Vol. 22 No. 1 Mei 2026 : 78-99
pISSN : 1907 - 8188
eISSN : 2797 - 4170
YUSTITIA
FAKULTAS HUKUM
UNIVERSITAS NGURAH RAI

PERLINDUNGAN HUKUM TERHADAP DATA PRIBADI KONSUMEN DALAM *E-COMMERCE*: PERSPEKTIF KONSTITUSIONALISME DIGITAL

I Made Sugita[1], I Made Sudharma[2]
[1,2] Prodi Hukum Hindu, Universitas Hindu Negeri I Gusti Bagus Sugriwa Denpasar
(imadesugita@uhnsugriwa.ac.id)

ABSTRAK

Proses registrasi data pribadi ke dalam sistem elektronik menyebabkan tingkat penggunaan layanan digital, termasuk *e-commerce*, semakin meningkat. Namun, kondisi ini sekaligus memperbesar kerentanan terjadinya kebocoran data pribadi konsumen pada *e-commerce* dan kemudian disalahgunakan oleh pihak yang tidak bertanggungjawab. Data pribadi dan hak privasi merupakan hak konstitusional yang harus dijamin dan dilindungi oleh negara seperti amanat Pasal 28G Ayat (1) Undang-Undang Dasar 1945, karena merupakan bagian integral dari hak asasi manusia yang harus dilindungi dalam penggunaan *platform* digital termasuk dalam transaksi *e-commerce.* Tujuan penelitian ini adalah untuk mengkaji terkait dengan perlindungan hukum terhadap data pribadi dalam *e-commerce* ditinjau dari perspektif konstitusionalisme digital dan kedua, terkait dengan tanggungjawab *marketplace* terhadap pelanggaran pengelolaan data pribadi konsumen dalam *e-commerce*. Metode penelitian yang digunakan dalam penelitian ini adalah penelitian hukum normatif, yang mengacu pada doktrin dan teori serta peraturan perundang-undangan serta penelitian sebelumnya yang relevan dengan masalah yang dihadapi. Hasil penelitian menunjukkan bahwa perlindungan data pribadi di berbagai regulasi telah mengatur perlindungan hukum terhadap data pribadi baik perlindungan hukum secara preventif maupun perlindungan hukum secara represif. Perlindungan secara preventif seperti persetujuan penggunaan data, perlindungan teknis pengamanan data serta dibentuknya otoritas pengawas independen pengedali data. Sementara perlindungan secara reperesif yaitu telah diaturnya mekanisme pengajuan keberatan, pengaduan dan tuntutan ganti rugi oleh konsumen yang merasa dirugikan dalam *e-commerce*. *Marketplace* memiliki tanggungjawab hukum atas kegagalan sistem pengamanan atau kelalaian data pribadi yang menggunakan layanannya. Apabila *marketplace* tidak melaksanakan kewajibannya, maka dapat dikenakan sanksi administratif berupa teguran, denda, penghentian sementara kegiatan, hingga sanksi pidana jika terbukti mengakibatkan kerugian.

Kata Kunci: Perlindungan Hukum, Data Pribadi, *E-Commerce*

pISSN : 1907 - 8188
eISSN : 2797 - 4170

ABSTRACT

The process of registering personal data into electronic systems has led to an increase in the use of digital services, including e-commerce. However, this situation also increases the vulnerability of consumers' personal data leaks in e-commerce and subsequent misuse by irresponsible parties. Personal data and the right to privacy are constitutional rights that must be guaranteed and protected by the state, as mandated by Article 28G Paragraph (1) of the 1945 Constitution, as they are an integral part of human rights that must be protected in the use of digital platforms, including e-commerce transactions. The purpose of this study is to examine the legal protection of personal data in e-commerce from the perspective of digital constitutionalism and, second, to examine the responsibility of marketplaces for violations of consumer personal data management in e-commerce. The research method used in this study is normative legal research, which refers to doctrines and theories, laws and regulations, and previous research relevant to the problem at hand. The results show that various regulations governing personal data protection include both preventive and repressive legal protection. Preventive protection includes data usage consent, technical data security safeguards, and the establishment of an independent data supervisory authority. Meanwhile, repressive protection includes mechanisms for filing objections, complaints, and claims for compensation by consumers who feel disadvantaged in e-commerce. Marketplaces are legally responsible for any security system failures or negligence in the personal data of those using their services. If a marketplace fails to fulfill its obligations, it may be subject to administrative sanctions in the form of warnings, fines, temporary suspension of activities, and even criminal sanctions if proven to have caused harm.

Keywords: Legal Protection, Personal Data, and E-Commerce

I. PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi dan informasi yang begitu pesat membuat dunia seolah-olah tanpa batas yang memungkinkan setiap orang atau warga negara dapat terhubung secara langsung dengan warga negara lain secara langsung dan cepat. Persebaran informasi tersebut yang didukung oleh sarana dan prasarana komunikasi membuat komunikasi antarwarga negara semakin luas. Semakin berkembangnya aplikasi sosial media seperti instagram, tiktok, facebook, telegram dan lain sebagainya semakin membuat konektivitas sesama antarwarga negara menjadi semakin pesat. Hal tersebut juga terjadi di dalam bidang perekonomian, dimana transformasi digital yang terjadi membuat transaksi dalam jual-beli barang dan jasa menjadi semakin mudah. Berbagai macam flatform digital yang bergerak dalam kegiatan jual beli barang dan jasa secara elektronik atau disebut dengan *e-commerce* diantaranya shopee, tokopedia, bukalapak dan lain sebagainya yang tentunya banyak

dimanfaatkan oleh masyarakat dalam jual beli barang dan jasa yang mereka butuhkan. Pemanfaatan sosial media tersebut berpengaruh juga terhadap penegakan hak-hak konstitusional warga negara terutama yang berkaitan dengan hak-hak yang harus dijamin dan dilindungi oleh negara agar akses ke lembaga penegak hukum menjadi semakin mudah dan transparan.[1]

Transformasi digital sangat berkaitan erat dengan konstitusionalisme.
Konstitusionalisme merupakan sebuah sistem yang didalamnya mengatur hubungan antara pemerintah dengan warga negara serta menjamin hak-hak warga negara tersebut agar terlindungi. [2] Di Indonesia, konstitusionalisme ini dapat dilihat dari ketentuan-ketentuan yang terdapat pada peraturan perundang-undangan yang muaranya berada pada ketentuan-ketentuan yang terdapat pada Undang-Undang Dasar 1945 (UUD 1945). UUD 1945 dijadikan sebagai hukum tertinggi di Indonesia yang didalamnya mengatur segala macam sendi-sendi kehidupan yang ada di Indonesia, mulai dari pengakuan terhadap hak asasi manusia, sistem pemerintahan hingga pengaturan terhadap hak-hak warga negara serta pengaturan segala bentuk kekuasaan yang ada di Indonesia yang selalu harus berlandaskan pada aturan hukum dan konstitusi negara. Jika dikaitkan di era digital saat ini, maka konstitusionalisme merupakan sebuah konsep yang menekankan perlunya mengikuti prinsip-prinsip konstitusionalisme untuk mengatur hubungan antara pemerintah dengan warga negara dalam konteks digital. Hal ini termasuk dalam menjamin dan melindungi data pribadi warga negara, hak cipta serta hak yang lainnya serta memastikan bahwa pemerintah serta warga negara dalam menggunakan teknologi digital agar menghormati hak-hak konstitusional. Selain itu, di era digital saat ini, tidak hanya pemerintah dan warga negara yang menjadi aktornya, namun campur tangan pihak swasta juga turut menjadi aktor yang berperan sangat strategis, terutama penyediaan pltaform media sosial yang berbasis digital seperti platform *e-commerce*.

Sebagai negara hukum, Indonesia berkewajiban melindungi dan menjamin terpenuhinya hak-hak dasar warga negara, termasuk hak atas privasi dan perlindungan data pribadi. Hal ini tercermin dalam Pasal 28G ayat (1) UUD 1945, yang menegaskan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda. Pasal tersebut menegaskan mengenai hak fundamental setiap individu untuk mendapatkan perlindungan dan rasa aman dari berbagai macam ancaman yang dapat menganggu kehidupan pribadinya,

[1] Nanang Subekti, I Gusti Ayu Ketut Rahmi Handayani, and Arief Hidayat, "Konstitusionalisme Digital Di Indonesia," *Peradaban Journal of Law and Society* 2, no. 1 (2023): 1–22, https://doi.org/10.59001/pjls.v2i1.74.

[2] Muhammad Rahmat Agus, "Konstitusinalisme Pelayanan Publik Di Era Digital Di Negara Republik Indonesia," 2023, https://osf.io/x7mep/download.

keluarga, kehormatan serta harta bendanya. Ketentuan ini jika dikaitkan dengan perlindungan data pribadi mengandung makna bahwa privasi atau data pribadi sebagai bagian integral dari hak asasi manusia yang harus dilindungi dalam penggunaan platform digital termasuk dalam transaksi *e-commerce*. Selain itu, secara khusus terkait dengan perlindungan data pribadi juga telah diatur di dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi atau sering disingkat dengan UU PDP. UU ini mengatur hak dan kewajiban berbagai pihak, baik pengelola data pribadi (*data controller*) maupun pengguna data pribadi (*data processor*), untuk memastikan data konsumen diproses secara sah, transparan, dan bertanggung jawab. Dalam konteks *e-commerce*, UU PDP melindungi informasi pribadi konsumen, seperti nama, alamat, nomor telepon, dan informasi pembayaran, dari penyalahgunaan, pencurian, atau kebocoran data. UU ini juga mewajibkan pelaku usaha *e-commerce* untuk memperoleh persetujuan eksplisit dari konsumen sebelum mengumpulkan atau menggunakan data mereka, serta memberikan hak kepada konsumen untuk mengakses, memperbaiki, dan menghapus data pribadinya. Selain itu, UU PDP menetapkan sanksi administratif dan pidana bagi pelanggaran perlindungan data, sehingga memberikan landasan hukum yang kuat untuk meningkatkan kepercayaan konsumen dalam transaksi elektronik.

Saat ini, *e-commerce* telah menjadi bagian yang tidak terpisahkan dalam era digital yang tumbuh dengan pesat serta mendominasi pasar global.[3] Selain itu, *e-commerce* telah memberikan banyak kesempatan bagi pelaku bisnis kecil (UMKM) dan menengah untuk menawarkan barang atau jasa mereka melalui platform digital yang tersedia. Perdagangan elektronik (*e-commerce*) menawarkan beragam keuntungan, antara lain akses yang lebih mudah, proses yang cepat, penghematan biaya, serta peluang menjangkau pasar internasional. Kehadirannya telah membawa perubahan besar dalam praktik bisnis maupun pola konsumsi masyarakat. Berkat kemajuan teknologi digital, *e-commerce* menjadi salah satu sektor ekonomi yang tumbuh pesat.[4]

Akibat hal tersebut pada akhirnya menyebabkan banyak masyarakat Indonesia kini mendaftarkan data pribadinya untuk menjadi anggota sekaligus pelanggan pada platform *e-*

[3] Erna Priliasari, "PERLINDUNGAN DATA PRIBADI KONSUMEN DALAM TRANSAKSI E-COMMERCE MENURUT PERATURAN PERUNDANG-UNDANGAN DI INDONESIA (Legal Protection of Consumer Personal Data in E-Commerce According To Laws Dan Regulations in Indonesia)," *Jurnal Rechts Vinding* 12, no. 2 (2023): 261–79.

[4] Tia Deja Pohan and Muhammad Irwan Padli Nasution, "Perlindungan Hukum Data Pribadi Konsumen Dalam Platform E Commerce," *Sammajiva: Jurnal Penelitian Bisnis Dan Manajemen* 1, no. 3 (2023): 42–48, https://doi.org/10.47861/sammajiva.v1i3.336.

pISSN : 1907 - 8188
eISSN : 2797 - 4170

commerce tertentu. Hal ini karena setiap calon pengguna diwajibkan mengisi formulir yang tersedia di laman web dengan mencantumkan informasi pribadi dasar. Tidak hanya *e-commerce*, berbagai layanan digital lainnya seperti dompet elektronik, aplikasi pertemanan, hingga aplikasi transportasi juga mensyaratkan pendaftaran data pribadi. Setiap kategori sistem elektronik maupun perusahaan digital memiliki kewenangan untuk mengakses informasi pengguna tersebut.

Proses registrasi data pribadi ke dalam sistem elektronik menyebabkan tingkat penggunaan layanan digital, termasuk *e-commerce*, semakin meningkat. Namun, kondisi ini sekaligus memperbesar kerentanan keamanan siber yang rawan disalahgunakan pihak tak bertanggung jawab. Tidak heran jika kerap terdengar kasus kebocoran data. Sebagai contoh, pada Mei 2020 tercatat sepuluh perusahaan digital mengalami insiden kebocoran data dengan total lebih dari 73 juta akun terdampak, salah satunya platform *e-commerce* Bhinneka.com.[5] Selian itu, Dilansir dari CNN Indonesia pada bulan April 2020, muncul beberapa kasus *cybercrime* di Indonesia, seperti terjadinya pembocoran data pribadi yang dilakukan oleh *hacker* untuk meretas sistem keamanan PSE dan mengambil sejumlah data pribadi yang bersifat konfidensial bagi seseorang. Salah satu contoh kasusnya yaitu ditemukan bahwa data pribadi dari sekitar 13 juta akun pengguna Bukalapak telah dijual di forum gelap daring. Informasi pribadi yang bocor meliputi nama lengkap, alamat email, nomor telepon, dan alamat pengiriman. Meskipun kata sandi akun tidak bocor dalam kasus ini, tetapi potensi penyalahgunaan data pribadi tersebut masih menjadi ancaman serius bagi para pengguna. Insiden ini menimbulkan kekhawatiran tentang keamanan data dan privasi konsumen di e-*commerce* di Indonesia. Bukalapak mengambil langkah cepat untuk memberikan peringatan kepada pengguna dan menyatakan bahwa mereka telah memperkuat keamanan sistem mereka. Kasus tersebut menunjukkan betapa pentingnya bagi perusahaan *e-commerce* di Indonesia untuk selalu meningkatkan keamanan dan perlindungan data konsumen.

Kebocoran data pribadi konsumen dalam *e-commerce* dapat memberikan dampak yang sangat merugikan bagi korban. Dampak yang paling jelas adalah hilangnya privasi, di mana informasi pribadi seperti nama, alamat, nomor telepon, hingga data keuangan dapat disalahgunakan oleh pihak yang tidak bertanggung jawab. Hal ini berpotensi menimbulkan kerugian finansial, misalnya melalui penipuan atau pencurian identitas yang dapat menyebabkan kerugian materi. Selain itu, kebocoran data juga dapat merusak reputasi korban, karena data pribadi yang bocor dapat digunakan

[5] Deanne Destriani Firmansyah Putri and Muhammad Helmi Fahrozi, "Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan Ruu Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.Com)," *Borneo Law Review* 5, no. 1 (2021): 46–68, https://doi.org/10.35334/bolrev.v5i1.2014.

pISSN : 1907 - 8188
eISSN : 2797 - 4170

untuk tujuan negatif atau dipublikasikan tanpa izin. Korban juga berisiko menjadi sasaran serangan siber lebih lanjut, seperti *phishing* atau penipuan *online*, yang semakin kompleks dan sulit dideteksi.

Permasalahan kebocoran data pribadi perlu mendapatkan perhatian serius serta penyelesaian yang jelas, mengingat perkembangan teknologi dan internet terus berlangsung sementara potensi tindak kejahatan juga tidak pernah hilang. Oleh karena itu, masyarakat membutuhkan jaminan perlindungan demi terciptanya rasa aman dan nyaman dalam memanfaatkan teknologi maupun internet. Peningkatan kualitas sistem keamanan pada layanan elektronik pun menjadi hal yang sangat penting. Harapannya dengan hal tersebut, konsumen atau masyarakat memperoleh perlindungan dan terpenuhinya hak-hak masyarakat terutama dalam berinternet dan bertransaksi khususnya *e-commerce* sebagaimana yang telah digariskan oleh peraturan perundang-undangan maupun konstitusi negara.

B. Metode Penelitian

Penelitian ini menggunakan metode penelitian hukum normatif, yang meliputi analisis terhadap teori dan doktrin hukum, kerangka konseptual, dan peraturan perundang-undangan yang sesuai atau relevan. Pendekatan yang digunakan yaitu pendekatan peraturan perundang-undangan. Pendekatan ini untuk memberikan penjelasan menyeluruh tentang masalah hukum yang telah dibahas melalui analisis peraturan perundang-undangan, konsep serta teori hukum. Sifat penelitian ini yaitu deskriptif analitis. Sifat penelitian ini tidak hanya mengkaji aturan hukum tertulis, tetapi juga menganalisis berbagai prinsip-prinsip dan kaidah-kaidah hukum yang berlaku sebagai dasar dalam merumuskan solusi terhadap permasalahan hukum tersebut secara menyeluruh dan sistematis yang kemudian dideskripsikan secara kualitatif.

II. Hasil dan Pembahasan

A. Perlindungan Hukum Terhadap Data Pribadi Dalam *E-Commerce* Ditinjau Dari Perspektif Konstitusionalisme Digital

Konstitusionalisme digital muncul sebagai jawaban atas perubahan yang dipicu oleh perkembangan teknologi informasi. Ruang digital bukan sekadar ranah teknis, tetapi juga merupakan arena politik dan hukum yang wajib berlandaskan prinsip demokrasi serta hak asasi manusia. Di Indonesia, konstitusionalisme digital bertujuan memperluas cakupan konstitusi sehingga mampu mengatur isu-isu seperti perlindungan data pribadi, kebebasan berpendapat, dan keamanan di dunia maya. Fokus utamanya adalah memastikan bahwa asas negara hukum tetap menjadi fondasi dalam

pISSN : 1907 - 8188
eISSN : 2797 - 4170

membangun peradaban baru manusia.[6]

Dalam konsep negara hukum, perlindungan hukum sangat dibutuhkan dalam melindungi hak-hak masyarakat dari ancaman maupun penyalahgunaan kewenangan. Menurut Setiono perlindungan hukum adalah tindakan atau upaya untuk melindungi masyarakat dari tindakan-tindakan yang tidak sesuai dengan aturan hukum dalam rangka mewujudkan ketertiban dan ketentraman sehingga memungkinkan manusia untuk menikmati hak-hak nya dengan baik.[7] Dengan demikian, perlindungan hukum dapat diartikan dengan segala upaya pemerintah untuk menjamin adanya kepastian hukum untuk memberi perlindungan kepada warga negaranya agar hak-haknya sebagai seorang warga negara tidak dilanggar, dan bagi yang melanggarnya akan dapat dikenakan sanksi sesuai peraturan yang berlaku.[8]

Pasal 28G Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 merupakan salah satu dasar konstitusional perlindungan hak asasi manusia, termasuk hak atas perlindungan data pribadi. Secara khusus, Pasal 28G ayat (1) berbunyi:

> "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi."

Meskipun hak atas privasi tidak disebutkan secara ekspilsit dalam ketentuan di atas, namun di dalam ketentuan tersebut telah memasukkan nilai-nilai privasi dalam perjanjian HAM Internasional. Selaras dengan hal tersebut, bahwa dalam Pasal 12 Deklarasi Universal Hak Asasi Manusia (DUHAM) atau Universal Declaration of Human Rights (UDHR) yang menyatakan bahwa "Tidak seorangpun boleh diganggu urusan pribadinya, keluarganya, rumah tangganya atau hubungan surat menyuratnya dengan sewenang-wenan, juga tidak diperkenankan melakukan pelanggaran atas kehormatan dan nama baiknya".[9]

Ketentuan ini menegaskan bahwa setiap warga negara memiliki hak konstitusional atas perlindungan diri pribadi, termasuk hak atas data pribadi yang

[6] Eka Wahyu Hidayat, "STUDI LITERATUR KONSTITUSIONALISME DIGITAL DI ERA E-" 24, no. May (2025).

[7] Setiono, *Supremasi Hukum* (Surakarta: UNS,2004), h.23.

[8] Hadjon, P.M, *Perlindungan Hukum Bagi Rakyat Indonesia* (Surabaya: PT. Bina Ilmu,1987), h.19.

[9] Nela mardiana Parihin, "U The Urgensi URGENSI PERLINDUNGAN DATA PRIBADI DALAM PRESPEKTIF HAK ASASI MANUSIA," *Jurnal Rechten : Riset Hukum Dan Hak Asasi Manusia* 5, no. 1 (2023): 16–23, https://doi.org/10.52005/rechten.v5i1.108.

pISSN : 1907 - 8188
eISSN : 2797 - 4170

merupakan bagian dari identitas dan integritas individu. Dalam konteks *e-commerce*, data pribadi konsumen seperti nama, alamat, nomor telepon, riwayat transaksi, hingga informasi rekening bank merupakan bagian dari diri pribadi yang dilindungi oleh konstitusi. Dengan demikian, perlindungan data pribadi bukan sekadar isu teknis atau administratif, melainkan merupakan hak asasi manusia yang dijamin UUD 1945. Oleh karena itu, penting bagi pemerintah dan pelaku *e-commerce* untuk meningkatkan kesadaran dan pemahaman tentang pentingnya perlindungan data pribadi.[10]

Di Indonesia, Undang-Undang Perlindungan Konsumen (UU No. 8 Tahun 1999) dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) (UU No. 19 Tahun 2016) merupakan dua kerangka hukum utama yang memiliki peran signifikan dalam melindungi konsumen dan mengatur transaksi elektronik, terutama menghadapi tantangan baru dalam era digital yang melibatkan isu privasi dan keamanan data. Undang-Undang Perlindungan Konsumen menegaskan hak konsumen untuk mendapatkan informasi yang jujur dan benar tentang barang/jasa, termasuk dalam transaksi digital, serta memberikan hak privasi dalam pengumpulan, penggunaan, dan pengolahan informasi pribadi oleh penyedia barang/jasa. Selain itu, mengakui transaksi elektronik, UU Perlindungan Konsumen mengatur hak-hak konsumen dalam konteks ini, termasuk memberikan informasi yang jelas dan komprehensif tentang transaksi elektronik, termasuk kebijakan privasi yang diterapkan oleh penyedia layanan.[11]

Selain itu, di Indonesia urgensi perlindungan terhadap data pribadi semakin disadari sehingga melahirkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Undang-undang ini mengatur hak-hak subjek data serta kewajiban pengendali dan pemroses data, termasuk sanksi administratif dan pidana bagi pihak yang melanggar. Dalam Pasal 58 UU PDP ditegaskan bahwa setiap orang dilarang secara melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya untuk mendapatkan keuntungan atau menimbulkan kerugian bagi subjek data. Hal ini menunjukkan bahwa negara berupaya menjamin keamanan data pribadi sebagai bagian dari perlindungan hukum di era digital.

[10] Rachel Milafebina, Idham Putra Lesmana, and Moody Rizqy Syailendra, "Perlindungan Data Pribadi Terhadap Kebocoran Data Pelanggan E-Commerence Di Indonesia," *Jurnal Tana Man* 4, no. 1 (2023): 158–69, https://ojs.staialfurqan.ac.id/jtm/.

[11] I Wayan Cenik Ardika, "Tinjauan Hukum Terhadap Perlindungan Data Pribadi Di Era Digital: Kasus Kebocoran Data Pengguna Layanan E-Commerce," *Indonesian Journal of Law and Justice* 2, no. 3 (2025): 11, https://doi.org/10.47134/ijlj.v2i3.3601.

pISSN : 1907 - 8188
eISSN : 2797 - 4170

Dengan demikian, pentingnya data pribadi dalam era digital tidak hanya terletak pada fungsinya dalam mendukung efisiensi dan kenyamanan teknologi, tetapi juga pada perlindungan yang harus diberikan oleh negara, pelaku usaha, dan masyarakat sendiri agar data tersebut tidak menjadi alat penyalahgunaan yang merugikan. Perlindungan hukum terhadap data pribadi dalam era digital sangatlah penting untuk memastikan data pribadi diproses dengan cara yang sah dan bertanggung jawab.[12]

Pengesahan UU PDP ini memberikan kerangka kerja yang khusus dan komprehensif dalam penanganan serta perlindungan data pribadi di Indonesia. Dalam menghadapi dinamika dan tantangan yang semakin berkembang seputar isu data pribadi, regulasi ini diharapkan dapat memperkuat kesiapan negara dalam melindungi data pribadi warganya. Selain itu, UU ini juga dirancang untuk memberikan jaminan rasa aman kepada individu terhadap data pribadi mereka. Lebih lanjut, regulasi ini memiliki peran penting dalam menjerat pelaku penyalahgunaan data pribadi dengan sanksi yang tegas, sehingga memberikan dasar hukum yang kokoh untuk menjaga integritas dan keamanan data pribadi.[13]

Perlindungan hukum terhadap data pribadi dalam *e-commerce* harus dilaksanakan secara preventif dan represif. Perlindungan hukum preventif bertujuan untuk mencegah terjadinya permasalahan-permasalahan yang berkaitan dengan penyalahgunaan data pribadi. Sementara perlindungan hukum represif bertujuan untuk menyelesaikan permasalahan atau sengketa yang timbul serta memberikan kesempatan kepada masyarakat yang merasa dirugikan hak-hak nya untuk mengajukan keberatan terhadap penyalahgunaan data pribadi dalam *e-commerce.*[14]

Terkait perlindungan hukum preventif, dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memuat beberapa ketentuan yang bersifat preventif dalam rangka melindungi data pribadi. Pasal 28 Ayat (1) mengatur bahwa setiap pengendali data wajib memiliki dasar hukum dan tujuan yang jelas dalam memproses data pribadi. Ketentuan ini mencerminkan pembatasan

[12] Jurnal Penelitian and Jenda Ingan Mahuli, "All Fields of Science J-LAS Perlindungan Hukum Terhadap Data Pribadi Dalam Era Digital Legal Protection of Personal Data in the Digital Era," *AFoSJ-LAS* 3, no. 4 (2023): 188–94, https://j-las.lemkomindo.org/index.php/AFoSJ-LAS/index.

[13] Hari Sutra Disemadi et al., "Perlindungan Data Pribadi Di Era Digital: Mengapa Kita Perlu Peduli?," *Sang Sewagati Journal* 1 (2), no. 2 (2023): 67–90, http://journal.uib.ac.id/index.php/sasenal/index.

[14] Zennia Almaida, "Perlindungan Hukum Preventif Dan Refresif Bagi Pengguna Uang Elektronik Dalam Menggunakan Transaksi Tol Nontunai," *Privat Law* 9 (2021): 222–23.

pISSN : 1907 - 8188
eISSN : 2797 - 4170

tujuan (*purpose limitation*) yang sangat penting dalam konteks *e-commerce* , di mana data konsumen tidak boleh digunakan untuk kepentingan lain selain transaksi yang disetujui. Perlindungan terhadap penyalahgunaan data lebih lanjut juga ditegaskan dalam Pasal 30, yang mewajibkan pengendali data untuk memperoleh persetujuan eksplisit dari subjek data sebelum memproses data pribadi. Persetujuan ini harus diberikan secara sadar dan tidak disamarkan melalui syarat dan ketentuan yang kabur, sehingga mendorong transparansi dan pemberdayaan konsumen.

Upaya preventif juga tampak dalam kewajiban teknis pengamanan data, pengendali data wajib melakukan perlindungan teknis dan organisasi untuk mencegah akses ilegal, pengungkapan, pengubahan, atau perusakan data pribadi. Hal ini mendorong pelaku usaha untuk mengimplementasikan sistem keamanan siber seperti *firewall*, enkripsi data, serta pengendalian akses berbasis otorisasi. Ketentuan ini juga diperkuat oleh Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE), khususnya Pasal 21 ayat (1), yang mewajibkan PSE untuk menjaga keutuhan, keautentikan, kerahasiaan, dan ketersediaan data pribadi yang dikelola dalam sistem elektronik mereka.

Dalam aspek kelembagaan, upaya preventif diwujudkan melalui pembentukan otoritas pengawas independen yang diamanatkan dalam Pasal 58 UU PDP. Lembaga ini bertanggung jawab mengawasi kepatuhan para pengendali data dan memberikan rekomendasi atau tindakan administratif apabila terjadi potensi pelanggaran. Keberadaan lembaga ini memungkinkan dilakukannya pengawasan proaktif terhadap implementasi perlindungan data pribadi, tanpa menunggu laporan atau pengaduan dari masyarakat. Pengawasan yang bersifat aktif dan sistematis ini menjadi bagian penting dalam menciptakan ekosistem digital yang aman, khususnya dalam sektor *e-commerce* yang melibatkan jutaan data konsumen setiap harinya.

Selain pendekatan regulatif, pemerintah juga mengembangkan upaya preventif melalui edukasi dan literasi digital kepada masyarakat. Kementerian Komunikasi dan Informatika (Kominfo) secara konsisten menyelenggarakan program literasi digital yang mencakup kesadaran tentang pentingnya menjaga data pribadi, cara mengenali aplikasi yang berisiko, dan pemahaman terhadap kebijakan privasi digital. Strategi ini berperan dalam membentuk konsumen yang lebih sadar dan kritis terhadap hak-haknya dalam dunia digital. Dengan demikian, upaya perlindungan tidak hanya dibebankan kepada pelaku usaha

pISSN : 1907 - 8188
eISSN : 2797 - 4170

dan regulator, tetapi juga melibatkan peran aktif masyarakat sebagai pemilik data.

Upaya preventif pemerintah juga tidak terlepas dari kerja sama internasional. Sebagai bagian dari ekosistem global, Indonesia terlibat dalam pembentukan *ASEAN Framework on Personal Data Protection* yang bertujuan menyelaraskan standar pelindungan data antarnegara anggota. Kerja sama ini penting mengingat banyak platform *e-commerce* yang berkedudukan di luar negeri namun tetap memproses data konsumen Indonesia. Dalam pendekatan normatif, harmonisasi hukum internasional menjadi bentuk upaya preventif yang dapat memperluas jangkauan yurisdiksi negara terhadap praktik pemrosesan data lintas batas. Hal ini sejalan dengan Pasal 55 UU PDP yang mengatur bahwa pengiriman data pribadi ke luar negeri hanya dapat dilakukan kepada negara yang memiliki tingkat perlindungan setara atau lebih tinggi dibanding Indonesia. Selain UU PDP, pemerintah juga menerbitkan berbagai regulasi teknis yang memperkuat upaya perlindungan data secara preventif. Salah satunya adalah Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE).

PP PSTE merupakan regulasi teknis yang memiliki peran penting dalam upaya pemerintah memberikan perlindungan preventif terhadap data pribadi konsumen, khususnya dalam sektor *e-commerce* . PP ini menjadi pelengkap dari UU ITE dan kini juga saling melengkapi dengan UU PDP, dalam hal penguatan infrastruktur perlindungan data. Salah satu bentuk upaya preventif dalam PP PSTE tercermin dalam Pasal 14 ayat (1), yang mewajibkan setiap Penyelenggara Sistem Elektronik (PSE) untuk menyelenggarakan sistem elektronik secara andal, aman, dan bertanggung jawab. Kata “aman” dalam konteks ini menjadi dasar hukum bahwa PSE memiliki kewajiban untuk membangun sistem yang mampu mencegah risiko kebocoran atau penyalahgunaan data pribadi. Upaya preventif ini dimulai sejak tahap perencanaan atau pengembangan sistem, dikenal dengan prinsip *privacy by design*, di mana perlindungan data bukan sekadar fitur tambahan, tetapi menjadi bagian inheren dari struktur sistem.

Dalam upaya melindungi data pribadi konsumen, pemerintah menetapkan kewajiban teknis bagi setiap pelaku usaha di bidang *e-commerce* untuk mengimplementasikan sistem pengamanan yang andal dan komprehensif. Sistem ini harus mampu melindungi data dari berbagai potensi gangguan, baik yang berasal dari dalam maupun luar sistem, melalui penerapan teknologi seperti enkripsi, *firewall*, serta sistem deteksi dan pencegahan intrusi (*IDS/IPS*). Lebih dari

pISSN : 1907 - 8188
eISSN : 2797 - 4170

sekadar memasang sistem pengamanan, pelaku usaha juga dituntut untuk memperbarui sistem tersebut secara berkala. Pendekatan ini dikenal sebagai *security by maintenance*, yang mencerminkan bahwa perlindungan terhadap data pribadi bersifat dinamis dan harus selalu responsif terhadap perkembangan ancaman siber.

Pendekatan ini sejalan dengan teori perlindungan hukum dalam upaya preventif pemerintah, di mana negara berperan aktif dalam mencegah pelanggaran hak-hak individu sebelum terjadi kerugian. Pemerintah mendorong pelaku usaha untuk melakukan audit keamanan secara rutin serta memantau potensi kerentanan yang ada dalam sistem mereka. Langkah ini tidak hanya bertujuan melindungi konsumen dari akses ilegal oleh pihak ketiga, tetapi juga menjadi bagian dari tanggung jawab hukum pelaku usaha untuk memastikan bahwa data pribadi konsumen dikelola dengan aman. Dengan sistem pengamanan yang adaptif dan berbasis evaluasi berkelanjutan, potensi risiko dapat ditekan sedini mungkin sebelum berkembang menjadi pelanggaran nyata.

PP PSTE merupakan regulasi teknis yang memiliki peran penting dalam upaya pemerintah memberikan perlindungan preventif terhadap data pribadi konsumen, khususnya dalam sektor *e-commerce* . PP ini menjadi pelengkap dari UU ITE dan kini juga saling melengkapi dengan UU PDP, dalam hal penguatan infrastruktur perlindungan data. Salah satu bentuk upaya preventif dalam PP PSTE tercermin dalam Pasal 14 ayat (1), yang mewajibkan setiap Penyelenggara Sistem Elektronik (PSE) untuk menyelenggarakan sistem elektronik secara andal, aman, dan bertanggung jawab. Kata “aman” dalam konteks ini menjadi dasar hukum bahwa PSE memiliki kewajiban untuk membangun sistem yang mampu mencegah risiko kebocoran atau penyalahgunaan data pribadi. Upaya preventif ini dimulai sejak tahap perencanaan atau pengembangan sistem, dikenal dengan prinsip *privacy by design*, di mana perlindungan data bukan sekadar fitur tambahan, tetapi menjadi bagian inheren dari struktur sistem.

Dalam upaya melindungi data pribadi konsumen, pemerintah menetapkan kewajiban teknis bagi setiap pelaku usaha di bidang *e-commerce* untuk mengimplementasikan sistem pengamanan yang andal dan komprehensif. Sistem ini harus mampu melindungi data dari berbagai potensi gangguan, baik yang berasal dari dalam maupun luar sistem, melalui penerapan teknologi seperti enkripsi, *firewall*, serta sistem deteksi dan pencegahan intrusi (*IDS/IPS*). Lebih dari sekadar memasang sistem pengamanan, pelaku usaha juga

pISSN : 1907 - 8188
eISSN : 2797 - 4170

dituntut untuk memperbarui sistem tersebut secara berkala. Pendekatan ini dikenal sebagai *security by maintenance*, yang mencerminkan bahwa perlindungan terhadap data pribadi bersifat dinamis dan harus selalu responsif terhadap perkembangan ancaman siber.

Pendekatan ini sejalan dengan teori perlindungan hukum dalam upaya preventif pemerintah, di mana negara berperan aktif dalam mencegah pelanggaran hak-hak individu sebelum terjadi kerugian. Pemerintah mendorong pelaku usaha untuk melakukan audit keamanan secara rutin serta memantau potensi kerentanan yang ada dalam sistem mereka. Langkah ini tidak hanya bertujuan melindungi konsumen dari akses ilegal oleh pihak ketiga, tetapi juga menjadi bagian dari tanggung jawab hukum pelaku usaha untuk memastikan bahwa data pribadi konsumen dikelola dengan aman. Dengan sistem pengamanan yang adaptif dan berbasis evaluasi berkelanjutan, potensi risiko dapat ditekan sedini mungkin sebelum berkembang menjadi pelanggaran nyata.

Pelaku usaha yang melanggar ketentuan dapat dikenai sanksi administratif berupa peringatan tertulis, penghentian sementara kegiatan, pemblokiran sistem elektronik, pencantuman dalam daftar hitam, hingga pencabutan izin, seperti yang tercantum dalam pasal 80 PP PMSE. Penerapan sanksi secara bertahap ini mencerminkan prinsip kehati-hatian dari pemerintah sebagai bentuk upaya preventif. Tujuannya adalah memberi ruang bagi pelaku usaha untuk melakukan perbaikan secara internal sebelum dijatuhi sanksi yang lebih berat. Dalam konteks perlindungan data pribadi, peringatan tertulis menjadi sarana penting untuk mendorong pelaku usaha segera memperbaiki sistem keamanan data yang rentan, sehingga potensi pelanggaran terhadap hak konsumen dapat dicegah sejak dini. Sanksi administratif hanya dapat dijatuhkan setelah melalui proses pemeriksaan administratif oleh instansi berwenang. Mekanisme ini memperlihatkan adanya upaya pengawasan yang bersifat preventif, karena bertujuan mengevaluasi secara objektif pelanggaran yang dilakukan oleh pelaku usaha sebelum diterapkan sanksi yang lebih berat. Pemeriksaan administratif ini juga dapat berfungsi sebagai sarana edukatif bagi pelaku usaha agar lebih memahami pentingnya perlindungan data pribadi dan menyesuaikan kebijakan serta sistem yang mereka kelola sesuai dengan regulasi yang berlaku. Berdasarkan uraian tersebut di atas, bahwa tanggungjawab pemerintah harus memastikan data-data pribadi masyarakat terlindungi dari hal-hal negatif sekaligus juga memberikan sanksi bagi pihak-pihak yang menyalahgunakan data pribadi yang dimiliki oleh masyarakat. Pemerintah harus berubah untuk

pISSN : 1907 - 8188
eISSN : 2797 - 4170

bertindak sebagai penjamin hak, bukan hanya sebagai regulator.[15]

Selain perlindungan hukum preventif, perlindungan hukum represif juga telah diatur dalam berbagai regulasi terkait perlindungan data pribadi di Indonesia. Upaya represif sangat penting ketika upaya preventif gagal mencegah pelanggaran. Bentuk upaya ini harus mampu memberikan rasa keadilan dan pemulihan hak secara konkret kepada pihak yang dirugikan. Oleh karena itu, pengaturan tentang tanggung jawab hukum, mekanisme penyelesaian sengketa, hingga pemberian sanksi administratif maupun pidana merupakan bagian penting dari upaya perlindungan hukum represif.

Dalam konteks kebocoran data pribadi konsumen pada transaksi *e-commerce* , upaya represif tercermin dalam berbagai instrumen hukum yang memberikan hak kepada subjek data untuk mengajukan keberatan, pengaduan, dan tuntutan ganti rugi terhadap pihak *marketplace* atau penyelenggara sistem elektronik yang lalai atau menyalahgunakan data. Berdasarkan Pasal 58 sampai dengan Pasal 65 UU PDP, konsumen dapat mengajukan pengaduan kepada otoritas pengawas dan menuntut kompensasi atas kerugian yang dialami.

Setiap individu yang datanya dikelola oleh pihak lain memiliki hak untuk mengajukan pengaduan apabila terjadi perlakuan yang tidak sesuai dengan ketentuan hukum, seperti yang tercantum dalam pasal 58 dan 59. Hak ini bersifat represif, karena memberikan mekanisme hukum langsung bagi konsumen untuk melaporkan pelanggaran yang mereka alami. Dalam *e-commerce* , apabila terjadi penyalahgunaan data oleh pelaku usaha misalnya kebocoran, pemanfaatan tanpa izin, atau penjualan data kepada pihak ketiga konsumen memiliki dasar hukum yang kuat untuk melaporkan tindakan tersebut kepada otoritas pengawas yang berwenang dalam pelindungan data pribadi.

Lebih lanjut, mekanisme pengaduan kini telah disesuaikan dengan perkembangan teknologi, memungkinkan konsumen menyampaikan laporan secara tertulis maupun melalui media elektronik. Kemudahan akses ini menjadi bentuk upaya pemerintah yang adaptif terhadap kebutuhan masyarakat digital, di mana mobilitas tinggi dan keterbatasan waktu seringkali menjadi hambatan dalam mencari keadilan. Dalam hal ini, keberadaan *e-government* memainkan peran penting sebagai fasilitator utama dalam penyediaan layanan pengaduan digital yang terintegrasi dan responsif. Melalui platform daring resmi milik

[15] Zurayya Fadila Rahla Azura, Zelly Dia Rofinda , Selfi Renita Rusjdi , Husni , Liganda Endo Mahata, "Jurnal Riset Ilmiah," *Jurnal Riset Ilmiah* 1, no. 01 (2022): 15–18, https://manggalajournal.org/index.php/SINERGI/article/view/1218/1479.

pISSN : 1907 - 8188
eISSN : 2797 - 4170

pemerintah, seperti situs pengaduan atau aplikasi pelayanan publik, konsumen dapat dengan mudah melaporkan pelanggaran tanpa harus hadir secara fisik di kantor instansi terkait.

Dengan prosedur pengaduan yang dapat dilakukan secara daring melalui *e-government*, konsumen tidak hanya mendapatkan akses hukum yang lebih efisien, tetapi juga peluang untuk memperoleh penanganan yang lebih cepat atas pelanggaran terhadap hak-hak mereka. Sistem ini mencerminkan modernisasi dalam perlindungan hukum, di mana negara hadir secara aktif dan inovatif dalam menjamin hak-hak warganya di tengah era digital. Lebih dari sekadar sarana teknis, *e-government* memperkuat posisi konsumen sebagai subjek hukum yang benar-benar dilindungi secara aktif, bahkan setelah pelanggaran terjadi, karena proses penegakan hukum tidak lagi dibatasi oleh ruang dan waktu.

Dalam sistem perlindungan data pribadi, peran otoritas pengawas sangat penting dalam menindaklanjuti setiap laporan atau pengaduan dari masyarakat. Otoritas ini tidak hanya bersifat pasif menunggu laporan, tetapi memiliki kewenangan aktif untuk memeriksa setiap pengaduan yang masuk. Proses pemeriksaan ini mencakup permintaan data, dokumen, maupun keterangan dari pihak-pihak yang diduga melakukan pelanggaran. Pendekatan investigatif ini menunjukkan bahwa negara tidak membiarkan pelanggaran terhadap data pribadi berjalan tanpa kontrol, melainkan bertindak sebagai pelindung hak-hak konsumen melalui fungsi pengawasan yang kuat.

Setelah proses pemeriksaan dilakukan, otoritas pengawas memiliki kewenangan untuk memberikan teguran, peringatan tertulis, maupun rekomendasi kepada pelaku usaha atau pengendali data agar segera melakukan perbaikan. Jika tidak diindahkan, tindakan ini dapat dilanjutkan dengan pemberian sanksi administratif. Langkah ini mencerminkan mekanisme korektif upaya represif, yaitu langkah yang dilakukan setelah terjadi pelanggaran untuk mengembalikan situasi seperti sediakala sekaligus memberi efek jera kepada pihak pelanggar. Dalam konteks *e-commerce* , langkah ini penting untuk menjaga kepercayaan konsumen terhadap sistem digital yang digunakan.

Selain sanksi administratif, sistem perlindungan hukum juga memberikan hak bagi konsumen sebagai pemilik data untuk menuntut ganti rugi apabila mengalami kerugian akibat pelanggaran data pribadi. Kerugian tersebut bisa berupa kerugian materiil, seperti kehilangan aset keuangan, maupun immateriil, seperti kerugian atas privasi atau reputasi. Bentuk kompensasi ini menjadi bukti nyata bahwa hukum memberikan perlindungan tidak hanya melalui pencegahan dan sanksi, tetapi juga melalui

pISSN : 1907 - 8188
eISSN : 2797 - 4170

pemulihan hak bagi pihak yang dirugikan. Konsumen berhak menempuh berbagai jalur penyelesaian untuk mendapatkan keadilan atas pelanggaran tersebut.

Untuk memperkuat perlindungan hukum bagi konsumen, sistem peradilan juga membuka ruang bagi gugatan perdata. Jika pelanggaran terhadap data pribadi mengakibatkan kerugian yang signifikan, konsumen dapat mengajukan gugatan ke pengadilan guna menuntut tanggung jawab hukum dari pihak pelanggar. Jalur ini memberikan kepastian hukum yang lebih kuat karena dilandasi oleh proses yudisial, termasuk pembuktian dan putusan pengadilan yang bersifat mengikat. Dengan demikian, konsumen tidak hanya bergantung pada tindakan administratif, tetapi juga memiliki jalur litigasi sebagai bentuk upaya represif pemerintah yang lebih formal dan tegas.

Di sisi lain, konsumen juga diberikan pilihan penyelesaian sengketa melalui mekanisme non-litigasi, seperti mediasi atau arbitrase, yang difasilitasi oleh lembaga yang berwenang. Jalur ini memberikan alternatif penyelesaian yang lebih cepat dan efisien, terutama bagi konsumen yang ingin menghindari proses peradilan yang panjang dan rumit. Meskipun bersifat damai, mekanisme ini tetap berada dalam kerangka upaya perlindungan hukum represif karena bertujuan untuk memulihkan hak-hak konsumen yang dilanggar. Fleksibilitas dalam penyelesaian sengketa ini menunjukkan bahwa perlindungan hukum terhadap data pribadi mencakup berbagai jalur yang dapat diakses sesuai kebutuhan dan kondisi korban. Selain itu, Pasal 26 ayat (2) UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE) juga memberikan dasar hukum bagi korban untuk menggugat pelaku secara perdata apabila penggunaan data pribadi dilakukan tanpa izin. Dalam hal ini, *marketplace* sebagai pengendali data dapat dimintai tanggung jawab secara hukum apabila terbukti lalai atau melanggar kewajiban pengamanan data.

PP No. 71 Tahun 2019 merupakan regulasi yang memperkuat upaya pemerintah dalam mengatur sistem dan transaksi elektronik, termasuk aspek keamanan data pribadi. Ketentuan dalam PP ini menyediakan dasar hukum bagi pemerintah untuk memberikan sanksi serta memulihkan hak konsumen yang dirugikan oleh pelaku penyelenggara sistem elektronik (PSE). Salah satu ketentuan penting yang menjadi landasan hukum represif adalah Pasal 20, yang mengatur bahwa PSE wajib menjamin keamanan data pribadi yang diolahnya. Jika terjadi pelanggaran terhadap ketentuan ini, maka PSE dianggap lalai dan dapat dikenai sanksi sesuai ketentuan perundang-undangan. Kewajiban ini tidak hanya berlaku saat

pISSN : 1907 - 8188
eISSN : 2797 - 4170

pengumpulan, tetapi juga selama pemrosesan, penyimpanan, dan penghapusan data. Kegagalan dalam memenuhi kewajiban ini dapat menjadi dasar pemberian sanksi represif oleh pemerintah.

B. Tanggungjawab *Marketplace* Terhadap Pelanggaran Pengelolaan Data Pribadi Konsumen Dalam *E-Commerce*

Marketplace sebagai penyelenggara sistem elektronik (PSE) dalam ekosistem *e-commerce* memiliki tanggung jawab hukum atas pengelolaan dan perlindungan data pribadi konsumen yang menggunakan layanannya. Berdasarkan Pasal 1 angka 4 UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), *marketplace* dikategorikan sebagai pengendali data pribadi, yakni pihak yang menentukan tujuan dan kendali atas pemrosesan data pribadi. Oleh karena itu, apabila terjadi kebocoran atau penyalahgunaan data konsumen, *marketplace* wajib bertanggung jawab secara hukum atas kegagalan sistem pengamanan atau kelalaian dalam pengelolaan data. Hal ini ditegaskan dalam Pasal 50 dan Pasal 55 UU PDP, yang menyatakan bahwa pengendali data wajib menjaga keamanan data pribadi serta menjamin pemrosesan dilakukan berdasarkan prinsip keadilan, transparansi, dan akuntabilitas. Ketentuan tersebut didukung oleh Pasal 26 ayat (1) UU ITE, yang mewajibkan penggunaan data pribadi hanya dapat dilakukan atas persetujuan pemilik data. Apabila *marketplace* melanggar ketentuan ini, maka dapat dikenakan sanksi administratif berupa teguran, denda, penghentian sementara kegiatan, hingga sanksi pidana jika terbukti mengakibatkan kerugian.

Lebih lanjut, tanggung jawab *marketplace* juga diatur dalam PP Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, di mana pada Pasal 14 dan Pasal 15 dinyatakan bahwa setiap PSE wajib menjamin keutuhan, ketersediaan, dan kerahasiaan data pribadi pengguna. Ini berarti *marketplace* memiliki kewajiban tidak hanya secara hukum formal, tetapi juga tanggung jawab secara moral dan teknis untuk memastikan sistem keamanannya memadai dan memperbarui kebijakan privasi secara transparan. Misalnya, jika terjadi kebocoran data akibat serangan siber dan terbukti bahwa *marketplace* tidak memiliki sistem proteksi yang kuat (seperti enkripsi atau autentikasi ganda), maka kelalaian tersebut menjadi dasar pertanggungjawaban. Berdasarkan Pasal 67 UU PDP, konsumen sebagai pemilik data juga memiliki hak untuk menuntut ganti rugi atas kerugian yang diderita akibat

pISSN : 1907 - 8188
eISSN : 2797 - 4170

kebocoran data. Namun, dalam praktiknya, konsumen sering kali kesulitan menempuh jalur hukum karena belum adanya otoritas pengawas independen yang efektif menjalankan fungsi kontrol dan penyelesaian sengketa secara cepat.

Dari segi penalaran hukum, tanggung jawab *marketplace* mencerminkan prinsip *strict liability* dalam hukum perlindungan data, yakni tanggung jawab yang melekat tanpa perlu pembuktian unsur kesalahan. Marketplace sebagai entitas dengan kemampuan teknis dan akses langsung terhadap data, berada dalam posisi strategis untuk mencegah risiko pelanggaran. Maka, semakin besar peran *marketplace* dalam transaksi *e-commerce* , semakin besar pula tanggung jawab yang harus dipikul dalam menjamin keamanan data pribadi konsumen.

Dalam UU PDP, korban pelanggaran data pribadi diberikan dua jalur utama untuk menuntut keadilan, yaitu melalui pengaduan secara perdata dan pidana. Jalur perdata dapat ditempuh apabila korban mengalami kerugian akibat penyalahgunaan data pribadinya; hal ini diatur dalam Pasal 14, yang memberikan hak kepada subjek data untuk mengajukan gugatan ganti rugi kepada pihak yang melanggar. Gugatan ini diajukan melalui mekanisme peradilan umum sebagaimana diatur dalam hukum acara perdata. Sementara itu, jalur pidana tersedia apabila pelanggaran terhadap data pribadi memenuhi unsur tindak pidana, sebagaimana diatur dalam Pasal 67 sampai Pasal 73. Dalam hal ini, korban dapat melapor ke aparat penegak hukum seperti kepolisian, yang kemudian akan memprosesnya sesuai prosedur pidana. Namun hingga kini, mekanisme teknis mengenai proses pengaduan, tata cara pelaporan, hingga lembaga pengawas yang berwenang menerima dan menangani pengaduan secara resmi belum diatur secara rinci, karena peraturan pelaksana dari UU PDP masih belum diterbitkan. Akibatnya, efektivitas akses keadilan bagi korban masih menghadapi hambatan implementatif.

Marketplace sebagai pengendali data pribadi bertanggung jawab penuh untuk menjamin keamanan, keutuhan, dan kerahasiaan data pengguna. Jika terjadi kebocoran yang diakibatkan oleh kelalaian *marketplace* dalam menerapkan sistem keamanan, maka *marketplace* dapat dikenai sanksi administratif, bahkan pidana, sesuai dengan ketentuan yang

pISSN : 1907 - 8188
eISSN : 2797 - 4170

berlaku. Di samping itu, UU No. 8 Tahun 1999 tentang Perlindungan Konsumen juga memberikan dasar bagi konsumen untuk menuntut ganti kerugian apabila terjadi kerugian akibat layanan yang tidak memenuhi standar keamanan, sebagaimana diatur dalam Pasal 19 ayat (1).

Secara normatif, tanggung jawab *marketplace* bersifat objektif karena melekat pada fungsinya sebagai pengelola data pribadi, sehingga tidak diperlukan pembuktian unsur kesalahan dalam klaim ganti rugi cukup dibuktikan adanya hubungan kausal antara kebocoran dan kerugian yang diderita konsumen. Selain melalui pengadilan, perselisihan dapat diselesaikan secara alternatif melalui lembaga penyelesaian sengketa seperti Badan Penyelesaian Sengketa Konsumen (BPSK), atau forum mediasi yang disediakan oleh otoritas perlindungan data di masa mendatang. Namun, hingga saat ini, Indonesia belum memiliki lembaga pengawas perlindungan data pribadi yang independen sebagaimana diamanatkan dalam UU PDP, sehingga efektivitas penanganan perselisihan masih bergantung pada kesiapan kelembagaan pemerintah, seperti Kementerian Komunikasi dan Informatika.

Oleh karena itu, dalam rangka memberikan perlindungan hukum yang maksimal, *marketplace* tidak hanya mematuhi norma formal yang tertulis dalam Undang-Undang, tetapi juga menerapkan kebijakan internal yang proaktif, seperti audit keamanan data, pemberitahuan insiden keamanan secara cepat, serta pengelolaan persetujuan pengguna secara jelas dan informatif. Dengan demikian, perlindungan data pribadi konsumen dalam *e-commerce* tidak hanya menjadi slogan normatif, tetapi juga bagian dari praktik nyata tanggung jawab hukum yang dapat ditegakkan.

III. Kesimpulan

Perlindungan hukum terhadap data pribadi merupakan hak konstitusional warga negara Republik Indonesia sebagaimana diatur dalam Pasal 28G Ayat (1) Undang-Undang Dasar 1945 dan di berbagai peraturan perundang-undangan lainnya seperti UU No. 8 Tahun 1999 tentang Perlindungan Konsumen, UU No. 11 Tahun 2008 tentang ITE, UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta peraturan pelaksanaannya. Perlindungan data pribadi dalam regulasi tersebut telah mengatur perlindungan hukum terhadap data pribadi baik perlindungan hukum secara preventif maupun perlindungan hukum secara

represif. Perlindungan secara preventif dalam Undang-Undang perlindungan data pribadi telah diatur bahwa dalam penggunaan data pribadi harus sebelumnya memperoleh persetujuan dari pemilik data serta dalam aspek teknis pengamanan data, pengendali wajib melakukan perlindungan teknis dan organisasi untuk mencegah akses illegal serta penyalahgunaan data pribadi. Sementara dalam aspek kelembagaan, upaya perlindungan preventif diatur bahwa dalam menjaga keamanan data harus dibentuk otoritas pengawas independen yang bertugas untuk mengawasi kepatuhan para pengendali data. Sementara upaya perlindungan hukum represif tercermin dalam berbagai instrumen hukum yang memberikan hak kepada subjek data untuk mengajukan keberatan, pengaduan, dan tuntutan ganti rugi terhadap pihak *marketplace* atau penyelenggara sistem elektronik yang lalai atau menyalahgunakan data. *Marketplace* memiliki tanggungjawab hukum atas kegagalan sistem pengamanan atau kelalaian data pribadi yang menggunakan layanannya. Apabila *marketplace* tidak melaksanakan kewajibannya, maka dapat dikenakan sanksi administratif berupa teguran, denda, penghentian sementara kegiatan, hingga sanksi pidana jika terbukti mengakibatkan kerugian.

Daftar Pustaka

Buku

Hadjon, P.M, *Perlindungan Hukum Bagi Rakyat Indonesia* Surabaya: PT. Bina Ilmu,1987.

Setiono, *Supremasi Hukum*, Surakarta: UNS, 2004.

Jurnal

Agus, Muhammad Rahmat. "Konstitusinalisme Pelayana Publik Di Era Digital Di Negara Republik Indonesia," 2023. https://osf.io/x7mep/download.

Almaida, Zennia. "Perlindungan Hukum Preventif Dan Refresif Bagi Pengguna Uang Elektronik Dalam Menggunakan Transaksi Tol Nontunai." *Privat Law* 9 (2021): 222–23.

Ardika, I Wayan Cenik. "Tinjauan Hukum Terhadap Perlindungan Data Pribadi Di Era Digital: Kasus Kebocoran Data Pengguna Layanan E-Commerce." *Indonesian Journal of Law and Justice* 2, no. 3 (2025): 11. https://doi.org/10.47134/ijlj.v2i3.3601.

Disemadi, Hari Sutra, Lu Sudirman, Junimart Girsang, and Arwa Meida Aninda. "Perlindungan Data Pribadi Di Era Digital: Mengapa Kita Perlu Peduli?" *Sang Sewagati Journal* 1 (2), no. 2 (2023): 67–90. http://journal.uib.ac.id/index.php/sasenal/index.

Firmansyah Putri, Deanne Destriani,

and Muhammad Helmi Fahrozi. "Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan Ruu Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.Com)." *Borneo Law Review* 5, no. 1 (2021): 46–68. https://doi.org/10.35334/bolrev.v5i1.2014.

Hidayat, Eka Wahyu. "STUDI LITERATUR KONSTITUSIONALISME DIGITAL DI ERA E-" 24, no. May (2025).

Milafebina, Rachel, Idham Putra Lesmana, and Moody Rizqy Syailendra. "Perlindungan Data Pribadi Terhadap Kebocoran Data Pelanggan E-Commerence Di Indonesia." *Jurnal Tana Man* 4, no. 1 (2023): 158–69. https://ojs.staialfurqan.ac.id/jtm/.

Parihin, Nela mardiana. "U The Urgensi URGENSI PERLINDUNGAN DATA PRIBADI DALAM PRESPEKTIF HAK ASASI MANUSIA." *Jurnal Rechten : Riset Hukum Dan Hak Asasi Manusia* 5, no. 1 (2023): 16–23. https://doi.org/10.52005/rechten.v5i1.108.

Penelitian, Jurnal, and Jenda Ingan Mahuli. "All Fields of Science J-LAS Perlindungan Hukum Terhadap Data Pribadi Dalam Era Digital Legal Protection of Personal Data in the Digital Era." *AFoSJ-LAS* 3, no. 4 (2023): 188–94. https://j-las.lemkomindo.org/index.php/AFoSJ-LAS/index.

Priliasari, Erna. "PERLINDUNGAN DATA PRIBADI KONSUMEN DALAM TRANSAKSI E-COMMERCE MENURUT PERATURAN PERUNDANG-UNDANGAN DI INDONESIA (Legal Protection of Consumer Personal Data in E-Commerce According To Laws Dan Regulations in Indonesia)." *Jurnal Rechts Vinding* 12, no. 2 (2023): 261–79.

Rahla Azura, Zelly Dia Rofinda , Selfi Renita Rusjdi , Husni , Liganda Endo Mahata, Zurayya Fadila. "Jurnal Riset Ilmiah." *Jurnal Riset Ilmiah* 1, no. 01 (2022): 15–18. https://manggalajournal.org/index.php/SINERGI/article/view/1218/1479.

Subekti, Nanang, I Gusti Ayu Ketut Rahmi Handayani, and Arief Hidayat. "Konstitusionalisme Digital Di Indonesia." *Peradaban Journal of Law and Society* 2, no. 1 (2023): 1–22. https://doi.org/10.59001/pjls.v2i1.74.

Tia Deja Pohan, and Muhammad Irwan Padli Nasution. "Perlindungan Hukum Data Pribadi Konsumen Dalam Platform E Commerce." *Sammajiva: Jurnal Penelitian Bisnis Dan Manajemen* 1, no. 3 (2023): 42–48. https://doi.org/10.47861/sammajiva.v1i3.336.

Peraturan Perundang-Undangan

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Nomor 6820).

Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Informasi dan Transaksi

Elektronik. (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Nomor 6905).

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 42, Tambahan Lembaran Negara Republik Indonesia Nomor 3821).

Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik (PMSE). (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 231. Tambahan Lembaran Negara Nomor 6420).

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Nomor 6400).