

Perlindungan Hukum Terhadap Data Pribadi Konsumen Dalam Transaksi *E-Commerce*

Rizaldi Umar¹.

¹. Program Studi Hukum Bisnis, Fakultas Hukum Bisnis, Universitas Gunung Lauser.
E-mail: rizaldiumar.sh.mkn@gmail.com (CA)

Abstrak: Perlindungan data pribadi menjadi isu penting dalam era digital saat ini, termasuk dalam konteks e-commerce. Jurnal ini menganalisis perlindungan hukum terhadap data pribadi konsumen berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Dengan mengkaji prinsip-prinsip dasar undang-undang dan kasuistik yang terjadi, diharapkan dapat memberikan gambaran mengenai efektivitas perlindungan data pribadi dalam transaksi e-commerce. Artikel ini mengkaji isu kebocoran data pribadi dalam ekosistem e-commerce di Indonesia, dengan fokus pada kasus kebocoran data pengguna IndoHome pada tahun 2022. Studi ini menggunakan pendekatan yuridis normatif untuk menganalisis regulasi yang berlaku, termasuk Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), serta peraturan lainnya yang relevan. Hasil penelitian menunjukkan bahwa meskipun UU PDP memberikan dasar hukum yang lebih jelas untuk perlindungan data pribadi, tantangan tetap ada dalam implementasinya. Kasus IndoHome menjadi contoh nyata kelemahan dalam sistem keamanan data dan akuntabilitas perusahaan. Selain itu, analisis ini mengungkapkan adanya celah dalam regulasi yang memungkinkan pelanggaran privasi tetap terjadi, serta kurangnya kesadaran konsumen terkait hak-hak mereka. Studi ini merekomendasikan penguatan regulasi, peningkatan kapasitas institusi, literasi digital, dan adopsi praktik terbaik internasional seperti General Data Protection Regulation (GDPR) Uni Eropa untuk menciptakan ekosistem digital yang lebih aman dan terpercaya.

Kata Kunci: Data Pribadi, *E-Commerce*, Transaksi.

Sitasi: Umar, R. (2026). Perlindungan Hukum Terhadap Data Pribadi Konsumen Dalam Transaksi E-Commerce. *Locus Journal of Academic Literature Review*, 5(8), 1197–1206.
<https://doi.org/10.56128/ljoalr.v5i8.1159>

1. Pendahuluan

Dalam transaksi *e-commerce*, data pribadi konsumen seringkali dikumpulkan dan diproses oleh penyedia layanan. Hal ini menimbulkan risiko pelanggaran privasi dan penyalahgunaan data. Undang-Undang Nomor 27 Tahun 2022 hadir sebagai upaya untuk melindungi data pribadi, di era digital ini telah membawa perubahan signifikan dalam preferensi dan perilaku belanja, yang memicu peralihan besar-besaran ke platform *e-commerce*. Keunggulan seperti kemudahan akses, ketersediaan produk yang beragam, dan harga yang kompetitif menjadi daya tarik utama platform ini. Era digital telah membawa perubahan mendalam dalam berbagai aspek kehidupan

manusia, terutama dalam pola konsumsi dan interaksi ekonomi melalui platform *e-commerce*. (Saragih et al., 2023)

Kemajuan pesat dalam teknologi informasi dan komunikasi telah memberikan berbagai kemudahan bagi masyarakat, terutama dalam mengakses produk dan layanan secara daring. Transformasi digital ini memungkinkan transaksi menjadi lebih cepat, efisien, dan mudah dilakukan kapan saja dan di mana saja. Namun, di balik manfaat yang ditawarkan, terdapat tantangan yang tidak kalah pentingnya untuk diperhatikan. Beberapa tantangan utama mencakup perlindungan hak konsumen, privasi, keamanan data, standar kualitas produk, dan mekanisme penyelesaian sengketa. Perlindungan hak konsumen menjadi sangat krusial mengingat banyaknya kasus penipuan atau ketidaksesuaian produk dengan deskripsi yang ditawarkan. Selain itu, keamanan data dan privasi juga menjadi isu sentral, karena semakin banyak data pribadi yang disimpan dan diproses oleh platform digital. Jika tidak dikelola dengan baik, data ini berpotensi disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab. (Fista et al., 2023)

Salah satu ancaman terbesar yang muncul dalam ekosistem digital adalah kebocoran data pribadi. Data pribadi kini dianggap sebagai salah satu aset paling berharga, baik bagi individu maupun bagi perusahaan, karena memiliki nilai ekonomis yang tinggi. Namun, nilai tersebut menjadikannya target empuk bagi pelaku kejahatan siber. Kebocoran data yang semakin sering terjadi tidak hanya membahayakan privasi individu, tetapi juga menimbulkan dampak buruk yang luas, termasuk kerugian finansial, kerusakan reputasi, dan tekanan psikologis bagi para korban. Selain itu, pelanggaran keamanan data juga dapat mengancam kepercayaan masyarakat terhadap layanan digital, yang pada akhirnya dapat menghambat perkembangan ekonomi digital secara keseluruhan. Pencurian data pribadi telah menjadi bentuk kejahatan yang berkembang seiring dengan kemajuan teknologi digital, di mana berbagai aktivitas kini dapat dilakukan melalui media digital. Meskipun perlindungan data memiliki banyak manfaat dan keuntungan, kebutuhan akan perangkat lunak pelindung data yang lebih ketat dan akurat menjadi semakin penting. Hal ini disebabkan oleh dampak negative yang ditimbulkan oleh perkembangan *e-commerce*, yang dirasakan merugikan banyak masyarakat. Beberapa dampak tersebut mencakup tindakan kecurangan yang menyebabkan kerugian finansial langsung, peretasan rekening bank, pencurian data pribadi, serta penggunaan akses oleh pihak yang tidak dikenal, sehingga menimbulkan keresahan di kalangan masyarakat. (Sobirin & Choeriyah, 2024)

Dalam konteks hukum pidana, tindak pidana pencurian data pribadi dapat ditemukan dalam Pasal 482 dan Pasal 483 KUHP baru. Namun, aturan ini belum secara spesifik mengatur pencurian data pribadi secara online, sehingga perlindungan terhadap

data pribadi konsumen *e-commerce* masih belum memadai. Peningkatan risiko tindak pidana pencurian data dan pelanggaran privasi pengguna *e-commerce* mencerminkan pergeseran fokus kejahatan ke ranah digital. Fenomena ini menjadi semakin kompleks dan meresahkan karena semakin banyaknya informasi sensitif yang disimpan dan dipertukarkan dalam ekosistem transaksi online.

Sebagai platform *e-commerce* terkemuka di Indonesia, IndiHome menjadi fokus penelitian dalam memahami kasus kebocoran data pribadi dari perspektif hukum pidana. Penelitian ini penting untuk memahami dampak kejahatan siber terhadap perlindungan data pribadi dan privasi pengguna *e-commerce*, serta untuk mengidentifikasi kelemahan dalam implementasi regulasi yang ada. Kasus kebocoran data yang terjadi pada platform Indihome pada tahun 2022 sekitar 26 juta akun pengguna menjadi salah satu contoh nyata risiko yang dihadapi oleh konsumen dalam ekosistem *e-commerce*. Insiden ini mengungkapkan lemahnya sistem keamanan yang diterapkan oleh perusahaan, serta kurangnya akuntabilitas dalam pengelolaan data pribadi. Pelanggaran seperti ini menunjukkan pentingnya perlindungan hukum yang kuat untuk mencegah insiden serupa di masa depan. (Ardika, 2025)

Insiden kebocoran data semacam ini mengarah pada pertanyaan mendasar tentang tanggung jawab perusahaan, mekanisme ganti rugi bagi konsumen, serta efektivitas regulasi yang ada. Secara global, upaya untuk meningkatkan perlindungan data pribadi telah dilakukan melalui berbagai kerangka kerja hukum. *General Data Protection Regulation* (GDPR) di Uni Eropa menjadi contoh standar global yang mengatur tata kelola data pribadi dengan ketat, termasuk hak konsumen untuk mengakses, memperbaiki, dan menghapus data mereka. Di Indonesia, pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi mencerminkan kesadaran pemerintah akan urgensi perlindungan data dalam menghadapi ancaman dunia digital. Undang-undang ini menjadi langkah penting dalam menciptakan kerangka hukum yang komprehensif. Namun, implementasi dan pengawasan terhadap undang-undang tersebut masih menghadapi berbagai tantangan, termasuk keterbatasan kapasitas institusi dan kesenjangan antara regulasi dan perkembangan teknologi. (Hasian & Fitria, 2025)

Hak konsumen dalam konteks perlindungan data pribadi menjadi salah satu isu penting yang harus mendapatkan perhatian serius. Konsumen memiliki hak fundamental untuk mengetahui bagaimana data mereka digunakan, serta untuk meminta perbaikan atau penghapusan data yang dianggap tidak relevan atau digunakan secara tidak sah. Dalam kasus kebocoran data, konsumen sering kali menghadapi situasi sulit untuk menuntut keadilan, baik karena keterbatasan akses terhadap mekanisme hukum maupun karena perusahaan yang bersangkutan tidak secara proaktif memberikan solusi yang memadai. Oleh karena itu, keberadaan kerangka hukum yang memberikan

jalur yang jelas bagi konsumen untuk mendapatkan ganti rugi dan memastikan akuntabilitas perusahaan menjadi kebutuhan mendesak. Di sisi lain, laju perkembangan teknologi sering kali melampaui kemampuan regulasi untuk beradaptasi. Hal ini menciptakan celah hukum yang dapat dimanfaatkan oleh pihak-pihak tidak bertanggung jawab, termasuk perusahaan yang tidak menerapkan standar keamanan yang memadai. Oleh karena itu, perlu adanya pendekatan yang holistik dalam mengatasi tantangan ini, termasuk penguatan regulasi, pengawasan yang lebih ketat, dan peningkatan literasi digital di kalangan konsumen.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis tantangan hukum terkait perlindungan data pribadi di era digital, khususnya dalam konteks *e-commerce*. Penelitian ini akan meninjau tanggung jawab perusahaan, efektivitas regulasi yang berlaku, serta hak konsumen dalam menghadapi kasus-kasus kebocoran data. Selain itu, kajian ini juga akan menawarkan rekomendasi kebijakan yang relevan guna memperkuat perlindungan data pribadi di Indonesia, dengan harapan dapat mewujudkan ekosistem digital yang lebih aman dan terpercaya bagi seluruh pihak.

2. Metode Penelitian

Metode penelitian yang digunakan dalam penulisan jurnal ini adalah penelitian yuridis normatif dengan pendekatan perundang-undangan (*statute approach*) dan pendekatan kasus (*case approach*), di mana penelitian ini mengkaji bahan hukum primer berupa peraturan perundang-undangan khususnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi serta bahan hukum sekunder berupa literatur, jurnal ilmiah, dan dokumen hukum terkait, yang kemudian dianalisis secara kualitatif untuk mengevaluasi efektivitas regulasi serta pertanggungjawaban hukum dalam kasus kebocoran data pada ekosistem *e-commerce*.

3. Hasil & Pembahasan

3.1. Praktik E-Commerce dan Tantangan Perlindungan Konsumen terhadap data pribadi di Indonesia

Perkembangan *e-commerce* di Indonesia berlangsung dengan pesat, didorong oleh peningkatan jumlah pengguna internet dan adopsi teknologi yang lebih luas. Transformasi dalam praktik *e-commerce* mencakup beberapa hal, yaitu meningkatnya penggunaan perangkat seluler, beragamnya jenis layanan yang ditawarkan, penerapan strategi pemasaran yang disesuaikan dengan kebutuhan lokal, serta kemajuan infrastruktur logistik. Semua ini mencerminkan adaptasi *e-commerce* terhadap kebutuhan pasar yang terus berubah, dan berkontribusi pada peningkatan pengalaman konsumen serta inklusi digital di seluruh negeri. (Sutrisna, 2021)

Perkembangan *e-commerce* ini juga mempengaruhi hak dan kesejahteraan konsumen. Hal ini terlihat dari meningkatnya kesadaran hukum, regulasi perlindungan konsumen, serta fokus pada kualitas layanan dan produk. Selain itu, privasi data dan keamanan menjadi perhatian utama, dengan perlindungan terhadap kejahatan siber yang semakin diperkuat. 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. Sementara itu, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) menetapkan aturan terkait perlindungan data pribadi, mencakup pengumpulan, pengolahan, dan penggunaan data pribadi konsumen oleh penyedia layanan elektronik. UU ITE menekankan pentingnya agar penyedia layanan melindungi data pribadi konsumen dan menjaga kerahasiaan informasi tersebut. Selain itu, UU ITE memberikan sanksi hukum bagi pelanggaran privasi, termasuk tindakan yang melibatkan penyalahgunaan data pribadi atau serangan terhadap keamanan data. Kedua undang-undang ini berupaya secara bersama-sama untuk meningkatkan literasi dan kesadaran konsumen mengenai hak dan kewajiban mereka dalam era digital, dengan penekanan pada ketentuan privasi yang jelas dan komprehensif.

Undang-Undang Perlindungan Konsumen (UU No. 8 Tahun 1999) di Indonesia berperan sentral dalam melindungi konsumen dan mengatasi tantangan baru dalam era digital, termasuk dalam konteks manipulasi pasar. Dalam aspek Hak Privasi dan Informasi, UU ini mengonfirmasi hak konsumen untuk memperoleh informasi yang jujur dan benar mengenai barang/jasa, termasuk dalam transaksi digital, serta mengakui hak privasi konsumen dalam pengumpulan, penggunaan, dan pengolahan informasi pribadi oleh penyedia barang/jasa. Perlindungan Konsumen dalam Transaksi Elektronik diwujudkan melalui pengakuan terhadap transaksi elektronik dan regulasi hak-hak konsumen, termasuk hak untuk mendapatkan informasi yang jelas dan komprehensif mengenai transaksi elektronik, termasuk kebijakan privasi penyedia layanan.

Perlindungan data pribadi konsumen menghadapi berbagai tantangan yang semakin kompleks seiring dengan berkembangnya aktivitas digital dan perdagangan elektronik. Salah satu tantangan utama adalah memastikan kepatuhan perusahaan terhadap regulasi perlindungan data pribadi. Berbagai negara telah menerapkan ketentuan yang ketat, seperti *General Data Protection Regulation* (GDPR) di Eropa dan Undang-Undang Perlindungan Data Pribadi di Indonesia. Kepatuhan terhadap regulasi tersebut menjadi tantangan, terutama bagi perusahaan yang memiliki keterbatasan sumber daya, karena ketidakpatuhan dapat menimbulkan konsekuensi hukum sekaligus merugikan konsumen. Di sisi lain, peningkatan aktivitas daring juga diikuti oleh meningkatnya risiko kejahatan siber, seperti pencurian data, penipuan, dan serangan *malware*. Kebocoran data pribadi dapat dimanfaatkan untuk berbagai tindak kejahatan yang tidak hanya menimbulkan kerugian finansial, tetapi juga berdampak terhadap keamanan dan kondisi psikologis konsumen. (Milafebina & Lesmana, 2023)

Tantangan lainnya berkaitan dengan masih rendahnya kesadaran konsumen mengenai hak-haknya atas data pribadi. Sebagian konsumen belum memahami bahwa mereka memiliki hak untuk mengakses, memperbaiki, maupun menghapus data pribadi yang disimpan oleh perusahaan. Kondisi tersebut dapat meningkatkan kerentanan terhadap penyalahgunaan data. Permasalahan juga muncul dari aspek transparansi, karena perusahaan tidak selalu memberikan informasi yang jelas dan mudah dipahami mengenai cara data pribadi dikumpulkan, digunakan, disimpan, dan dibagikan. Kurangnya transparansi menyebabkan konsumen kesulitan mengetahui risiko serta tujuan pemrosesan data yang mereka berikan. Selain itu, keamanan data yang belum memadai, khususnya pada perusahaan dengan keterbatasan sumber daya dan pengetahuan teknis, dapat memperbesar peluang terjadinya kebocoran maupun serangan siber.

Keterbatasan teknologi dan infrastruktur turut menjadi hambatan dalam mewujudkan perlindungan data pribadi yang optimal. Perangkat lunak yang rentan maupun perangkat keras dan sistem keamanan yang tidak memadai dapat menciptakan celah bagi terjadinya pelanggaran data. Tantangan tersebut semakin kompleks dalam konteks globalisasi, terutama karena transaksi *e-commerce* sering melibatkan konsumen, perusahaan, dan penyedia layanan dari berbagai negara yang memiliki ketentuan perlindungan data yang berbeda. Perbedaan regulasi tersebut menuntut perusahaan untuk mampu menyesuaikan praktik pengelolaan datanya dengan berbagai rezim hukum yang berlaku. Di samping itu, praktik pengumpulan data secara berlebihan juga menjadi persoalan karena perusahaan sering kali mengumpulkan data melebihi kebutuhan untuk menyediakan suatu layanan. Pengumpulan yang berlebihan tidak hanya bertentangan dengan prinsip minimisasi data, tetapi juga memperluas potensi risiko apabila data tersebut mengalami kebocoran atau disalahgunakan.

Dengan demikian, perlindungan data pribadi konsumen memerlukan kepatuhan hukum, peningkatan kesadaran konsumen, transparansi pengelolaan data, penguatan keamanan teknologi, serta penerapan prinsip minimisasi data secara konsisten.

3.2. Pertanggungjawaban Hukum Terhadap Data Pribadi Konsumen Dalam Transaksi *E-Commerce* Menurut Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi untuk selanjutnya disebut UU PDP. memberikan dasar hukum yang jelas mengenai tanggung jawab perusahaan dalam menjaga data konsumen. Dengan penerapan UU PDP, pemerintah berharap dapat meminimalisir insiden kebocoran data yang selama ini sering mengganggu berbagai perusahaan teknologi di Indonesia. Keamanan siber telah menjadi isu global, dan Indonesia tidak terhindar dari ancaman ini. Kasus kebocoran data di berbagai sektor, mulai dari perbankan hingga platform digital, telah menimbulkan kekhawatiran yang besar di kalangan masyarakat. (Anindya & Subiyanto, 2025)

UU PDP mencakup berbagai aspek penting yang sebelumnya diabaikan dalam regulasi terkait data di Indonesia. Undang-undang ini mengatur berbagai hal, mulai dari pengumpulan, penyimpanan, dan pemrosesan data, hingga penghapusan data. UU PDP memberikan hak kepada individu untuk meminta akses, melakukan koreksi, dan bahkan menghapus data pribadi mereka jika diperlukan.

Pasal 1 Poin 2 UU PDP menyatakan bahwa perlindungan data pribadi adalah seluruh upaya untuk melindungi data dalam rangkaian pemrosesan data pribadi, guna menjamin hak konstitusional subjek data pribadi, serta mengatur bagaimana data tersebut akan diberikan dan digunakan oleh pihak lain. Pasal 4 mengklasifikasikan data pribadi menjadi dua jenis: data pribadi umum dan data pribadi spesifik. Data pribadi umum, seperti nama, alamat, status, agama, dan nomor telepon, dapat digunakan secara umum. Sementara itu, data pribadi spesifik merupakan data yang sensitif, seperti data kesehatan, data biometrika, atau catatan kriminal.

Salah satu hal penting dalam UU PDP adalah hak pemilik data. Setiap individu berhak untuk mengetahui bagaimana data mereka digunakan, siapa yang menggunakannya, memperbaiki data atau menolak penggunaan data, serta meminta penghapusan data jika diperlukan. Konsep ini memberikan hak penuh kepada pemilik data atas penggunaan informasi pribadi mereka.

PT Telekomunikasi Indonesia Tbk (Telkom) merupakan badan hukum berbentuk Perseroan Terbatas yang terus mengembangkan jaringan IndiHome ke seluruh pelosok Indonesia agar layanan koneksi internet cepat tersebut dapat dinikmati seluruh rakyat

Indonesia. IndiHome (Indonesia Digital Home) adalah layanan *internet fixed broadband* terkemuka di Indonesia yang menyediakan paket triple play (internet cepat, TV kabel, dan telepon rumah) berbasis teknologi serat optik. Total pelanggan IndiHome mencapai 11,3 juta (B2C & B2B) per semester I-2025, dengan pertumbuhan residensial 10% menjadi 10,1 juta pelanggan. Salah satu kasus kebocoran data IndiHome pada Agustus 2022 melibatkan sekitar 26 juta riwayat penelusuran (*browsing history*) dan data pribadi pengguna (nama, NIK) yang disebar di forum peretas. Peretas mengklaim memiliki data tersebut, sementara Telkom melakukan investigasi validitas dan memperkuat sistem keamanan. Kasus ini menyoroti risiko privasi dan pentingnya UU PDP. (Halizah & dkk, 2025)

Undang-Undang PDP memberikan mandat yang jelas mengenai kewajiban Pengendali Data Pribadi. Pasal 20 UU PDP menyatakan bahwa Pengendali Data wajib melindungi Data Pribadi yang dikelolanya. Perlindungan ini mencakup aspek teknis dan manajerial. Kegagalan memenuhi kewajiban ini, seperti yang terjadi pada kasus Indihome, dapat berimplikasi hukum berat, mulai dari sanksi administratif (teguran tertulis, denda administratif, hingga penghentian pemrosesan data), ganti rugi perdata, hingga sanksi pidana (Pasal 57 -76 UU PDP). Kasus ini menjadi preseden penting dan ujian nyata pertama bagi efektivitas penegakan UU PDP di Indonesia.

Dalam konteks hukum positif Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) secara tegas menetapkan bahwa pengendali data dalam hal ini Telkomsel sebagai penyedia layanan IndiHome memiliki tanggung jawab hukum atas keamanan data pribadi milik pelanggannya. Meski demikian, sejumlah kasus yang muncul, seperti kebocoran data 26,7 juta pengguna IndiHome di situs gelap pada 2022, menunjukkan adanya kelemahan serius dalam mekanisme perlindungan yang dijalankan Telkomsel. Padahal, ketentuan Pasal 39 UU PDP secara eksplisit mengamanatkan bahwa pengendali data wajib menjamin keamanan sistem informasi yang dikelolanya, sedangkan Pasal 46 mengatur keharusan untuk menyampaikan pemberitahuan resmi kepada otoritas berwenang dan subjek data paling lambat 72 jam sejak diketahui terjadinya pelanggaran. (Halizah & dkk, 2025)

Tidak berhenti di situ, Pasal 47 UU PDP memperkenalkan prinsip *strict liability*, yaitu tanggung jawab mutlak di mana pengendali data tetap dinyatakan bertanggung jawab secara hukum meskipun tidak terbukti adanya kesengajaan atau kelalaian secara langsung. Konsep ini mempertegas bahwa Telkomsel tidak hanya wajib bertanggung jawab secara teknis, tetapi juga secara yuridis apabila gagal menjalankan fungsi pencegahan terhadap insiden kebocoran data. Konsekuensinya, Telkomsel dapat dikenakan sanksi administratif, mulai dari teguran tertulis, denda maksimal sebesar

2% dari total pendapatan tahunan, hingga pencabutan izin pengelolaan data sebagaimana diatur dalam Pasal 57 dan 58 UU PDP.

Jika dianalisis melalui pendekatan teori pertanggungjawaban hukum, maka kelalaian yang terjadi pada Telkomsel patut dikualifikasikan sebagai kelalaian sistemik, yang mencerminkan kegagalan dalam memenuhi kewajiban administratif, serta berpotensi mengarah pada tanggung jawab perdata dan pidana, tergantung pada tingkat dampak serta kerugian yang dialami oleh pemilik data. Dalam implementasinya, Telkomsel belum menunjukkan komitmen yang utuh dalam bentuk transparansi proses investigasi, pemberian kompensasi kepada korban, serta audit keamanan digital secara terbuka yang dapat memastikan bahwa kejadian serupa tidak akan terulang. Hal tersebut jelas bertentangan dengan prinsip perlindungan data sebagai bagian dari hak asasi manusia, sebagaimana bahwa informasi pribadi merupakan bagian integral dari HAM yang wajib dijamin oleh negara dan entitas privat (Novel & Subiyanto, 2025). Oleh karena itu, mekanisme pertanggungjawaban hukum yang semestinya dijalankan oleh Telkomsel harus bersifat menyeluruh, dimulai dari pemenuhan kewajiban notifikasi publik, pembaruan sistem keamanan internal, pelaksanaan audit independen, hingga penyediaan skema kompensasi yang layak bagi para korban kebocoran data. Apabila tanggung jawab ini diabaikan, makapelanggaran yang terjadi tidak hanya bersifat hukum, tetapi juga mencederai etika dan integritas korporasi karena telah mengkhianati kepercayaan publik terhadap penyelenggara layanan digital nasional.

Mengacu pada teori pertanggungjawaban hukum dan UU PDP, mekanisme pertanggungjawaban yang harus dijalankan oleh Telkomsel atas kebocoran data pengguna IndiHome mencakup tanggung jawab pidana, perdata, dan administratif. Tindakan Telkomsel yang tidak transparan, tidak responsif, dan tidak melakukan perbaikan sistem secara menyeluruh menunjukkan bahwa kewajiban hukum sebagaimana diamanatkan oleh UU PDP belum sepenuhnya dijalankan. Oleh karena itu, diperlukan penguatan pengawasan hukum, pemberian sanksi tegas, serta penyusunan sistem kompensasi yang adil bagi korban kebocoran data. Dalam hal ini, kehadiran negara melalui otoritas pengawas seperti Kementerian Komunikasi dan Informatika (Kominfo) dan Badan Siber dan Sandi Negara (BSSN) menjadi sangat penting untuk memastikan adanya penegakan hukum yang adil, tegas, dan berpihak kepada hak-hak digital warga negara.

4. Penutup

Praktik *e-commerce* di Indonesia telah berkembang pesat seiring dengan meningkatnya adopsi teknologi dan jumlah pengguna internet. Meskipun sektor ini menawarkan kemudahan dan aksesibilitas yang luas, isu perlindungan data pribadi tetap menjadi tantangan krusial yang memerlukan perhatian serius dari berbagai pihak. Kehadiran

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan landasan hukum yang kuat dan komprehensif—meliputi pengaturan pengumpulan, pemrosesan, penyimpanan, penghapusan data, hingga kepastian hak-hak konsumen di era digital. Namun, efektivitas regulasi ini sangat bergantung pada implementasi yang konsisten serta komitmen kolektif antara pemerintah, pelaku industri, dan masyarakat. Melalui sinergi yang kuat dan peningkatan kepatuhan hukum, ekosistem *e-commerce* yang aman, tepercaya, dan optimal dalam melindungi privasi konsumen dapat terwujud, sehingga bermuara pada penguatan kepercayaan publik dalam bertransaksi secara elektronik.

Referensi

- Anindya, R. P., & Subiyanto, A. E. (2025). Tanggung Jawab Platform Tokopedia dalam Kasus Kebocoran Data Menurut Undang-Undang tentang Perlindungan Data Pribadi. *Journal of Artificial Intelligence and Digital Business (RIGGS)*, 4(3), 89.
- Ardika, I. W. C. (2025). Tinjauan Hukum terhadap Perlindungan Data Pribadi di Era Digital: Kasus Kebocoran Data Pengguna Layanan E-Commerce. *Indonesian Journal of Law and Justice*, 2(3), 79.
- Fista, Y. L., Machmud, A., & Suartini. (2023). Perlindungan Hukum Konsumen Dalam Transaksi E-commerce Ditinjau dari Perspektif Undang-Undang Perlindungan Konsumen. *Jurnal Binamulia Hukum*, 12(1), 178.
- Halizah, E., & dkk. (2025). Analisis Pelanggaran Etika Profesi TI dalam Kebocoran Data 279 Juta Pengguna Indihome: Studi Kasus Tanggung Jawab Perlindungan Data Pribadi. *TEKNOBIS: Teknologi, Bisnis Dan Pendidikan*, 3(2), 281.
- Hasian, D. P., & Fitria, A. (2025). Pertanggung Jawaban Telkomsel Atas Kebocoran Rahasia Data Pribadi Pengguna Indihome. *Arus Jurnal Sosial Dan Humaniora (AJSH)*, 5(2), 80.
- Milafebina, R., & Lesmana, I. P. (2023). Perlindungan Data Pribadi terhadap Kebocoran Data Pelanggan E-commerce di Indonesia. *Jurnal Tana Mana*, 4(1), 101.
- Novel, S., & Subiyanto, A. E. (2025). Perlindungan Hukum terhadap Data Pribadi Konsumen dalam Tindak Pidana Phishing pada Jasa Layanan E-Commerce Tokopedia. *Jurnal Pendidikan Tambusai*, 9(2), 7.
- Saragih, A. E., Bagaskara, M. F., & Mulyadi. (2023). Perlindungan Hukum Terhadap Konsumen Dalam Transaksi E-Commerce. *Jurnal Kajian Hukum Dan Pendidikan Kewarganegaraan*, 2(2), 50.
- Sobirin, L. A., & Choeriyah, P. U. (2024). Perlindungan Hukum Terhadap Konsumen Dalam Transaksi E-Commerce Ditinjau Dari Undang-Undang Perlindungan Konsumen. *Jurnal Binamulia Hukum*, 7(1), 26.
- Sutrisna, C. (2021). Aspek Hukum Perlindungan Data Pribadi dan Kondisi Darurat Kebocoran atas Data Pribadi di Indonesia. *Wacana Paramarta Jurnal Ilmu Hukum*, 5(2), 30.
