



Department of Digital Business

Journal of Artificial Intelligence and Digital Business (RIGGS)

Homepage: <https://journal.ilmudata.co.id/index.php/RIGGS>

Vol. 5 No. 2 (2026) pp: 10090-10098

P-ISSN: 2963-9298, e-ISSN: 2963-914X

Perlindungan Hukum terhadap Konsumen atas Penyalahgunaan Data Pribadi pada Platform E-Commerce Pasca Berlakunya Undang-Undang Nomor 27 Tahun 2022

Viona Zahwa Salsabila, Yulia Qamariyanti
Fakultas Hukum, Universitas Lambung Mangkurat
vionazahwasalsabila@gmail.com, yulia.qamariyanti@ulm.ac.id

Abstrak

Perkembangan platform e-commerce di Indonesia telah memfasilitasi transaksi elektronik, tetapi di sisi lain, hal ini meningkatkan risiko kebocoran dan penyalahgunaan data pribadi konsumen. Data pribadi yang dikumpulkan dan diproses oleh platform e-commerce bernilai tinggi dan oleh karena itu memerlukan perlindungan hukum yang memadai. Studi ini bertujuan untuk menganalisis bentuk-bentuk perlindungan hukum bagi konsumen terhadap penyalahgunaan data pribadi di platform e-commerce dan untuk menganalisis tanggung jawab hukum platform e-commerce sebagai pengendali data pribadi dalam mencegah penyalahgunaan data pribadi konsumen setelah diberlakukannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan, pendekatan konseptual, dan pendekatan kasus. Bahan hukum yang digunakan terdiri atas bahan hukum primer, sekunder, dan tersier yang dianalisis secara preskriptif untuk memperoleh argumentasi hukum yang komprehensif terkait perlindungan data pribadi dalam transaksi elektronik. Penelitian menunjukkan bahwa perlindungan hukum bagi konsumen terhadap penyalahgunaan data pribadi diimplementasikan melalui tindakan preventif berupa peraturan perundang-undangan dan peningkatan literasi digital, serta tindakan represif melalui mekanisme pengaduan, penyelesaian sengketa, dan pemberian sanksi. Namun, implementasi perlindungan hukum tersebut masih menghadapi berbagai kendala, seperti rendahnya literasi digital masyarakat, kesulitan mengidentifikasi pelaku pelanggaran, terbatasnya akses pelaporan, serta belum jelasnya mekanisme kompensasi bagi korban. Selain itu, platform e-commerce sebagai pengendali data pribadi memiliki tanggung jawab hukum berdasarkan prinsip tanggung jawab mutlak untuk menjamin keamanan dan kerahasiaan data pribadi konsumen. Meskipun demikian, pengaturan mengenai pembagian tanggung jawab antar pihak dalam ekosistem digital masih memerlukan pengaturan yang lebih jelas guna memberikan kepastian hukum serta perlindungan yang optimal bagi konsumen di Indonesia.

Kata kunci: Perlindungan Konsumen, Data Pribadi, E-Commerce, UU PDP, Tanggung Jawab Hukum

1. Latar Belakang

Perkembangan teknologi digital yang semakin pesat telah mendorong penggunaan platform *e-commerce* secara masif di seluruh dunia, termasuk Indonesia. Masyarakat Indonesia saat ini semakin terbiasa melakukan berbagai aktivitas ekonomi secara daring, mulai dari berbelanja kebutuhan sehari-hari, memesan makanan, hingga melakukan transaksi keuangan melalui aplikasi digital. Platform *e-commerce* seperti Tokopedia, Shopee, Lazada, Bukalapak, dan berbagai platform sejenis telah menjadi bagian yang tidak terpisahkan dari kehidupan modern masyarakat Indonesia.

Di sisi lain, kemudahan yang ditawarkan oleh platform *e-commerce* juga diiringi oleh meningkatnya risiko yang berkaitan dengan keamanan data pribadi konsumen. Setiap kali konsumen melakukan registrasi akun maupun transaksi pada platform *e-commerce*, mereka diwajibkan untuk menyerahkan sejumlah data pribadi seperti nama lengkap, nomor telepon, alamat, alamat surat elektronik (*email*), hingga data pembayaran dan riwayat transaksi. Data-data tersebut memiliki nilai yang sangat tinggi, baik dari sisi ekonomi maupun privasi, sehingga menjadi target bagi pihak-pihak yang tidak bertanggung jawab. Apabila data pribadi tersebut tidak dilindungi dengan baik, maka dapat menimbulkan berbagai risiko penyalahgunaan data, kebocoran data pribadi, pencurian identitas, hingga tindak penipuan yang merugikan konsumen secara finansial maupun non-finansial.

Indonesia telah mencatat sejumlah kasus kebocoran dan penyalahgunaan data pribadi yang melibatkan platform *e-commerce* besar. Salah satu kasus yang paling banyak mendapat perhatian publik adalah dugaan kebocoran data pengguna Tokopedia pada tahun 2020, yang disebut-sebut melibatkan jutaan akun pengguna dan diperjualbelikan di forum digital atau dark web. Kasus ini kemudian dibawa ke ranah hukum melalui gugatan Komunitas Konsumen Indonesia (KKI) yang terdaftar sebagai Putusan Pengadilan Negeri Jakarta Pusat Nomor 235/Pdt.G/2020/PN.Jkt.Pst tanggal 15 Juni 2022 atas dasar Perbuatan Melawan Hukum. Selain itu, terdapat pula kasus kebocoran data BPJS Kesehatan pada tahun 2021 yang melibatkan ratusan juta data warga negara Indonesia. Kasus-kasus tersebut mencerminkan betapa seriusnya ancaman terhadap keamanan data pribadi dalam sistem elektronik di Indonesia.

Sebelum berlakunya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), pengaturan mengenai perlindungan data pribadi di Indonesia masih tersebar dalam berbagai regulasi yang terpisah-pisah, yakni Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UUPK), Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Kondisi regulasi yang terfragmentasi tersebut menyebabkan kepastian hukum mengenai hak pemilik data, kewajiban pengendali data, serta mekanisme penegakan hukum belum terlaksana secara optimal.

Dengan disahkannya UU PDP pada tanggal 20 September 2022 dan berlakunya secara penuh sejak 17 Oktober 2024 setelah berakhirnya masa transisi dua tahun, Indonesia kini memiliki landasan hukum yang lebih komprehensif dan terpadu dalam mengatur perlindungan data pribadi warga negaranya. UU PDP mengatur berbagai aspek mulai dari jenis data pribadi, hak subjek data, kewajiban pengendali dan prosesor data, mekanisme pengawasan, penyelesaian sengketa, hingga sanksi administratif dan pidana bagi pelanggar. Kehadiran UU PDP ini diharapkan dapat menutup celah hukum yang selama ini menjadi hambatan dalam penanganan kasus penyalahgunaan data pribadi konsumen.

Namun demikian, berlakunya UU PDP tidak serta-merta menyelesaikan seluruh permasalahan yang ada. Masih terdapat beberapa pasal dalam UU PDP yang menimbulkan kekaburan norma dan berpotensi melemahkan perlindungan hukum bagi konsumen. Pasal 12 UU PDP mengenai hak konsumen untuk memperoleh ganti rugi belum mengatur secara rinci mekanisme pengajuan klaim, pembuktian, serta bentuk dan prosedur pemulihan kerugian. Pasal 46 UU PDP tentang kewajiban pemberitahuan apabila terjadi kegagalan perlindungan data belum menetapkan secara tegas batas waktu dan mekanisme teknisnya. Sementara itu, Pasal 35 UU PDP belum eksplisit mengatur pembagian tanggung jawab dalam ekosistem digital yang melibatkan berbagai pihak seperti pengendali data, pemroses data, seller, dan pihak ketiga lainnya. Kondisi tersebut berpotensi menimbulkan ketidakpastian hukum dalam pelaksanaan perlindungan data pribadi konsumen di platform *e-commerce*.

Berdasarkan uraian latar belakang di atas, penelitian ini bertujuan untuk menganalisis dua permasalahan utama, yaitu: (1) bagaimana bentuk perlindungan hukum terhadap konsumen terkait penyalahgunaan data pribadi pada platform *e-commerce* pasca berlakunya UU PDP; dan (2) bagaimana tanggung jawab hukum platform *e-commerce* sebagai pengendali data pribadi dalam mencegah penyalahgunaan data pribadi konsumen. Penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan ilmu hukum perlindungan konsumen dan hukum teknologi informasi, serta menjadi masukan bagi para pembuat kebijakan dalam memperkuat kerangka regulasi perlindungan data pribadi di Indonesia.

2. Metode Penelitian

Penelitian ini menggunakan metode penelitian hukum normatif (*doctrinal research*), yaitu penelitian hukum yang dilakukan dengan memeriksa bahan-bahan hukum untuk menjawab permasalahan hukum yang ada. Pendekatan yang digunakan dalam penelitian ini meliputi tiga pendekatan, yaitu pendekatan perundang-undangan (*statute approach*) yang mengkaji UU PDP, UU ITE, UUPK, dan peraturan pelaksanaannya; pendekatan konseptual (*conceptual approach*) yang mengkaji konsep perlindungan konsumen, privasi data, dan tanggung jawab hukum dalam lingkungan digital; serta pendekatan kasus (*case approach*) yang mengkaji kasus-kasus kebocoran data yang melibatkan platform *e-commerce* di Indonesia.

Sumber bahan hukum dalam penelitian ini terdiri atas tiga jenis. Pertama, bahan hukum primer yaitu peraturan perundang-undangan yang bersifat mengikat, meliputi Undang-Undang Nomor 8 Tahun 1999 tentang

Perlindungan Konsumen, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik. Kedua, bahan hukum sekunder yang memberikan penjelasan terhadap bahan hukum primer, meliputi buku, jurnal ilmiah, tesis, dan artikel terkait. Ketiga, bahan hukum tersier berupa kamus hukum dan ensiklopedia sebagai bahan pendukung.

Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*) dengan cara penelusuran, pengumpulan, dan studi dokumen baik secara konvensional maupun melalui teknologi informasi. Analisis bahan hukum dilakukan secara kualitatif dengan pendekatan deskriptif-analitis, yang difokuskan pada norma-norma hukum yang relevan dan implementasinya untuk menggambarkan, menafsirkan, dan mengevaluasi peraturan serta praktik hukum yang terkait dengan topik penelitian. Metode penalaran yang digunakan adalah metode deduksi, yakni dari premis umum berupa peraturan perundang-undangan ditarik kesimpulan khusus mengenai permasalahan yang diteliti.

3. Hasil dan Diskusi

3.1 Perkembangan E-Commerce dan Urgensi Perlindungan Data Pribadi Konsumen di Indonesia

Perkembangan *e-commerce* di Indonesia tidak dapat dilepaskan dari dinamika globalisasi dan kemajuan teknologi informasi yang terus berlangsung. Sejarah *e-commerce* dimulai pada era 1970-an ketika Michael Aldrich mengembangkan sistem transaksi bisnis berbasis komputer, kemudian berkembang pada era 1980-an dengan adopsi kartu kredit secara luas, dan mengalami lompatan besar pada era 1990-an dengan kemunculan *World Wide Web* oleh Tim Berners-Lee pada tahun 1991. Amazon didirikan pada tahun 1994 sebagai toko buku online pertama, diikuti oleh eBay pada tahun 1995 dan Alibaba pada tahun 1999, yang menjadi tonggak penting dalam perkembangan *e-commerce* global.

Di Indonesia, pertumbuhan *e-commerce* semakin mengalami akselerasi terutama sejak munculnya berbagai platform marketplace lokal pada era 2010-an. Pandemi COVID-19 pada tahun 2020 turut mempercepat transformasi digital dan memperkuat kebiasaan belanja online masyarakat Indonesia secara signifikan. Data menunjukkan bahwa nilai transaksi *e-commerce* Indonesia terus meningkat dari tahun ke tahun, menjadikan Indonesia sebagai salah satu pasar *e-commerce* terbesar di Asia Tenggara. Kemudahan yang ditawarkan oleh platform *e-commerce* mencakup kemampuan menjangkau pelanggan yang lebih luas tanpa batasan geografis, efisiensi biaya operasional, serta kemudahan dalam pengumpulan dan analisis data konsumen.

Namun, di balik berbagai manfaat tersebut, perkembangan *e-commerce* juga membawa konsekuensi serius berupa meningkatnya risiko penyalahgunaan data pribadi konsumen. Dalam setiap transaksi elektronik, konsumen secara tidak sadar memberikan jejak data yang sangat berharga kepada platform *e-commerce*. Data yang dikumpulkan tidak hanya mencakup informasi identitas seperti nama dan alamat, tetapi juga mencakup data perilaku konsumen seperti pola belanja, preferensi produk, lokasi geografis, dan kebiasaan transaksi. Data-data tersebut memiliki nilai ekonomi yang tinggi dan dapat disalahgunakan untuk berbagai kepentingan yang merugikan konsumen, mulai dari penargetan iklan yang tidak diinginkan, penjualan data kepada pihak ketiga tanpa persetujuan, pencurian identitas, hingga penipuan finansial.

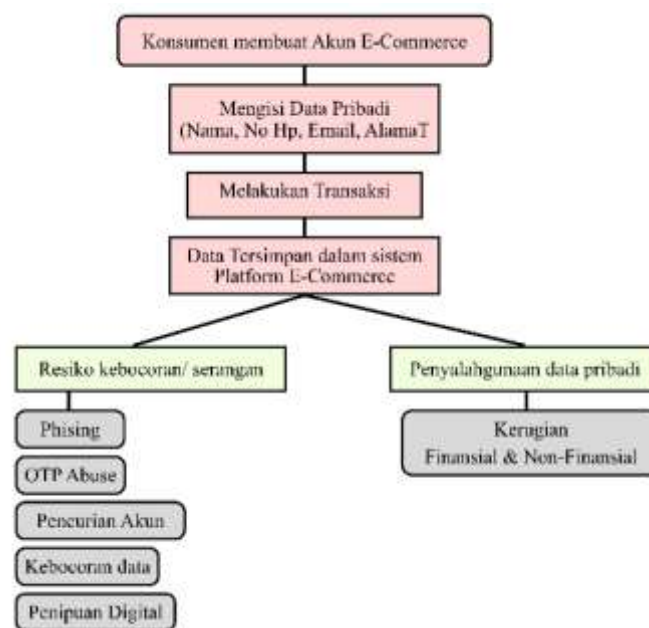
Perlindungan data pribadi pada dasarnya merupakan bagian dari hak asasi manusia yang fundamental, khususnya hak atas privasi. Di Indonesia, hak atas perlindungan diri pribadi telah dijamin secara konstitusional dalam Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, yang menyatakan bahwa 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. Oleh karena itu, urgensi perlindungan data pribadi konsumen dalam transaksi *e-commerce* bukan hanya merupakan kebutuhan praktis, tetapi juga merupakan kewajiban konstitusional negara.

3.2 Perlindungan Hukum Terhadap Konsumen Terkait Penyalahgunaan Data Pribadi pada Platform E-Commerce

Perlindungan hukum terhadap konsumen dalam konteks penyalahgunaan data pribadi di platform *e-commerce* dianalisis menggunakan teori perlindungan hukum yang dikemukakan oleh Philipus M. Hadjon. Menurut Philipus M. Hadjon, perlindungan hukum bagi masyarakat dapat dibagi menjadi dua bentuk, yaitu perlindungan hukum preventif dan perlindungan hukum represif. Perlindungan hukum preventif bertujuan untuk mencegah terjadinya sengketa atau pelanggaran melalui pengaturan norma dan mekanisme pengawasan, sedangkan perlindungan hukum represif diberikan setelah pelanggaran terjadi dalam bentuk penyelesaian sengketa, pemberian ganti rugi, dan pengenaan sanksi.

Selain teori Philipus M. Hadjon, Satjipto Rahardjo juga memberikan pandangan penting mengenai perlindungan hukum. Menurut Satjipto Rahardjo, perlindungan hukum adalah memberikan pengayoman terhadap Hak Asasi Manusia (HAM) yang dirugikan orang lain dan perlindungan itu diberikan kepada masyarakat agar dapat menikmati semua hak-hak yang diberikan oleh hukum. Dalam konteks perlindungan data pribadi konsumen, pandangan ini bermakna bahwa negara dan pelaku usaha memiliki kewajiban untuk memastikan bahwa hak privasi dan keamanan data pribadi konsumen dilindungi dari setiap bentuk penyalahgunaan.

Untuk memahami alur penyalahgunaan data pribadi dan bentuk perlindungan hukum yang tersedia, dapat dilihat pada ilustrasi berikut ini:



Gambar 2.1. Alur Penyalahgunaan Data Pribadi pada Platform E-Commerce
Sumber: Diolah oleh Penulis, 2026

Berdasarkan Gambar 2.1 di atas, proses penyalahgunaan data pribadi pada platform *e-commerce* umumnya diawali dengan pengumpulan data pribadi konsumen pada saat registrasi akun maupun transaksi elektronik. Data yang telah terkumpul kemudian disimpan dalam sistem elektronik platform *e-commerce*. Pada tahap penyimpanan inilah risiko kebocoran dan serangan siber muncul. Apabila sistem keamanan tidak memadai atau terdapat celah keamanan (*vulnerability*), data pribadi konsumen berpotensi diakses oleh pihak yang tidak bertanggung jawab dan disalahgunakan melalui berbagai modus, seperti phishing, penyalahgunaan kode OTP, pencurian akun, kebocoran data pribadi, maupun penipuan digital. Akibat dari penyalahgunaan data pribadi tersebut, konsumen dapat mengalami kerugian yang bersifat finansial seperti kehilangan aset atau uang, maupun kerugian yang bersifat non-finansial seperti pencemaran nama baik, gangguan psikologis, dan hilangnya kepercayaan terhadap transaksi digital.

Peta perlindungan hukum yang tersedia bagi konsumen, baik yang bersifat preventif maupun represif, disajikan sebagai berikut



Gambar 2.2 Bentuk Perlindungan Hukum Konsumen atas Penyalahgunaan Data Pribadi
Sumber: Diolah oleh Penulis, 2026

3.2.1. Perlindungan Hukum Preventif

Perlindungan hukum preventif merupakan upaya pencegahan yang dilakukan sebelum terjadinya pelanggaran atau kerugian. Dalam konteks penyalahgunaan data pribadi di platform *e-commerce*, perlindungan hukum preventif diwujudkan melalui dua dimensi, yaitu dari sisi konsumen dan dari sisi regulasi.

Dari sisi konsumen, terdapat beberapa tindakan yang dapat dilakukan untuk meminimalkan risiko penyalahgunaan data pribadi. Pertama, konsumen harus berhati-hati terhadap tautan (link) yang mencurigakan yang dikirim melalui pesan singkat, surat elektronik, maupun media sosial yang mengatasnamakan platform *e-commerce* tertentu, karena tautan tersebut dapat digunakan oleh pelaku untuk memperoleh data pribadi konsumen secara tidak sah melalui metode phishing. Kedua, konsumen dilarang memberikan kode One Time Password (OTP) kepada siapapun, termasuk kepada pihak yang mengaku sebagai perwakilan resmi platform *e-commerce*, karena kode OTP merupakan kode rahasia yang digunakan untuk memverifikasi identitas pengguna dan dapat digunakan untuk mengambil alih akun. Ketiga, konsumen perlu memastikan bahwa platform yang digunakan merupakan aplikasi atau situs resmi yang memiliki sistem keamanan yang memadai, dengan cara mengunduh aplikasi hanya dari toko aplikasi resmi dan memverifikasi keaslian situs web sebelum memasukkan data pribadi. Keempat, konsumen perlu meningkatkan kehati-hatian dengan memperhatikan setiap permintaan data pribadi yang dianggap tidak wajar dan memahami prosedur transaksi yang benar.

Dari sisi regulasi, perlindungan hukum preventif diwujudkan melalui berbagai ketentuan dalam peraturan perundang-undangan yang mewajibkan platform *e-commerce* untuk menerapkan standar keamanan data yang tinggi. UU PDP mengatur kewajiban pengendali data untuk memperoleh persetujuan yang sah dari pemilik data sebelum melakukan pemrosesan data pribadi, menjaga kerahasiaan dan keamanan data pribadi yang dikelola, serta membatasi pemrosesan data hanya untuk tujuan yang telah disetujui oleh pemilik data. Selain itu, Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik mengatur standar perlindungan data pribadi yang harus dipenuhi oleh perusahaan dalam menyimpan dan mengelola data konsumen, mencakup kewajiban untuk memperoleh data secara jujur dan sah, menjaga keakuratan data, serta memiliki sistem pengamanan yang memadai untuk mencegah kebocoran.

Peranan negara dalam memberikan perlindungan hukum preventif bagi konsumen dalam transaksi *e-commerce* mencakup tiga hal pokok, yaitu menghilangkan hambatan hukum dan memberikan pengaturan dalam transaksi; memberikan fasilitas pengaturan terhadap upaya perlindungan hukum bagi konsumen yang diberikan oleh pelaku usaha (*self-regulation*); serta meningkatkan literasi hukum dan kesadaran konsumen dalam melakukan transaksi elektronik secara aman. Ketiga peranan tersebut saling melengkapi satu sama lain dalam membangun ekosistem digital yang aman dan terpercaya bagi seluruh pihak yang terlibat.

3.2.2. Perlindungan Hukum Represif

Perlindungan hukum represif merupakan upaya perlindungan yang diberikan setelah terjadinya pelanggaran, dengan tujuan untuk menyelesaikan sengketa dan memberikan pemulihan bagi pihak yang dirugikan. Dalam konteks penyalahgunaan data pribadi di platform *e-commerce*, terdapat beberapa mekanisme perlindungan hukum represif yang tersedia bagi konsumen.

Mekanisme pertama adalah pengaduan kepada platform *e-commerce*. Konsumen yang mengalami penyalahgunaan data pribadi dapat melaporkan kejadian tersebut kepada platform *e-commerce* yang bersangkutan agar dilakukan pemeriksaan, pemblokiran akun penyalahguna, maupun tindakan penanganan lainnya sesuai dengan kebijakan internal platform. Mekanisme ini merupakan jalur pertama yang paling mudah diakses oleh konsumen dan umumnya dapat dilakukan melalui fitur pelaporan yang tersedia dalam aplikasi atau situs web platform *e-commerce*. Mekanisme kedua adalah pengaduan kepada otoritas yang berwenang. Apabila penyalahgunaan data pribadi mengakibatkan kerugian finansial, konsumen dapat menyampaikan laporan kepada Otoritas Jasa Keuangan (OJK) atau *Indonesia Anti-Scam Centre* (IASC) untuk memperoleh bantuan penanganan dan tindak lanjut terhadap dugaan penipuan digital. Selain itu, konsumen juga dapat melaporkan kasus penyalahgunaan data kepada Badan Siber dan Sandi Negara (BSSN) atau Kementerian Komunikasi dan Informatika sebagai otoritas yang berwenang dalam pengawasan keamanan siber dan perlindungan data pribadi di Indonesia.

Mekanisme ketiga adalah penyelesaian sengketa melalui jalur non-litigasi. Konsumen dapat menempuh penyelesaian sengketa di luar pengadilan melalui mekanisme mediasi, konsiliasi, atau arbitrase. Badan Penyelesaian Sengketa Konsumen (BPSK) yang dibentuk berdasarkan UUPK juga dapat menjadi alternatif penyelesaian sengketa bagi konsumen yang mengalami kerugian akibat penyalahgunaan data pribadi dalam transaksi *e-commerce*. Penyelesaian melalui jalur non-litigasi pada umumnya lebih cepat, lebih murah, dan lebih mudah diakses oleh konsumen dibandingkan jalur litigasi.

Mekanisme keempat adalah penyelesaian sengketa melalui jalur litigasi. Apabila penyelesaian di luar pengadilan tidak berhasil atau tidak memuaskan, konsumen dapat mengajukan gugatan melalui pengadilan guna memperoleh ganti rugi dan perlindungan atas hak-haknya yang telah dilanggar. Gugatan dapat diajukan berdasarkan ketentuan dalam UUPK, UU PDP, maupun ketentuan umum dalam hukum perdata mengenai perbuatan melawan hukum (Pasal 1365 KUHPerdata). Contoh nyata penggunaan jalur litigasi ini adalah gugatan dalam Putusan Pengadilan Negeri Jakarta Pusat Nomor 235/Pdt.G/2020/PN.Jkt.Pst yang diajukan oleh Komunitas Konsumen Indonesia terhadap PT Tokopedia dan Menteri Komunikasi dan Informatika atas dugaan kebocoran data pribadi pengguna.

3.2.3. Hambatan dalam Pelaksanaan Perlindungan Hukum

Meskipun berbagai mekanisme perlindungan hukum telah tersedia, pelaksanaannya dalam praktik masih menghadapi sejumlah hambatan yang signifikan. Hambatan pertama adalah keterbatasan akses terhadap mekanisme pelaporan dan penyelesaian sengketa. Tidak semua konsumen memahami prosedur pelaporan yang benar, dan terbatasnya akses terhadap informasi serta layanan pengaduan di beberapa wilayah menyulitkan sebagian konsumen untuk mendapatkan bantuan ketika menjadi korban penyalahgunaan data pribadi.

Hambatan kedua adalah sulitnya mengidentifikasi pelaku penyalahgunaan data pribadi. Penyalahgunaan data pribadi dalam transaksi elektronik umumnya dilakukan melalui akun anonim, identitas palsu, nomor telepon sementara, atau akun milik pihak lain, sehingga mempersulit proses identifikasi pelaku dan penegakan hukum. Kondisi ini mengakibatkan konsumen sering mengalami kesulitan dalam mendapatkan kepastian hukum atau mencari pertanggungjawaban atas kerugian yang dialami.

Hambatan ketiga adalah rendahnya literasi digital masyarakat. Perkembangan teknologi yang pesat belum sepenuhnya diimbangi dengan tingkat literasi digital yang memadai. Banyak konsumen masih kurang memahami pentingnya menjaga kerahasiaan data pribadi, mengenali modus-modus penipuan digital, dan memahami risiko memberikan data pribadi kepada pihak yang tidak berwenang. Kondisi ini membuat konsumen lebih rentan terhadap masalah perlindungan data pribadi dalam transaksi *e-commerce*.

Hambatan keempat adalah belum optimalnya pengaturan mengenai mekanisme ganti rugi dan pembagian tanggung jawab. Meskipun berbagai peraturan telah mengatur perlindungan data pribadi, masih terdapat ketidakjelasan mengenai mekanisme kompensasi dan pembagian tanggung jawab jika terjadi pelanggaran data pribadi yang melibatkan berbagai pihak dalam ekosistem digital. Kekaburan norma dalam beberapa pasal UU PDP

sebagaimana diuraikan sebelumnya berpotensi menimbulkan tantangan hukum bagi konsumen yang mencari ganti rugi atas kerugian yang dialami.

3.3. Tanggung Jawab Hukum Platform *E-Commerce* Sebagai Pengendali Data Pribadi

Platform *e-commerce* dalam perspektif hukum perlindungan data pribadi memiliki kedudukan sebagai pengendali data pribadi (*data controller*). Berdasarkan Pasal 1 angka 4 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Pengendali Data Pribadi adalah setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan data pribadi. Kedudukan sebagai pengendali data pribadi ini menimbulkan berbagai kewajiban hukum yang bersifat proaktif dan komprehensif bagi platform *e-commerce* dalam melindungi data pribadi penggunanya.

Platform *e-commerce* seperti Tokopedia, Shopee, dan Lazada dalam praktiknya tidak hanya berfungsi sebagai penyedia layanan transaksi jual beli secara elektronik, tetapi juga secara aktif mengumpulkan berbagai data pribadi pengguna, termasuk nama, alamat, nomor telepon, informasi pembayaran, dan riwayat transaksi. Selain itu, platform tersebut juga menentukan tujuan dari pemrosesan data, antara lain untuk pelaksanaan transaksi, pengiriman barang, promosi, analisis perilaku konsumen, personalisasi iklan, dan keperluan bisnis lainnya. Aktivitas-aktivitas tersebut secara jelas menempatkan platform *e-commerce* sebagai pengendali data pribadi yang harus tunduk pada seluruh ketentuan dalam UU PDP.

Tanggung jawab hukum platform *e-commerce* dalam UU PDP dibangun atas fondasi prinsip *strict liability*, yang menekankan kewajiban proaktif dalam melindungi data pribadi tanpa perlu dibuktikan adanya unsur kesengajaan atau kelalaian. Artinya, apabila terjadi kebocoran atau penyalahgunaan data pribadi konsumen, platform *e-commerce* bertanggung jawab secara hukum terlepas dari ada atau tidaknya niat untuk menyalahgunakan data tersebut. Prinsip ini memberikan perlindungan yang lebih kuat bagi konsumen karena konsumen tidak perlu membuktikan unsur kesalahan dari pihak platform *e-commerce*.

Kewajiban dasar platform *e-commerce* sebagai pengendali data meliputi beberapa aspek penting. Pertama, kewajiban memiliki dasar pemrosesan yang sah (*lawful basis*) untuk setiap aktivitas pemrosesan data, baik berdasarkan persetujuan subjek data, pemenuhan kontrak, kewajiban hukum, kepentingan vital, tugas publik, maupun kepentingan sah. Dalam praktik *e-commerce*, persetujuan subjek data menjadi dasar hukum yang paling relevan, namun hal ini menimbulkan kompleksitas terkait kualitas persetujuan yang harus diberikan secara bebas, spesifik, terinformasi, dan tidak ambigu. Kedua, kewajiban menjamin transparansi kepada konsumen mengenai jenis data yang dikumpulkan, tujuan pemrosesan, pihak-pihak yang menerima data, serta hak-hak konsumen sebagai subjek data. Ketiga, kewajiban menerapkan langkah keamanan teknis dan organisasional yang memadai untuk melindungi data pribadi dari akses tidak sah, kebocoran, atau penyalahgunaan, termasuk penerapan enkripsi data, pembatasan akses, dan audit keamanan berkala.

Selain kewajiban di atas, UU PDP juga mengatur kewajiban platform *e-commerce* untuk memberikan notifikasi kepada otoritas yang berwenang dan kepada subjek data dalam hal terjadi kebocoran atau kegagalan perlindungan data pribadi. Kewajiban notifikasi ini merupakan bentuk akuntabilitas pengendali data yang memungkinkan konsumen untuk segera mengambil langkah-langkah pencegahan guna meminimalkan kerugian yang mungkin timbul akibat kebocoran data tersebut. Namun sebagaimana diuraikan sebelumnya, Pasal 46 UU PDP yang mengatur kewajiban notifikasi ini masih belum menetapkan secara tegas mengenai batas waktu, bentuk, serta mekanisme teknis pemberitahuan kepada subjek data, sehingga berpotensi menimbulkan perbedaan interpretasi dalam implementasi oleh pengendali data.

Apabila terjadi pelanggaran terhadap kewajiban-kewajiban tersebut, platform *e-commerce*, dapat dikenakan berbagai bentuk sanksi. Dari sisi hukum administrasi, sanksi yang dapat dijatuhkan meliputi peringatan tertulis, penghentian sementara pemrosesan data, penghapusan data pribadi, hingga denda administratif dalam jumlah yang signifikan. Dari sisi hukum perdata, platform *e-commerce* dapat digugat untuk memberikan ganti rugi kepada konsumen yang mengalami kerugian akibat penyalahgunaan atau kebocoran data pribadi. Dari sisi hukum pidana, dalam kondisi tertentu pengurus platform dapat dikenakan sanksi pidana berupa pidana penjara dan denda apabila terbukti melakukan penyalahgunaan atau pemalsuan data pribadi secara sengaja.

Meskipun kerangka hukum yang ada telah memberikan landasan yang cukup komprehensif, masih terdapat permasalahan penting terkait pembagian tanggung jawab dalam ekosistem digital yang kompleks. Dalam praktik

e-commerce, seringkali terdapat berbagai pihak yang terlibat dalam pemrosesan data pribadi konsumen, seperti platform *e-commerce* itu sendiri sebagai pengendali data utama, penyedia layanan pembayaran, perusahaan logistik, vendor teknologi, pengiklan, serta berbagai pihak ketiga lainnya. Ketidakjelasan pembagian tanggung jawab di antara para pihak tersebut apabila terjadi kebocoran data menjadi salah satu permasalahan hukum yang paling kompleks dan belum terjawab secara memadai dalam UU PDP saat ini. Diperlukan peraturan pelaksana yang secara eksplisit mengatur mekanisme pembagian tanggung jawab tersebut agar konsumen dapat memperoleh kepastian hukum dan perlindungan yang optimal.

4. Kesimpulan

Berdasarkan hasil analisis dan pembahasan yang telah diuraikan, dapat ditarik dua kesimpulan utama dari penelitian ini. Pertama, perlindungan hukum terhadap konsumen terkait penyalahgunaan data pribadi pada platform *e-commerce* di Indonesia belum terlaksana secara optimal meskipun telah terdapat berbagai peraturan perundang-undangan yang mengaturnya. Perlindungan hukum preventif telah diwujudkan melalui kewajiban-kewajiban yang dibebankan kepada pengendali data dan melalui peran negara dalam membangun ekosistem digital yang aman, sedangkan perlindungan hukum represif tersedia melalui mekanisme pengaduan kepada platform *e-commerce*, OJK, IASC, serta jalur non-litigasi dan litigasi. Namun dalam praktiknya, implementasi perlindungan hukum tersebut masih menghadapi berbagai hambatan yang signifikan, meliputi rendahnya literasi digital masyarakat, sulitnya identifikasi pelaku penyalahgunaan data, keterbatasan akses pelaporan dan penyelesaian sengketa, serta kekaburan norma dalam beberapa pasal UU PDP yang berkaitan dengan mekanisme ganti rugi, kewajiban pemberitahuan kebocoran data, dan pembagian tanggung jawab antar pihak dalam ekosistem digital. Kedua, tanggung jawab hukum platform *e-commerce* sebagai pengendali data pribadi dalam mencegah penyalahgunaan data pribadi konsumen telah diatur secara cukup komprehensif dalam UU Nomor 27 Tahun 2022, yang membangun tanggung jawab tersebut di atas fondasi prinsip *strict liability*. Platform *e-commerce* berkewajiban untuk memiliki dasar pemrosesan yang sah, menjamin transparansi, mendapatkan persetujuan eksplisit dari konsumen, menerapkan langkah-langkah keamanan yang memadai, serta memberikan notifikasi apabila terjadi kebocoran data. Namun demikian, implementasi tanggung jawab hukum tersebut dalam praktik masih menghadapi berbagai tantangan, terutama terkait belum jelasnya pembagian tanggung jawab hukum antara pengendali data, pemroses data, dan berbagai pihak ketiga dalam ekosistem digital yang semakin kompleks. Berdasarkan kesimpulan tersebut, penelitian ini merekomendasikan agar pemerintah segera menyusun peraturan pelaksana UU PDP yang secara rinci mengatur mekanisme ganti rugi, batas waktu notifikasi kebocoran data, serta pembagian tanggung jawab antar pihak dalam ekosistem digital. Pemerintah juga perlu meningkatkan program literasi digital secara merata dan memperkuat kapasitas lembaga pengawas perlindungan data pribadi. Di sisi lain, platform *e-commerce* perlu didorong untuk secara proaktif menerapkan langkah-langkah pencegahan seperti

Referensi

1. S. C. Salim dan J. Neltje, "Analisis Perlindungan Hukum Terhadap Data Pribadi Dalam Transaksi E-Commerce," Vol. 4, 2021
2. P. Purnamasari et al., "Perlindungan Hukum Data Pribadi Konsumen dalam Transaksi E-Commerce di Bekasi," Jurnal Pengabdian Kepada Masyarakat, Vol. 3, No. 2, 2025.
3. B. Christine dan C.S.T. Kansil, "Hambatan Penerapan Perlindungan Data Pribadi di Indonesia Setelah Disahkannya UU No. 27 Tahun 2022," Jurnal Ilmiah Indonesia, Vol. 7, No. 09, Sep. 2022.
4. Y. Pratomo, "UU Perlindungan Data Pribadi Berlaku Sepenuhnya di Indonesia," Kompas.com. 2024.
5. K. N. Adistiya et al., "Perlindungan Hukum bagi Konsumen terhadap Kebocoran Data Pribadi Berdasarkan Pasal 16 Ayat (2) Huruf e UU No. 27 Tahun 2022," Jurnal Ilmu Hukum Sui Generis, Vol. 4, No. 3, Jul. 2024.
6. Republik Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Pasal 12, 35, dan 46. <https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022>
7. N. Rosmawarni et al., E-Commerce. Jakarta: PT Penamudamedia, 2024.
8. H. K. Zaenal dan M. Orias, "Urgensi Perlindungan Hukum Data Pribadi Konsumen dalam Transaksi E-Commerce," Community Development Journal, Vol. 5, No. 4, 2024.
9. D. A. Alpiana et al., "Tanggungjawab Pelaku Usaha dalam Transaksi E-Commerce Perspektif Perlindungan Konsumen," Lex Journal: Kajian Hukum & Keadilan, Surabaya: Universitas Dr. Soetomo.
10. S. Iskandar, "Perkembangan E-Commerce di Indonesia: Regulasi dan Tantangannya," Media Hukum Indonesia, Vol. 3, No. 4, Okt. 2025.
11. Philipus M. Hadjon, Perlindungan Hukum Bagi Rakyat Indonesia. Surabaya: Bina Ilmu, 1987.
12. F. B. Wibisono dan E. Pranoto, "Upaya Perlindungan Hukum bagi Korban Tindak Pidana Kesusilaan melalui Media Online," Jurnal Kolaboratif Sains, Vol. 6, No. 12, Des. 2023.
13. P. Sihombing, W. S. Widiarty, dan B. Nadapdap, "Perlindungan Hukum terhadap Data Pribadi Konsumen dalam Transaksi E-Commerce di Indonesia," Jurnal Sosial dan Teknologi, Vol. 6, No. 1, 2026.
14. D. Christian, "Kewajiban-Kewajiban Penting dalam UU PDP dan Sanksinya Jika Melanggar," Hukumonline Klinik.
15. YAPLegal.id, "Panduan Lengkap UUPK dan Perlindungan Konsumen," diakses 27 Apr. 2026.
16. A. H. Barkatullah, Perlindungan Hukum bagi Konsumen dalam Transaksi E-Commerce. Bandung: Nusamedia, 2022.
17. S. Dewi, Perlindungan Privasi atas Informasi Pribadi di Internet. Bandung: Widya Padjadjaran, 2009.

18. N. Afifah, "Tanggung Jawab Hukum Platform E-Commerce terhadap Keamanan Data Pribadi," Jurnal Legalitas, Vol. 2, No. 1, Jan. 2024.
19. A. S. Diah dan S. A. Wiraguna, "Tanggung Jawab Hukum Platform E-Commerce atas Kebocoran Data Pribadi dalam Perspektif UU No. 27 Tahun 2022," Jurnal Kajian Hukum dan Kebijakan Publik, Vol. 2, No. 2, 2025
20. UU No. 27 Tahun 2022, "Sinergi: Jurnal Ilmiah Multidisiplin, Vol. 2, No. 1, 2026.
21. R. P. P. Karo-Karo dan T. Prasetyo, Pengaturan Perlindungan Data Pribadi di Indonesia; Perspektif Teori Keadilan Bermartabat. Bandung: Nusa Media, 2020.
22. I. R. Anshari, "Perlindungan Hukum atas Data Pribadi Konsumen dalam Transaksi E-Commerce," Tesis Magister Hukum, Fakultas Hukum, Universitas Islam Sultan Agung Semarang, 2024.