerce*.

2. Metode Penelitian

Dalam penelitian ini metode yang digunakan adalah metode penelitian normatif, yang dalam konstruksinya meliputi analisis permasalahan dengan mengelola data yang diperoleh dari peraturan perundang-undangan (*statue approach*) sebagai landasan penelitian. Sumber hukum yang dijadikan acuan adalah peraturan hukum yang mengatur tentang perdagangan *online* transaksi elektronik yakni Undang-Undang Nomor 11 Tahun 2008 yang sudah di ubah menjadi Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 7 Tahun 2014 Tentang Perdagangan Undang-Undang Nomor 27 Tahun 2022, dan Peraturan Pemerintah Nomor 80 Tahun 2019 Tentang Perdagangan Melalui Sistem Elektronik, perlindungan konsumen yang kegiatan bisnisnya dilakukan melalui *marketplace e-commerce* yang ada di Indonesia.

3. Hasil dan Pembahasan

3.1 Urgensi Perlindungan Hukum Terhadap Data Privasi Konsumen E-Commerce Yang Menjadi Korban Kejahatan Siber

Berdasarkan Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen adalah setiap orang pemakai barang dan/atau jasa yang tersedia dalam masyarakat, baik bagi kepentingan diri sendiri, keluarga, orang lain, maupun makhluk hidup lain dan tidak untuk diperdagangkan. Selanjutnya merujuk pada pasal 4 Undang-Undang Nomor 8 tahun 1999 Tentang Perlindungan Konsumen diuraikan hak konsumen adalah sebagai berikut :

Hak konsumen adalah:

- Hak atas kenyamanan, keamanan, dan keselamatan dalam mengkonsumsi barang dan/atau jasa;
- Hak untuk memilih barang dan/atau jasa serta mendapatkan barang dan/atau jasa tersebut sesuai dengan nilai tukar dan kondisi serta jaminan yang dijanjikan;
- Hak atas informasi yang benar, jelas, dan jujur mengenai kondisi dan jaminan barang dan/atau jasa;
- Hak untuk didengar pendapat dan keluhannya atas barang dan/atau jasa yang digunakan;
- Hak untuk mendapatkan advokasi, perlindungan, dan upaya penyelesaian sengketa perlindungan konsumen secara patut;

- f. hak untuk mendapat pembinaan dan pendidikan konsumen;
- g. hak untuk diperlakukan atau dilayani secara benar dan jujur serta tidak diskriminatif;
- h. hak untuk mendapatkan kompensasi, ganti rugi dan/atau penggantian, apabila barang dan/atau jasa yang diterima tidak sesuai dengan perjanjian atau tidak sebagaimana mestinya;
- i. hak-hak yang diatur dalam ketentuan peraturan perundang-undangan lainnya.

Melihat progresifitas teknologi yang semakin pesat, transaksi *e-commerce* telah menjadi bagian integral dalam kehidupan masyarakat. Kemajuan ini terlihat dalam alat – alat transaksi yang hanya menggunakan barang elektronik melalui aplikasi keuangan yang saat ini sudah menjadi platform untuk melakukan kegiatan perdagangan. Akan tetapi di sisi lain, perkembangan teknologi juga menghadirkan berbagai tantangan salah satunya adalah ancaman kejahatan siber terhadap data privasi konsumen. Kejahatan siber dalam transaksi *e-commerce* melibatkan berbagai modus seperti pencurian identitas, penipuan kartu kredit dan penyalahgunaan data pribadi konsumen (Widayanti, 2022) Oleh karena itu perlindungan hukum terhadap data privasi konsumen menjadi semakin mendesak.

Menurut Erna, dilihat dari dinamika perlindungan data privasi konsumen jika di analisis dengan menggunakan teori perlindungan konsumen, menegaskan bahwa negara harus hadir dalam melindungi hak-hak konsumen dari praktik bisnis yang merugikan termasuk penyalahgunaan data pribadi (Priiasari, 2023). Dalam konteks konsep hukum, perlindungan data pribadi konsumen berkaitan dengan hak atas privasi. Kewajiban penyelenggara *e-commerce* dalam menjaga keamanan data serta hak konsumen untuk mengetahui penggunaan data konsumen di fungsikan (Nainggolan, 2021). Konsep ini sejalan dengan prinsip kehati-hatian dalam pengelolaan data pribadi, yang menuntut perusahaan untuk menerapkan standar keamanan yang tinggi guna mencegah kebocoran dan penyalahgunaan data. Merujuk pada pasal 28 G Undang-Undang dasar Tahun 1945 mengatur bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan harta benda yang dibawah kekuasaannya serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan. Di dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Taun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE) Pasal 26 ayat 2 disebutkan bahwa penggunaan data pribadi melalui media elektronik harus berdasarkan persetujuan yang bersangkutan, dan kerugian yang timbul karena adanya penyalahgunaan data pribadi dapat menempuh jalur non litigasi melalui musyawarah, menempuh jalur litigasi dengan mengajukan gugatan ke pengadilan.

Data pribadi konsumen dalam transaksi *e-commerce* mencakup informasi yang sangat sensitif, seperti nama, alamat, nomor telepon dan rincian pembayaran. Jika data tersebut terekspose dan jatuh ke tangan pihak-pihak yang salah, maka konsumen yang melakukan kegiatan bisnis di platform *e-commerce* dapat mengalami kerugian finansial maupun non-finansial. Perlindungan terhadap data privasi sebagai bagian dari penghormatan atas hak privasi (*the right of privacy*) harus dimulai dengan memberikan kepastian hukum (Situmeang, 2021). Dengan meningkatnya jumlah kasus kebocoran data, urgensi penguatan regulasi hukum terkait perlindungan data pribadi harus dilakukan. Menurut Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, setiap individu memiliki hak atas keamanan data pribadinya. Pasal 4 UU No. 27 Tahun 2022 menyatakan bahwa pengendalian data wajib memastikan keamanan dan integritas data pribadi yang dikumpulkan, diproses dan. Namun dalam praktiknya, masih banyak pelaku *e-commerce* yang belum sepenuhnya mematuhi regulasi ini. Terlihat sampai saat ini menurut survey pada media diatas masih banyak kasus-kasus yang terjadi akibat kebocoran data privasi.

Melihat perkembangan teknologi yang barengi dengan tingkat kejahatan yang modern, memberikan tantangan untuk pengguna platform *e-commerce* yang ingin melakukan transaksi. Sudah banyak beberapa kasus-kasus kejahatan penipuan yang mengatasnamakan platform *e-commerce* dengan berbagai macam modus seperti memberikan hadiah fiktif, memberikan pesan resmi dari pihak perbankan dll. Kejahatan seperti ini pun dapat dilakukan karena didukung oleh beberapa faktor antara lain:

1. Kebocoran data user.

Pada bagian ini biasanya akibat dari kesalahan pengguna gawai. Penting untuk di ingat bahwa informasi pribadi tidak boleh dibagikan, termasuk SIM, nomor rekening, kode verifikasi, KTP dan informasi rahasia lainnya. Setelah data-data tersebut bocor, maka kesempatan itulah digunakan oleh oknum pelaku kejahatan siber untuk melakukan tindak kejahatan siber.

2. Faktor Pengetahuan Pengguna yang minim.

Pada umumnya era digital yang terus berkembang harus di barengi dengan kemampuan sumber daya manusia yang mumpuni. Edukasi untuk memahami resiko yang terkait dalam kejahatan siber melalui transaksi online harus terus di gaungkan dan di realisasikan. Melalui edukasi yang masif masyarakat dapat mengikuti perkembangan teknologi modern saat ini.

3. Sistem keamanan dan kebijakan pemerintah relatif melemah.

Posisi pemerintah yang kurang dalam penguatan perlindungan konsumen melalui penegakan hukum sehingga memberi peluang pada oknum pelaku kejahatan siber untuk terus melakukan tindakannya tanpa ada rasa takut terhadap sanksi hukum yang di atur dalam Undang-Undang (Laksmana, 2024).

Selain beberapa hal diatas, faktor yang menyebabkan lemahnya perlindungan hukum terhadap data privasi konsumen dalam *e-commerce* adalah rendahnya kesadaran masyarakat mengenai hak-hak yang secara hukum diberikan, lemahnya penegakan hukum serta minimnya standar keamanan yang diterapkan oleh platform digital. Selain itu, belum adanya mekanisme kompensasi yang jelas pada korban kejahatan siber yang semakin meperburuk keadaan kegiatan bisnis *e-commerce*. Melihat kelemahan tersebut perlu adanya pengaturan dalam perlindungan hukum untuk masyarakat yang melakukan transaksi melalui *e-commerce*.

Melihat juga perkembangan kebocoran data privasi yang di akibatkan oleh masyarakat yang kurang telaten dalam menggunakan gawai (*gadget*), mengharuskan adanya edukasi kepada konsumen yang bertujuan untuk memperkuat kewaspadaan dalam memberikan data pribadi secara online diplatform manapun. Konsumen harus memahami hak-hak mereka dan mengetahui langkah-langkah yang dapat dilakukan jika menjadi korban siber. Kampanye literasi digital yang melibatkan berbagai pihak, termasuk pemerintah, akademisi dan pelaku industri dapat menjadi solusi untuk meningkatkan kesadaran masyarakat.

Dalam konteks perlindungan hukum, pendekatan yang dapat dilakukan meliputi regulasi yang lebih ketat, penguatan penegakan hukum, serta peningkatan kesadaran publik terhadap pentingnya menjaga data pribadi. Peran pemerintah sangat penting dalam meningkatkan efektifitas perlindungan hukum terhadap data privasi konsumen. Pemerintah perlu mengawasi pelaku bisnis *e-commerce* agar menerapkan standar keamanan data yang tinggi serta memberikan sanksi tegas terhadap pelaku kejahatan (*scamming*) yang merugikan masyarakat. Kerja sama antara sektor publik dan swasta dalam mencegah serta menangani kejahatan siber menjadi kunci utama dalam menciptakan lingkungan digital yang lebih aman.

Perlindungan hukum terhadap data privasi konsumen dalam *e-commerce* merupakan aspek penting dan vital dalam menjaga kepercayaan publik terhadap transaksi digital. Regulasi yang lebih ketat, peningkatan kesadaran masyarakat, serta penguatan penegakan hukum adalah tiga pilar utama yang harus diperkuat guna menghadapi tantangan kejahatan siber di masa mendatang. Dengan meningkatnya ancaman terhadap data privasi konsumen, urgensi perlindungan hukum dalam ekosistem *e-commerce* tidak dapat diabaikan. Penegakan hukum yang lebih ketat, edukasi konsumen serta Kerjasama antara setiap *stakeholder* menjadi langkah utama yang harus dilakukan untuk memastikan bahwa konsumen dapat bertransaksi secara aman di dunia digital.

3.2 Pengaturan Perlindungan Hukum Terhadap Data Privasi Konsumen E-Commerce Yang Menjadi Korban Kejahatan Siber.

Pada perkembangan digital yang lebih modern, *e-commerce* telah menjadi bagian integral dari kehidupan sehari-hari. Akan tetapi, dengan meningkatnya penggunaan platform online, risiko kejahatan siber juga semakin meningkat. Data privasi konsumen seringkali menjadi target utama bagi para pelaku kejahatan siber. Oleh karena itu, perlindungan hukum terhadap data privasi konsumen menjadi sangat penting. Perlindungan hukum terhadap data privasi konsumen dalam transaksi *e-commerce* merupakan aspek yang sangat penting dalam pertumbuhan ekonomi saat ini. Terkait perlindungan hukum, menurut Isnaeni sumber perlindungan hukum terdiri dari 2 jenis yaitu perlindungan internal dan eksternal. Perlindungan hukum internal yaitu para pihak dapat diwujudkan disaat kedudukan hukum antara kedua belah pihak relatif seimbang, yang artinya para pihak memiliki *bargaining power* yang berimbang, sehingga atas dasar hak asasi manusia, para pihak mempunyai keleluasaan untuk menyatakan kehendak sesuai kepentingannya (Muzakki, 2024).

Perlindungan atas privasi mempunyai kaitan erat dengan pemenuhan atas data pribadi. Teori perlindungan data pribadi mengacu pada prinsip-prinsip yang mendasari bagaimana data individu harus dikumpulkan, disimpan, dan digunakan. Menurut Paul M. Schwartz, perlindungan data pribadi melibatkan hak individu untuk mengontrol informasi pribadi mereka dan melindungi mereka dari penyalahgunaan data oleh pihak ketiga. Hal ini penting untuk menjaga kepercayaan konsumen terhadap layanan *e-commerce*. Kejahatan siber merujuk pada tindakan kriminal yang dilakukan dengan memanfaatkan teknologi informasi dan komunikasi. Menurut definisi yang diberikan oleh *United Nations Office on Drugs and Crime* (UNODC), kejahatan siber mencakup berbagai jenis aktivitas ilegal yang dilakukan melalui internet, termasuk pencurian identitas dan pelanggaran data. Pasal 26 ayat (1) UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah diubah dengan UU No. 19 Tahun 2016 menyebutkan bahwa penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan. Asas hukum yang mengatur perlindungan data pribadi dapat ditemukan dalam berbagai regulasi, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia. UU ini memberikan kerangka hukum untuk melindungi data pribadi dari penyalahgunaan dan menetapkan sanksi bagi pelanggar (Aruan, 2024). Berdasarkan Pasal 1 angka 29 Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik menacntumkan bahwa data pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau di kombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau nonelektronik.

Merujuk dalam Pasal 84 Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan atas Undang-Undang No. 23 Tahun 2006 tentang Administrasi Kependudukan, mengatur mengenai data pribadi penduduk yang harus dilindungi yaitu :

- (a) Keterangan tentang cacat fisik dan/atau mental;
- (b) Sidik jari;
- (c) Iris mata;
- (d) Tandatangan; dan
- (e) Elemen data lainnya yang merupakan aib seseorang.

Perlindungan Data Pribadi Konsumen Dalam Transaksi Elektronik juga diatur di dalam Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik yakni :

1. Defenisi data pribadi
Peraturan Kominfo 20/2016 mengelaborasi mengenai pengertian data pribadi. Data pribadi diartikan sebagai segala informasi mengenai individu yang dapat diidentifikasi secara langsung atau tidak langsung, baik sendiri atau dengan menghubungkannya dengan informasi lain. Definisi ini mencakup segala jenis informasi, termasuk nama, alamat, nomor telepon, alamat email, nomor identitas, riwayat transaksi, dan informasi lain yang berhubungan dengan individu
2. Hak Pribadi atas Data Pribadi.
Peraturan Kominfo 20/2016 mengakui hak pribadi individu atas data pribadi mereka. Konsumen mempunyai hak untuk mengetahui, mengakses, mengoreksi, menghapus, membatasi penggunaan, dan memindahkan data pribadi mereka yang dikelola oleh pihak lain. Konsumen juga berhak untuk mengajukan keluhan atau protes jika data pribadi mereka digunakan secara tidak sah atau melanggar ketentuan peraturan ini.
3. Kewajiban Pengelola Data Pribadi.
Peraturan Kominfo 20/2016 menetapkan kewajiban bagi pengelola data pribadi, yaitu pihak yang mengumpulkan, mengolah, menyimpan, dan mengelola data pribadi. Pengelola data pribadi harus mengikuti prinsip keadilan, transparansi, keterbatasan tujuan, ketepatan, kemanfaatan, akurasi, keamanan, dan tanggung jawab dalam mengelola data pribadi konsumen.
4. Persyaratan Penyimpanan dan Penggunaan Data Pribadi.
Peraturan Kominfo 20/2016 menetapkan persyaratan tentang penyimpanan dan penggunaan data pribadi. Data pribadi harus disimpan dalam batas waktu yang wajar sesuai dengan tujuan pengumpulan data tersebut. Pengelola data pribadi juga harus memastikan keamanan data pribadi dari akses, penggunaan, dan pengungkapan yang tidak sah.

5. Notifikasi Pelanggaran data

Peraturan Kominfo 20/2016 mewajibkan pengelola data pribadi untuk memberikan notifikasi kepada konsumen jika terjadi pelanggaran keamanan yang mengakibatkan akses, penggunaan, atau pengungkapan data pribadi yang tidak sah. Notifikasi tersebut harus dilakukan sesegera mungkin agar konsumen dapat mengambil langkah-langkah untuk melindungi diri mereka dari potensi penyalahgunaan data.

6. Penggunaan Data Pribadi Untuk Pemasaran

Peraturan Kominfo 20/2016 mengatur tentang penggunaan data pribadi untuk kepentingan pemasaran. Pengelola data pribadi harus mendapatkan izin atau persetujuan dari konsumen sebelum menggunakan data pribadi untuk tujuan pemasaran, kecuali jika ada ketentuan hukum yang mengizinkan penggunaan data pribadi tanpa izin.

7. Pengalihan Data Pribadi

Peraturan Kominfo 20/2016 mengatur tentang pengalihan data pribadi ke pihak ketiga. Pengalihan data pribadi ke pihak ketiga hanya dapat dilakukan dengan persetujuan tertulis dari konsumen, kecuali jika ada ketentuan hukum atau peraturan yang mengizinkan pengalihan data pribadi.

8. Penghapusan data pribadi

Peraturan Kominfo 20/2016 menetapkan kewajiban untuk menghapus data pribadi konsumen jika tujuan pengumpulan data tersebut telah tercapai atau data pribadi tidak diperlukan lagi untuk tujuan yang sah. Penghapusan data pribadi harus dilakukan secara aman dan terjamin.

Dalam perkembangan *ecommerce* yang pesat, perlindungan hukum terhadap data privasi konsumen menjadi aspek krusial yang harus diperhatikan. Pengaturan hukum yang jelas dan tegas diperlukan untuk mencegah dan menangani pelanggaran data pribadi yang dapat merugikan konsumen. Diberbagai negara, regulasi perlindungan data privasi telah dikembangkan untuk mengatasi ancaman kejahatan siber yang semakin kompleks (Priliasari, 2023). Indonesia sendiri telah mengadopsi Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (UU PDP) sebagai bentuk perlindungan hukum bagi masyarakat. Dalam perspetif hukum, pengaturan perlindungan data privasi konsumen di Indonesia masih menghadapi berbagai tantangan, terutama dalam implementasi dan penegakan hukum. UU Perlindungan Data Pribadi mengatur tentang hak-hak individu terkait data pribadinya serta kewajiban pengendali dan pemroses data dalam menjaga kerahasiaan informasi yang dikumpulkan. Akan tetapi, efektifitas penerapan regulasi ini masih dipengaruhi oleh kesiapan infrastruktur hukum dan teknologi di Indonesia. Secara konsep hukum, perlindungan data privasi konsumen dalam *e-commerce* berkaitan dengan hak konstitusional individu terhadap privasi sebagaimana tercantum dalam Pasal 28G ayat (1) Undang-Undang Dasar 1945. Hal ini pun juga di perkuat dalam Pasal 26 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang menyatakan bahwa penggunaan data pribadi harus mendapatkan persetujuan dari pemiliknya. Oleh karena itu, aspek regulasi harus memastikan bahwa konsumen memiliki kendali atas data pribadinya dan dapat menuntut jika terjadi penyalahgunaan.

Melihat perspektif perbandingan hukum, beberapa negara telah menunjukkan progresifitas yang mumpuni dalam perlindungan data pribadi. Seperti Uni Eropa yang melalui *General Data Protection Regulation* (GDPR) yang memberikan standar ketat terhadap perlindungan data individu. *General Data Protection Regulation* (GDPR) adalah regulasi perlindungan data yang berlaku di Uni Eropa sejak 25 Mei 2018. Regulasi ini bertujuan untuk melindungi data pribadi individu dalam ruang lingkup Uni Eropa dan memperketat pengelolaan data oleh perusahaan yang beroperasi di wilayah tersebut atau menangani data warga Uni Eropa. Meskipun GDPR merupakan regulasi yang dibuat oleh Uni Eropa, pengaruhnya meluas ke negara lain termasuk Indonesia, mengingat banyaknya interaksi bisnis global yang melibatkan pengolahan data lintas batas. Penerapan prinsip GDPR di Indonesia menjadi relevan seiring dengan berkembangnya regulasi perlindungan data pribadi dalam negeri. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) pun dijadikan sebagai pilar utama perlindungan hukum untuk data pribadi di Indonesia. Dalam konteks ini, terdapat beberapa prinsip GDPR yang di adopsi dalam UU PDP, seperti transparansi, akuntabilitas dan hak individu atas data pribadi. Selain itu GDPR menekankan pentingnya keamanan data dan mitigasi resiko kebocoran informasi. Perusahaan yang tidak mematuhi regulasi ini dapat dikenai sanksi yang signifikan, dengan denda hingga 4% dari total pendapatan tahunan.

global atau sekitar 20 juta euro, tergantung mana yang lebih besar. GDPR mengharuskan perusahaan untuk memastikan tingkat keamanan tinggi dalam penyimpanan dan pengolahan data pribadi, serta memberikan hak kepada konsumen untuk menghapus data mereka jika tidak lagi diperlukan (Sirait, 2019)

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) hadir sebagai *lex specialis* dalam perlindungan hukum terhadap data pribadi. UU ini memberikan definisi yang tegas mengenai data pribadi dan menetapkan kewajiban bagi pengendali data untuk menjaga kerahasiaan, integritas, dan ketersediaan data pribadi. Penyelenggara sistem elektronik sebagai pengendali data memiliki tanggung jawab hukum untuk mencegah kebocoran atau penyalahgunaan data. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan tonggak penting dalam sistem hukum Indonesia, karena memberikan dasar hukum yang komprehensif terhadap perlindungan data pribadi. UU ini hadir sebagai bentuk respons negara atas meningkatnya ancaman terhadap privasi individu, khususnya dalam ekosistem digital seperti *e-commerce*, yang rentan terhadap penyalahgunaan data pribadi oleh pelaku usaha maupun pihak ketiga yang tidak sah. UU PDP secara eksplisit mendefinisikan data pribadi sebagai "setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau non-elektronik." Definisi ini mencakup data umum seperti nama, alamat, nomor telepon dan juga data spesifik seperti informasi keuangan, biometrik, hingga riwayat transaksi online.

Dalam konteks *e-commerce*, data pribadi konsumen biasanya dikumpulkan melalui akun pengguna, transaksi pembelian, sistem pembayaran, dan pelacakan perilaku konsumen. Proses ini menuntut pelaku usaha untuk menaati prinsip-prinsip pengolahan data sebagaimana diatur dalam UU PDP, termasuk prinsip *lawfulness, fairness, purpose limitation, data minimization, dan integrity & confidentiality*. Artinya, setiap pemrosesan data harus sah, terbuka, proporsional, dan aman. Substansi UU PDP mengatur kewajiban pelaku usaha (sebagai pengendali data) untuk memperoleh persetujuan eksplisit dari subjek data sebelum memproses datanya. Persetujuan ini tidak boleh bersifat implisit, tersembunyi dalam syarat penggunaan, atau dipaksakan melalui ketentuan yang tidak seimbang. Pasal 20 UU PDP menegaskan bahwa persetujuan harus diberikan secara sadar, spesifik, dan berdasarkan informasi yang cukup kepada pemilik data.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi tonggak penting dalam sistem hukum nasional karena secara khusus memberikan landasan hukum terhadap hak-hak subjek data pribadi, termasuk konsumen *e-commerce*. UU ini hadir sebagai bentuk perlindungan negara atas hak konstitusional setiap warga negara terhadap data pribadinya, sebagaimana diamanatkan dalam Pasal 28G ayat (1) UUD 1945. Dalam lingkup perdagangan digital, konsumen sering kali menjadi pihak yang rentan terhadap pelanggaran data akibat lemahnya sistem keamanan digital pelaku usaha. Dalam Pasal 1 angka 1 UU PDP, data pribadi didefinisikan sebagai "setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau non-elektronik." Ini mencakup berbagai jenis informasi konsumen, seperti nama, alamat, nomor telepon, nomor identitas, data keuangan, hingga preferensi belanja. Luasnya cakupan ini menunjukkan bahwa setiap informasi yang dikumpulkan dalam platform *e-commerce* sangat mungkin masuk dalam kategori data pribadi yang harus dilindungi.

Undang-Undang Perlindungan Data Pribadi telah menetapkan prinsip-prinsip pemrosesan data pribadi dalam Pasal 3, yaitu data pribadi harus diperoleh secara terbatas dan spesifik, sah secara hukum, transparan, untuk tujuan tertentu, dan tidak bertentangan dengan ketentuan peraturan perundang-undangan. Selain itu dalam Pasal 4, diatur bahwa pemrosesan data pribadi wajib dilakukan berdasarkan persetujuan dari subjek data, kecuali dalam keadaan tertentu yang dikecualikan oleh Undang-Undang. Ketentuan mengenai persetujuan dijelaskan lebih lanjut dalam Pasal 20 ayat (1) yang menyatakan bahwa "Pemrosesan Data Pribadi hanya dapat dilakukan berdasarkan persetujuan yang sah dari Pemilik Data Pribadi," dan ayat (2) menyatakan bahwa persetujuan tersebut harus diberikan secara eksplisit dan dapat dibuktikan. Dalam praktik *e-commerce*, ini menegaskan bahwa pelaku usaha wajib memperoleh persetujuan yang tegas dari konsumen sebelum mengumpulkan atau memproses data pribadinya.

Konsumen sebagai subjek data juga diberikan hak-hak hukum yang signifikan. Dalam Pasal 7–13 Undang-Undang Perlindungan Data Pribadi, disebutkan berbagai hak subjek data, antara lain hak untuk mendapatkan informasi mengenai kejelasan identitas pihak yang meminta data, hak untuk mengakses dan

memperbaiki data, hak untuk menghapus data (*right to erasure*), hingga hak untuk menarik kembali persetujuan. Pelaksanaan hak ini menjadi instrumen yuridis untuk mengontrol penggunaan data pribadi oleh penyedia layanan *e-commerce*. Kewajiban pengendali data untuk menjamin keamanan data ditegaskan dalam Pasal 35, yang berbunyi: “Pengendali Data Pribadi wajib mencegah Data Pribadi agar tidak diakses secara tidak sah dan tidak diproses secara tidak sah atau melawan hukum.” Hal ini menuntut pelaku usaha untuk memiliki sistem keamanan data yang memadai. ketika terjadi pelanggaran atau kelalaian, maka pengendali data dapat dimintai pertanggungjawaban hukum. Pada saat terjadi pelanggaran data pribadi, Pasal 39 ayat (1) mewajibkan pengendali data untuk “memberitahukan secara tertulis kepada Pemilik Data Pribadi paling lambat 3 x 24 (tiga kali dua puluh empat) jam setelah diketahui terjadi kegagalan perlindungan Data Pribadi.” Pemberitahuan ini harus mencakup setidaknya penyebab kegagalan, data yang terkena dampak, dan upaya penanganannya sebagaimana diatur dalam Pasal 39 ayat (2).

Untuk penegakan hukum, Pasal 57 sampai dengan Pasal 58 mengatur sanksi administratif yang dapat dikenakan kepada pengendali atau prosesor data yang melanggar ketentuan UU PDP, antara lain teguran tertulis, penghentian sementara aktivitas pengolahan data, hingga denda administratif maksimal 2% dari pendapatan tahunan. Sedangkan Pasal 67 ayat (1) mengatur bahwa setiap orang yang dengan sengaja dan melawan hukum memperoleh atau mengungkapkan Data Pribadi yang bukan miliknya dipidana penjara paling lama 4 tahun dan/atau denda paling banyak Rp 4.000.000.000. UU PDP juga memperkenalkan lembaga pengawas independen yang diatur dalam Pasal 58, yakni Otoritas Pelindungan Data Pribadi. Lembaga ini memiliki kewenangan strategis dalam melakukan pengawasan, pemantauan kepatuhan, pemeriksaan, serta memberikan sanksi administratif kepada pelaku pelanggaran. Kehadiran otoritas ini merupakan bentuk konkret tanggung jawab negara dalam menjamin pemenuhan hak-hak subjektif data secara terukur dan dapat dipertanggungjawabkan. Dengan demikian, substansi UU PDP secara eksplisit dan sistematis telah mengatur perlindungan hukum terhadap data pribadi konsumen, termasuk dalam ranah *e-commerce* yang rentan terhadap kejahatan siber. Melalui kombinasi prinsip, kewajiban, hak, sanksi, dan lembaga pengawas, undang-undang ini menghadirkan mekanisme preventif sekaligus represif yang menjadi kerangka dasar perlindungan hukum berbasis hak privasi dan keamanan informasi digital di Indonesia.

4. Kesimpulan

Urgensi perlindungan hukum terhadap data privasi konsumen dalam *e-commerce* merupakan aspek krusial dalam menjaga kepercayaan publik terhadap transaksi digital. Regulasi yang lebih ketat, peningkatan kesadaran masyarakat, serta penguatan penegakan hukum adalah tiga pilar utama yang harus diperkuat guna menghadapi tantangan kejahatan siber di masa mendatang. Perlindungan hukum terhadap data privasi konsumen dalam *e-commerce* merupakan aspek penting dan vital dalam menjaga kepercayaan publik terhadap transaksi digital. Regulasi yang lebih ketat, peningkatan kesadaran masyarakat, serta penguatan penegakan hukum adalah tiga pilar utama yang harus diperkuat guna menghadapi tantangan kejahatan siber di masa mendatang. Dengan meningkatnya ancaman terhadap data privasi konsumen, urgensi perlindungan hukum dalam ekosistem *e-commerce* tidak dapat diabaikan. Penegakan hukum yang lebih ketat, edukasi konsumen serta kerja sama antara setiap *stakeholder* menjadi langkah utama yang harus dilakukan untuk memastikan bahwa konsumen dapat bertransaksi secara aman di dunia digital.

Konsumen sebagai subjek data juga diberikan hak-hak hukum yang signifikan. Dalam Pasal 7–13 Undang-Undang Perlindungan Data Pribadi, disebutkan berbagai hak subjek data, antara lain hak untuk mendapatkan informasi mengenai kejelasan identitas pihak yang meminta data, hak untuk mengakses dan memperbaiki data, hak untuk menghapus data (*right to erasure*), hingga hak untuk menarik kembali persetujuan. Pelaksanaan hak ini menjadi instrument yuridis untuk mengontrol penggunaan data pribadi oleh penyedia layanan *e-commerce*. Kewajiban pengendali data untuk menjamin keamanan data ditegaskan dalam Pasal 35, yang berbunyi: “Pengendali Data Pribadi wajib mencegah Data Pribadi agar tidak diakses secara tidak sah dan tidak diproses secara tidak sah atau melawan hukum.” Hal ini menuntut pelaku usaha untuk memiliki sistem keamanan data yang memadai. Jika terjadi pelanggaran atau kelalaian, maka pengendali data dapat dimintai pertanggungjawaban hukum. Jika terjadi pelanggaran data pribadi, Pasal 39 ayat (1) mewajibkan pengendali data untuk “memberitahukan secara tertulis kepada Pemilik Data Pribadi paling lambat 3 x 24 (tiga kali dua puluh empat) jam setelah diketahui terjadi kegagalan perlindungan Data

Pribadi.” Pemberitahuan ini harus mencakup setidaknya penyebab kegagalan, data yang terkena dampak, dan upaya penanganannya sebagaimana diatur dalam Pasal 39 ayat (2).

Bibliografi

- Aruan, J. E. S. (2024). PERLINDUNGAN DATA PRIBADI DITINJAU DARI TEORI PERLINDUNGAN HUKUM DAN TEORI PERLINDUNGAN HAK ATAS PRIVASI. *Jurnal Globalisasi Hukum*, 1(1), 1–22. <https://doi.org/10.25105/jgh.v1i1.19499>
- Dwi Mayasari, I. D.A., & Gde Rudy, D. (2021). Urgensi Rekonstruksi Pengaturan Praktek Perjanjian Perdagangan Melalui E-Commerce. *Jurnal Komunikasi Hukum (JKH)*, 7(1), 235. <https://doi.org/10.23887/jkh.v7i1.31473>
- Fransisco, W. (2020). Interaktif Masyarakat Terhadap Hukum Dalam Kehidupan Normal Baru Pasca COVID-19. *Journal of Judicial Review*, 22(2), 151. <https://doi.org/10.37253/jjr.v22i2.1483>
- Laksana, A. (2024). Analisis Perlindungan Hukum Konsumen Terhadap Praktik Pembulatan Harga BBM Di SPBU: Perspektif UU Perlindungan Konsumen. *Sekolah Tinggi Ilmu Hukum IBLAM*.
- Lukito, I. (2017). Tantangan Hukum dan Peran Pemerintah Dalam Pembangunan E-Commerce. *Pusat Pengkajian Dan Pengembangan Kebijakan Badan Penelitian Dan Pengembangan Hukum Dan HAM Kementerian Hukum Dan HAM R.I*, 11(3), 349–367.
- Muzakki, A. S. (2024). Analisis Perlindungan Hukum bagi Konsumen dan Pelaku Usaha dari Anomali Perdagangan Online dalam Era Digitalisasi. UNS (Sebelas Maret University).
- Nainggolan, I. (2021). Perlindungan Hukum Bagi Pelaku Usaha E-Commerce Ditinjau Dari Hukum Positif Indonesia. *Prosiding Seminar Nasional Kewirausahaan*, 2(1), 1060–1067.
- Pramita, R., & Suganda, M.A. (2023). Aspek Hukum Perlindungan Konsumen Dalam Praktik Bisnis Penawaran Online: Studi Kasus Pada Platform E-Commerce. *Innovative: Journal Of Social Science Research*, 3(6), 8753–8765.
- Prasetya, A. P. (2023). *Perlindungan Hukum Terhadap Konsumen yang Membeli Obat-obatan Palsu Melalui Transaksi Jual Beli Online*. Universitas Islam Indonesia.
- Prihasari, E. (2023). Perlindungan Data Pribadi Konsumen Dalam Transaksi E-Commerce. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, 12(2).
- Sirait, Y. H. (2019). GENERAL DATA PROTECTION REGULATION (GDPR) DAN KEDAULATAN NEGARA NON-UNIEROPA. *Gorontalo Law Review*, 2(2), 60. <https://doi.org/10.32662/golrev.v2i2.704>
- Situmeang, S. M. T. (2021). PENYALAHGUNAAN DATA PRIBADI SEBAGAI BENTUK KEJAHATAN SEMPURNA DALAM PERSPEKTIF HUKUM SIBER. *SASI*, 27(1), 38. <https://doi.org/10.47268/sasi.v27i1.394>
- Widayanti, P.W. (2022). TINDAK PIDANA PENCURIAN DATA NASABAH DALAM BIDANG PERBANKAN SEBAGAI CYBER CRIME. *Legacy: Jurnal Hukum Dan Perundang-Undangan*, 2(2), 1–21. <https://doi.org/10.21274/legacy.2022.2.2.1-21>