Jurnal Hukum & Pembangunan Masyarakat

Vol. 17 No. 12, Desember 2025

TANGGUNG JAWAB PELAKU USAHA TERHADAP KEBOCORAN DATA PRIBADI KONSUMEN DALAM TRANSAKSI ELEKTRONIK DI INDONESIA

Maetza Kirana Azzahra[1], Nourma Dewi[2], Firstnandiar Glica Aini[3]
Universitas Islam Batik Surakarta
email: kiranamaetza@gmail.com[1], nourmadewi03@gmail.com[2], firstnandiar@gmail.com[4]

Abstrak

Globalisasi dan perkembangan teknologi digital telah mempercepat pertumbuhan e-commerce di Indonesia, yang sekaligus meningkatkan intensitas pertukaran data pribadi konsumen pada platform daring. Kondisi ini menghadirkan risiko pelanggaran data yang semakin besar, terutama ketika sistem keamanan platform tidak mampu melindungi informasi sensitif pengguna. Penelitian ini bertujuan menganalisis efektivitas kerangka hukum perlindungan data pribadi dalam menjamin keamanan data konsumen serta mengkaji bentuk tanggung jawab pelaku usaha terhadap insiden kebocoran data dalam sektor e-commerce. Melalui metode penelitian hukum normatif dengan pendekatan peraturan perundang-undangan serta analisis kasus, ditemukan bahwa regulasi yang berlaku saat ini belum sepenuhnya memberikan perlindungan yang memadai. Kelemahan utama terletak pada belum jelasnya pembagian tanggung jawab antara pengendali dan pemroses data, keterlambatan pembentukan Badan Perlindungan Data Pribadi (BPDP) sebagai otoritas pengawasan, serta pengaturan sanksi yang belum memberikan efek jera. Selain itu, kewajiban pelaku usaha dalam memberikan perlindungan dan pemulihan bagi konsumen juga belum optimal. Kasus kebocoran data di Bukalapak dan Tokopedia menunjukkan bahwa respons pelaku usaha lebih berfokus pada peningkatan sistem keamanan tanpa memberikan kompensasi langsung kepada konsumen yang dirugikan. Hal ini menegaskan perlunya penguatan regulasi melalui implementasi efektif Undang-Undang Perlindungan Data Pribadi, termasuk mekanisme penegakan hukum dan standar keamanan yang lebih ketat. Reformasi ini penting untuk memastikan bahwa hak privasi konsumen terlindungi secara utuh di tengah ekosistem digital yang terus berkembang.

Kata Kunci: Tanggung Jawab, Pelaku Usaha, Pelanggaran, Data Pribadi.

ABSTRACT

Globalization and rapid technological advancements have accelerated the growth of e-commerce in Indonesia, resulting in an increasing volume of personal data exchanged on digital platforms. This condition heightens the risk of data breaches, especially when platform security systems fail to adequately safeguard users' sensitive information. This study aims to analyze the effectiveness of Indonesia's personal data protection regulations in ensuring consumer data security and to examine the responsibilities of business actors in addressing data breaches within the e-commerce sector. Using a normative legal research method with legislative and case-study approaches, the findings show that the current regulatory framework does not yet fully protect consumers. Major weaknesses include the lack of clear delineation of responsibilities between data controllers and processors, the absence of the Personal Data Protection Authority (BPDP) as an independent supervisory body, and unclear prioritization of sanctions capable of providing deterrent effects. Furthermore, business entities' obligations to provide protection and remedies for affected consumers remain suboptimal. Data breach cases involving Bukalapak and Tokopedia demonstrate that business responses are mostly limited to improving security mechanisms without offering compensation to harmed consumers. These gaps emphasize the need to strengthen the regulatory framework through effective implementation of the Personal Data Protection Law, including robust enforcement mechanisms and stricter security standards. Such reforms are crucial to ensuring that consumer privacy rights are fully protected within Indonesia's rapidly evolving digital ecosystem.

Keywodds: *Absolute Jurisdiction, Administrative Court, Merger Theory, Management Of State Receivables.*

PENDAHULUAN

Perkembangan teknologi digital di Indonesia telah mengubah berbagai aspek kehidupan, terutama dalam penggunaan dan pengelolaan data pribadi. Di era digital ini, data pribadi konsumen menjadi aset yang sangat penting, tidak hanya bagi individu tetapi juga bagi perusahaan yang memanfaatkan data tersebut untuk berbagai keperluan, seperti personalisasi layanan, iklan, hingga analisis perilaku konsumen. Sektor-sektor seperti e-commerce, media sosial, dan layanan keuangan digital merupakan contoh utama yang memanfaatkan data pribadi pengguna dalam jumlah besar. Penggunaan teknologi digital pada sektor-sektor ini memerlukan akses yang luas terhadap data pribadi, yang mencakup informasi sensitif seperti alamat, nomor telepon, nomor kartu kredit, dan bahkan data biometrik.

Di sektor e-commerce, misalnya platform seperti Shopee, Tokopedia, dan Lazada memanfaatkan data pribadi pengguna untuk mempermudah proses transaksi, meningkatkan pengalaman belanja, serta menyediakan rekomendasi produk yang sesuai dengan preferensi konsumen. Namun, di balik kenyamanan ini, terdapat risiko kebocoran data yang mengancam keamanan konsumen. Kasus kebocoran data yang melibatkan platform e-commerce menunjukkan bahwa semakin banyak data yang disimpan, semakin tinggi risiko pencurian dan penyalahgunaan informasi oleh pihak yang tidak bertanggung jawab. Kebocoran data pada Tokopedia yang memengaruhi 91 juta pengguna pada tahun 2020 adalah contoh nyata betapa rentannya sistem keamanan digital dalam melindungi data pribadi pengguna.

Tidak hanya e-commerce, platform media sosial juga menghadapi tantangan serupa. Facebook, Instagram, TikTok, dan Twitter mengumpulkan data pribadi penggunanya, termasuk data lokasi, riwayat aktivitas online, hingga preferensi konten. Data ini kemudian digunakan untuk kepentingan personalisasi iklan dan interaksi pengguna. Meski personalisasi ini mempermudah pengguna untuk mendapatkan konten yang sesuai dengan minat mereka, risiko kebocoran data tetap menghantui. Pengguna sering kali tidak menyadari sejauh mana data mereka digunakan dan bagaimana perusahaan tersebut melindungi privasi mereka. Kasus kebocoran data pada Facebook pada tahun 2018 yang memengaruhi jutaan pengguna di seluruh dunia, termasuk di Indonesia, menjadi bukti bahwa penggunaan data pribadi di platform media sosial perlu diatur secara ketat.

Lebih lanjut, layanan keuangan digital seperti mobile banking, fintech, dan dompet elektronik (e-wallet) juga sangat bergantung pada data pribadi. Aplikasi seperti OVO, Dana, dan BCA Mobile mengharuskan pengguna untuk memberikan data sensitif, termasuk nomor rekening, informasi keuangan, dan data biometrik. Meski layanan ini memberikan kemudahan dalam bertransaksi, risiko penyalahgunaan data pribadi tetap tinggi. Kasus kebocoran data di sektor perbankan, seperti yang terjadi pada Bank Syariah Indonesia (BSI) di tahun 2023, di mana 1,5 TB data nasabah bocor dan dijual di situs gelap, menyoroti pentingnya proteksi lebih baik terhadap data pribadi konsumen di sektor ini.

Statistik pengguna internet di Indonesia juga menunjukkan pertumbuhan pesat dalam jumlah pengguna, yang menambah kompleksitas permasalahan privasi dan perlindungan data pribadi. Menurut laporan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), jumlah pengguna internet di Indonesia mencapai 221 juta jiwa pada tahun 2024, atau sekitar 79,5% dari total populasi. Angka ini meningkat dari tahun sebelumnya, di mana pada tahun 2023 jumlah pengguna internet mencapai 215 juta jiwa. Tingginya jumlah pengguna internet ini menandakan semakin besarnya potensi risiko kebocoran data pribadi, terutama di wilayah urban yang memiliki penetrasi internet lebih tinggi dibandingkan dengan wilayah rural.

Dalam beberapa tahun terakhir, Indonesia telah menghadapi berbagai kasus kebocoran data yang cukup signifikan. Beberapa contoh kasus tersebut antara lain kebocoran data BPJS Kesehatan pada tahun 2021 yang melibatkan data pribadi 279 juta peserta, kebocoran data

Tokopedia pada tahun 2020 yang berdampak pada 91 juta pengguna, serta kebocoran data Bank Syariah Indonesia (BSI) pada tahun 2023. Semua kasus ini menyoroti betapa rentannya sistem keamanan data di Indonesia terhadap ancaman siber, serta urgensi bagi pemerintah untuk memberikan perlindungan yang lebih kuat terhadap data pribadi konsumen.

Berangkat dari berbagai persoalan yang telah dipaparkan sebelumnya, terlihat bahwa perkembangan teknologi digital yang begitu pesat tidak hanya membawa kemudahan, tetapi juga menghadirkan tantangan serius bagi perlindungan data pribadi konsumen. Kondisi ini menunjukkan bahwa pengelolaan data pribadi bukan lagi isu teknis semata, melainkan telah berkembang menjadi persoalan hukum, etika, dan tata kelola yang kompleks. Di tengah meningkatnya penggunaan teknologi digital dalam berbagai aspek kehidupan sehari-hari mulai dari aktivitas ekonomi, interaksi sosial, hingga layanan public perlindungan terhadap data pribadi menjadi kebutuhan fundamental yang harus dijamin keberadaannya. Namun, hingga kini kerangka regulasi dan penegakan hukum terkait perlindungan data pribadi di Indonesia masih menghadapi berbagai kendala, khususnya dalam konteks tanggung jawab pelaku usaha ketika terjadi kebocoran data yang merugikan konsumen.

Pelaku usaha digital, baik dalam bentuk perusahaan e-commerce, platform media sosial, maupun penyelenggara layanan keuangan digital, pada dasarnya memiliki kewajiban hukum dan moral untuk menjaga keamanan data pribadi konsumen. Namun, banyak kasus kebocoran data yang terjadi menunjukkan bahwa kewajiban tersebut belum sepenuhnya dilaksanakan dengan baik. Dalam banyak kasus, pelaku usaha sering kali menempatkan keamanan data sebagai prioritas sekunder, sementara fokus utama lebih diarahkan pada pengembangan bisnis dan penguasaan pasar. Padahal, data pribadi merupakan aset sensitif yang rentan disalahgunakan, baik untuk kepentingan ekonomi, kriminal, maupun politik. Kurangnya transparansi perusahaan dalam mengelola data, minimnya pemberitahuan kepada pengguna ketika terjadi insiden kebocoran, serta tidak adanya kompensasi memadai kepada konsumen menjadi masalah yang kerap muncul dalam praktik.

Situasi ini diperburuk dengan lemahnya penegakan hukum dan belum optimalnya implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Meskipun UU PDP telah menjadi tonggak penting dalam upaya memperkuat perlindungan data pribadi di Indonesia, keberadaannya masih menghadapi tantangan implementasi, seperti kurangnya kesiapan infrastruktur, koordinasi antarinstansi, serta mekanisme sanksi yang belum sepenuhnya berjalan efektif. Banyak pelaku usaha, terutama perusahaan kecil dan menengah, belum memahami secara menyeluruh kewajibannya dalam mengelola data pribadi konsumen, seperti kewajiban melakukan *data protection impact assessment*, menerapkan prinsip *privacy by design*, dan menyediakan sistem keamanan digital yang memadai. Sementara itu, konsumen belum memiliki literasi digital yang kuat untuk memahami hak-haknya dalam mengontrol, mengakses, dan meminta penghapusan data pribadinya.

Di sisi lain, peningkatan kasus kebocoran data dalam beberapa tahun terakhir memperlihatkan bahwa ancaman terhadap keamanan data pribadi kini tidak hanya berasal dari pihak luar melalui serangan siber (*cyber attack*), tetapi juga dari kelalaian internal perusahaan. Banyak insiden kebocoran terjadi karena lemahnya standar keamanan, penggunaan sistem yang tidak diperbarui, hingga kecerobohan sumber daya manusia dalam menangani informasi sensitif. Hal ini membuat banyak konsumen kehilangan rasa percaya terhadap pelaku usaha digital dan bahkan membatasi penggunaan layanan digital tertentu karena khawatir akan risiko kebocoran data.

Dari perspektif hukum, pertanyaan besar yang muncul adalah sejauh mana pelaku usaha bertanggung jawab atas kerugian yang dialami konsumen akibat kebocoran data pribadi? Dalam konteks transaksi elektronik, pelaku usaha berkewajiban menjamin keamanan data pribadi berdasarkan prinsip kepatuhan pada etika bisnis, perlindungan konsumen, dan peraturan perundang-undangan. Ketika terjadi kebocoran data, pelaku usaha harus memberikan pemberitahuan segera kepada pemilik data, mengambil langkah mitigasi untuk mencegah kerugian lebih lanjut, serta menyediakan kompensasi jika terbukti lalai dalam memberikan perlindungan. Namun, praktik di lapangan menunjukkan banyak pelaku usaha yang mengabaikan kewajiban tersebut. Pengguna sering kali mengetahui kebocoran data dari media massa atau pihak ketiga, bukan dari perusahaan yang seharusnya bertanggung jawab memberikan informasi secara langsung. Selain itu, mekanisme penyelesaian sengketa antara konsumen dan pelaku usaha masih belum jelas, sehingga banyak konsumen tidak mendapatkan pemulihan yang layak.

Melihat kondisi tersebut, penelitian mengenai tanggung jawab pelaku usaha terhadap kebocoran data pribadi konsumen dalam transaksi elektronik menjadi sangat penting untuk dilakukan. Penelitian ini akan mengkaji sejauh mana norma hukum yang ada mampu memberikan perlindungan efektif, apa saja kelemahan dalam implementasinya, serta bagaimana upaya yang dapat dilakukan untuk memperkuat sistem perlindungan data pribadi di Indonesia. Penelitian ini juga bertujuan untuk memberikan gambaran mengenai pola tanggung jawab pelaku usaha, baik tanggung jawab hukum, administratif, maupun perdata, serta menganalisis bagaimana mekanisme pertanggungjawaban tersebut seharusnya ditegakkan untuk melindungi kepentingan konsumen.

Selain itu, penelitian ini penting untuk memberikan kontribusi akademik terhadap pengembangan literatur perlindungan data pribadi di era digital. Di tengah meningkatnya kebutuhan perlindungan data dan semakin kompleksnya pola interaksi digital, pemahaman mengenai aspek hukum perlindungan data menjadi sangat relevan. Penelitian ini akan membantu mengidentifikasi celah regulasi yang ada, sekaligus memberikan rekomendasi konkret untuk penyempurnaan kebijakan dan peningkatan kesadaran pelaku usaha dalam menerapkan standar keamanan data yang lebih baik.

Secara praktis, penelitian ini diharapkan mampu memberikan manfaat bagi pemerintah, pelaku usaha, dan masyarakat luas. Bagi pemerintah, hasil penelitian dapat menjadi dasar evaluasi terhadap efektivitas regulasi perlindungan data pribadi serta menjadi masukan dalam merancang kebijakan yang lebih komprehensif. Bagi pelaku usaha, penelitian ini dapat menjadi pedoman dalam memahami dan melaksanakan kewajiban mereka dalam mengelola data pribadi konsumen secara aman dan bertanggung jawab. Sedangkan bagi konsumen, penelitian ini memberikan pemahaman mengenai hak-hak mereka dan bagaimana memperjuangkan perlindungan yang lebih baik atas data pribadi yang mereka serahkan kepada pelaku usaha.

Dengan demikian, penelitian berjudul “Tanggung Jawab Pelaku Usaha Terhadap Kebocoran Data Pribadi Konsumen Dalam Transaksi Elektronik Di Indonesia” bukan hanya relevan secara teoritis, tetapi juga memiliki urgensi praktis dalam menjawab tantangan nyata yang dihadapi Indonesia dalam era digital. Melalui penelitian ini, diharapkan muncul deskripsi

yang komprehensif mengenai permasalahan, tanggung jawab hukum, dan solusi strategis untuk memperkuat perlindungan data pribadi di tengah pesatnya perkembangan teknologi digital.

METODE PENELITIAN

Jenis penelitian yang digunakan adalah penelitian hukum normatif. Penelitian hukum normatif dilakukan dengan cara mengkaji asas-asas hukum dan peraturan perundang-undangan.

HASIL DAN PEMBAHASAN

1. Pengaturan hukum mengenai pelindungan data pribadi konsumen dalam transaksi elektronik di Indonesia

Perlindungan data pribadi sering kali terkait erat dengan konsep privasi, sebagaimana yang pertama kali didefinisikan oleh Allan Westin. Ia menggambarkan privasi sebagai hak individu, kelompok, atau institusi untuk menentukan apakah informasi tentang diri mereka boleh dibagikan kepada pihak lain atau tidak. Oleh karena itu, definisi ini dikenal sebagai information privacy, karena fokusnya pada data pribadi. Di Indonesia, data pribadi seharusnya dilindungi secara hukum oleh pemerintah, mengingat hal ini merupakan bagian dari hak asasi manusia warga negara. Bahkan, Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 secara eksplisit mengakui hak atas perlindungan diri pribadi dalam Pasal 28 huruf G.

Dengan landasan konstitusional ini, yang menempatkan data pribadi sebagai hak asasi manusia, Indonesia telah menetapkan beberapa regulasi untuk melindungi data pribadi. Salah satunya adalah Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pasal 36 undang-undang ini mewajibkan pengendali data pribadi untuk menjaga kerahasiaannya. Selain itu, Pasal 38 menekankan kewajiban pengendali untuk melindungi data dari pemrosesan yang tidak sah. Regulasi lain yang relevan adalah Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Pasal 15 ayat (1) menyatakan bahwa setiap penyelenggara sistem elektronik harus mengoperasikan sistemnya secara andal dan aman, serta bertanggung jawab atas kelancaran operasinya. Tak kalah penting, Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik (PP PMSE) juga turut berperan. Pasal 58 dalam peraturan ini mengharuskan setiap pelaku usaha yang memperoleh data pribadi untuk bertindak sebagai pengemban amanat dalam menyimpan dan mengelola data tersebut sesuai dengan ketentuan hukum yang berlaku. Untuk menegakkan perlindungan ini, diperlukan lembaga pengawas yang diatur dalam Undang-Undang Perlindungan Data Pribadi, khususnya Pasal 58 hingga 60. Lembaga ini diberi wewenang untuk merumuskan kebijakan, mengawasi kepatuhan pengendali data, dan menjatuhkan sanksi administratif atas pelanggaran.

Namun, menurut pernyataan Dirjen Aplikasi Informatika Kominfo, Semuel Abrijani, lembaga ini baru akan terbentuk dan beroperasi pada Oktober 2024. Sementara itu, penyebab kebocoran data pribadi oleh pelaku usaha sering kali meliputi serangan siber, phishing, kesalahan manusia, dan pencurian data secara langsung. Berdasarkan teori perlindungan hukum, yang bertujuan memberikan pengayoman atas hak individu di hadapan hukum dan melindungi hak asasi manusia dari kerugian yang disebabkan pihak lain, Indonesia sebenarnya telah memiliki sejumlah regulasi terkait perlindungan data pribadi. Meski demikian, dalam praktiknya, aturan-aturan ini belum sepenuhnya mampu melindungi kepentingan dan hak individu. Beberapa masalah utama yang muncul antara lain: pertama, ketidakjelasan mengenai tanggung jawab ganti rugi, di mana Undang-Undang Perlindungan Data Pribadi tidak merinci bentuk tanggung jawab atau kondisi yang memungkinkan penolakan atau pemberian ganti rugi kepada subjek data. Kedua, lembaga perlindungan data pribadi yang hingga kini belum terbentuk.

Ketiga, risiko perselisihan yang berujung pada arbitrase internasional dengan kekuatan hukum yang lebih kuat. Keempat, tidak adanya pemisahan tegas antara sanksi administratif, perdata, atau pidana dalam penyelesaian sengketa data pribadi. Akibatnya, materi Undang-Undang Perlindungan Data Pribadi terlihat belum lengkap, sehingga belum dapat sepenuhnya mengakomodasi kepentingan konsumen. Hal ini tercermin dari masih tingginya kasus kebocoran data pribadi di Indonesia, yang menunjukkan efektivitas undang-undang ini masih terbatas dalam penerapan sehari-hari.

Selain berbagai persoalan tersebut, kompleksitas pengaturan hukum mengenai perlindungan data pribadi dalam transaksi elektronik di Indonesia juga dipengaruhi oleh karakteristik perkembangan teknologi digital yang sangat cepat. Regulasi yang telah dibentuk sering kali tidak mampu mengimbangi dinamika ancaman keamanan siber yang terus berevolusi, sehingga mekanisme perlindungan yang tersedia belum sepenuhnya efektif mencegah kebocoran data. Hal ini menegaskan bahwa perlindungan data pribadi bukan hanya soal tersedianya perangkat hukum, tetapi juga menyangkut kesiapan institusi, infrastruktur keamanan, dan kepatuhan pelaku usaha dalam menerapkan standar perlindungan data yang ketat. Tanpa dukungan ekosistem yang kuat, regulasi hanya akan menjadi norma tertulis yang sulit ditegakkan secara optimal.

UU Perlindungan Data Pribadi (UU PDP) memang menjadi tonggak penting dalam perkembangan hukum data di Indonesia karena mengatur aspek-aspek fundamental seperti kategori data pribadi, hak subjek data, kewajiban pengendali dan prosesor data, mekanisme pemrosesan data, hingga sanksi administratif dan pidana. Namun demikian, sejumlah pasal dalam UU ini masih memerlukan aturan turunan agar dapat diimplementasikan secara efektif. Misalnya, ketentuan mengenai *data breach notification* yang mengharuskan pengendali data memberitahukan insiden kebocoran paling lambat tiga hari setelah ditemukannya pelanggaran. Pada praktiknya, belum tersedia pedoman teknis mengenai tata cara pelaporan, bentuk notifikasi, maupun standar bukti yang harus disampaikan. Kekosongan pengaturan ini berpotensi menimbulkan interpretasi berbeda-beda di antara pelaku usaha, bahkan memungkinkan adanya kelalaian atau penghindaran tanggung jawab dengan alasan ambigu regulasi.

Aspek penting lainnya adalah mekanisme pertanggungjawaban hukum (liability) yang belum diatur secara rinci. UU PDP memang menyebutkan kewajiban pemberian ganti rugi, namun tidak menjelaskan besaran minimal kompensasi, kriteria kerugian yang dapat diakui, maupun batas tanggung jawab pelaku usaha dalam kondisi tertentu, misalnya ketika kebocoran data terjadi akibat *force majeure* atau tindakan kriminal pihak ketiga yang tidak dapat dicegah. Hal ini menyebabkan ketidakpastian hukum bagi konsumen yang menjadi korban kebocoran data, sekaligus memberikan celah bagi pelaku usaha untuk menghindari pertanggungjawaban dengan menyatakan bahwa insiden terjadi di luar kendali mereka.

Ketiadaan lembaga pengawas independen yang seharusnya dibentuk berdasarkan UU PDP juga menjadi hambatan besar dalam penerapan perlindungan data. Selama lembaga ini belum beroperasi, fungsi pengawasan masih dijalankan oleh Kementerian Komunikasi dan Informatika (Kominfo) yang kapasitasnya kerap diragukan dalam hal independensi dan efektivitas. Banyak kritik muncul karena Kominfo sekaligus berperan sebagai regulator, pengawas, sekaligus penegak kebijakan, sehingga menimbulkan kekhawatiran konflik kepentingan. Belum adanya otoritas perlindungan data yang berdiri sendiri juga membuat proses penegakan hukum berjalan lambat, terutama ketika terjadi insiden kebocoran data berskala besar. Dalam banyak kasus, pelaku usaha hanya diberi teguran atau sanksi administratif yang relatif ringan, tanpa kewajiban untuk memulihkan kerugian konsumen secara proporsional.

Selain faktor regulasi, tantangan lain terletak pada rendahnya literasi digital masyarakat. Banyak konsumen yang belum memahami hak-haknya sebagai pemilik data pribadi, sehingga tidak mampu menuntut pertanggungjawaban ketika menjadi korban kebocoran data. Sebagian besar pengguna aplikasi digital menerima syarat dan ketentuan (*terms and conditions*) tanpa membacanya, sehingga tidak mengetahui bagaimana data mereka dikumpulkan, digunakan, atau dibagikan. Rendahnya kesadaran ini semakin diperparah oleh budaya digital yang cenderung permisif, di mana masyarakat sering kali tidak berhati-hati dalam membagikan informasi pribadi seperti nomor identitas, foto, lokasi, dan data sensitif lainnya di berbagai platform digital. Kondisi ini menciptakan celah besar bagi pelaku kejahatan siber untuk mengeksploitasi data pribadi secara ilegal.

Di sisi pelaku usaha, kepatuhan terhadap standar keamanan data juga masih sangat bervariasi. Perusahaan besar mungkin telah menerapkan sistem keamanan canggih, namun pelaku usaha kecil dan menengah (UMKM digital) sering kali tidak memiliki kapasitas teknis maupun finansial untuk menerapkan standar keamanan sesuai ketentuan. Mereka cenderung memprioritaskan pengembangan bisnis dibandingkan investasi pada infrastruktur keamanan. Padahal, UU PDP tidak membedakan tanggung jawab berdasarkan ukuran perusahaan: setiap pengendali data, tanpa kecuali, wajib menyediakan keamanan yang memadai. Hal ini berpotensi menjadi beban besar bagi pelaku usaha kecil, sekaligus menempatkan konsumen pada risiko tinggi.

Tantangan lainnya adalah tumpang tindih regulasi dan koordinasi antarinstansi. Selain UU PDP dan UU ITE, terdapat berbagai aturan sektoral yang mengatur perlindungan data di bidang perbankan, kesehatan, perasuransian, dan perdagangan. Namun, banyak aturan ini tidak terintegrasi, sehingga menimbulkan dualisme atau bahkan konflik pengaturan. Misalnya, sektor perbankan mewajibkan kerahasiaan data nasabah berdasarkan Undang-Undang Perbankan, tetapi ketika terjadi kebocoran, proses pelaporan harus melewati sejumlah prosedur lain yang diatur dalam UU PDP dan UU ITE. Ketidakharmonisan regulasi ini membuat proses penanganan insiden kebocoran data sering kali berjalan lambat dan tidak efektif.

Indonesia juga menghadapi tantangan besar dalam aspek penegakan hukum siber. Meskipun berbagai regulasi telah mengatur sanksi pidana bagi pelaku kebocoran data, penegakan hukumnya sering kali terbentur keterbatasan sumber daya aparat penegak hukum, baik dari segi jumlah personel yang ahli di bidang digital forensik maupun fasilitas pendukung investigasi. Di sisi lain, kejahatan siber bersifat lintas negara, sehingga penanganannya memerlukan kerja sama internasional yang tidak selalu mudah dilakukan.

Secara keseluruhan, dapat disimpulkan bahwa meskipun Indonesia telah memiliki perangkat hukum yang cukup untuk melindungi data pribadi konsumen dalam transaksi elektronik, efektivitas implementasinya masih jauh dari optimal. Tantangan yang ada mencakup ketidaklengkapan aturan teknis, belum terbentuknya otoritas pengawas, rendahnya literasi digital masyarakat, kapasitas pelaku usaha yang belum merata, serta lemahnya koordinasi dan penegakan hukum. Oleh karena itu, diperlukan langkah-langkah strategis untuk memperkuat perlindungan data pribadi, seperti percepatan pembentukan lembaga perlindungan data, harmonisasi regulasi sektoral, peningkatan kesadaran publik, serta pengawasan ketat terhadap kepatuhan pelaku usaha. Tanpa upaya serius dan terstruktur, tujuan untuk menciptakan ekosistem transaksi elektronik yang aman dan terpercaya akan sulit terwujud secara menyeluruh.

2. Bentuk tanggung jawab hukum pelaku usaha terhadap kebocoran data pribadi konsumen dalam transaksi elektronik

Konsep tanggung jawab hukum erat kaitannya dengan kewajiban hukum, di mana seseorang dianggap bertanggung jawab atas tindakan tertentu. Hans Kelsen, dalam teorinya, menjelaskan bahwa tanggung jawab hukum berarti seseorang memikul beban sanksi atas perbuatan yang bertentangan dengan hukum.

Beberapa regulasi telah mengatur tanggung jawab pelaku usaha atas kebocoran data konsumen. Misalnya, Pasal 47 Undang-Undang Perlindungan Data Pribadi mewajibkan

pengendali data pribadi untuk bertanggung jawab atas pemrosesan data dan menunjukkan pertanggungjawaban dalam memenuhi prinsip-prinsip perlindungan. Namun, dalam kenyataan, tanggung jawab ini belum sepenuhnya dijalankan di Indonesia. Berikut beberapa kasus yang menggambarkan hal tersebut:

1. Kasus Bukalapak

Kasus kebocoran data Bukalapak pada 2019 menjadi salah satu insiden awal yang menunjukkan lemahnya sistem keamanan siber pelaku usaha digital di Indonesia. Sebanyak 13 juta data pengguna dicuri oleh peretas internasional, menunjukkan bahwa perusahaan besar sekalipun tidak kebal dari ancaman serangan siber. Jenis data yang bocor seperti email, nomor ponsel, alamat, dan tanggal lahir merupakan data pribadi umum, namun tetap berpotensi dimanfaatkan untuk kejahatan sosial engineering, pencurian identitas, dan penipuan daring.

Dari perspektif tanggung jawab hukum, pernyataan CEO Bukalapak bahwa perusahaan telah menerapkan sistem perlindungan berlapis belum mencerminkan pemenuhan kewajiban sebagaimana diatur UU PDP. Pasal 47 UU PDP menegaskan bahwa pengendali data wajib memastikan prinsip keamanan data, termasuk menjaga agar tidak terjadi akses ilegal. Pernyataan bahwa sistem sudah berlapis tidak cukup apabila terbukti data tetap berhasil diretas. Dalam hukum perlindungan data, tanggung jawab pengendali data bersifat *strict liability*, yaitu tetap bertanggung jawab meskipun serangan terjadi oleh pihak ketiga.

Respons Bukalapak juga tidak mencakup pemberian ganti rugi kepada konsumen. Padahal, berdasarkan Pasal 12–14 UU PDP, subjek data memiliki hak atas kompensasi jika data mereka disalahgunakan. Tidak ada kejelasan mekanisme kompensasi, tidak ada audit independen, dan tidak ada jaminan bahwa data yang bocor tidak akan digunakan kembali di masa depan. Perusahaan hanya melakukan pembaruan sistem keamanan, memberi imbauan kepada pengguna, dan bekerja sama dengan pihak berwenang, namun tidak ada bentuk pemulihan kerugian.

Hal ini mencerminkan paradigma lama pelaku usaha digital yang menganggap kebocoran data sebagai isu teknis, bukan isu hukum yang melibatkan tanggung jawab perdata kepada konsumen. Ketiadaan tindakan kompensasi menunjukkan bahwa norma perlindungan data tidak dianggap mengikat secara kuat. Jika dianalisis dengan teori tanggung jawab hukum Hans Kelsen, Bukalapak tidak benar-benar memikul beban sanksi atau konsekuensi sebagaimana diamanatkan oleh norma hukum, sehingga tidak ada efek jera maupun standar perlindungan yang meningkat secara signifikan.

2. Kasus Tokopedia

Kebocoran data Tokopedia pada 2020 menjadi kasus terbesar di Indonesia, melibatkan 91 juta pengguna dan lebih dari 7 juta merchant. Besarnya jumlah data yang bocor menunjukkan risiko tinggi yang dihadapi pengguna ketika mempercayakan data kepada platform e-commerce raksasa. Data yang bocor termasuk user ID, tanggal lahir, nomor telepon, dan kata sandi terenkripsi, yang memiliki dampak sangat serius terhadap keamanan akun keuangan dan identitas digital pengguna.

Dalam konteks tanggung jawab pelaku usaha, respons Tokopedia dinilai tidak memadai. Pengumuman melalui email yang hanya berisi permintaan maaf, pemberitahuan investigasi, dan imbauan penggantian kata sandi tidak mencerminkan bentuk tanggung jawab hukum yang proporsional. Konsumen tidak menerima ganti rugi, padahal risiko kerugian yang timbul dari penyalahgunaan data sangat tinggi. Sampai hari ini, tidak ada laporan bahwa Tokopedia memberikan kompensasi finansial atau dukungan hukum bagi pengguna yang dirugikan.

Berdasarkan ketentuan UU PDP, pengendali data wajib:

a. memberitahu subjek data secara lengkap mengenai jenis data yang bocor,
b. menjelaskan risiko yang mungkin dihadapi,
c. memberikan langkah mitigasi yang jelas,
d. memberikan akses penyelesaian sengketa,
e. dan menyediakan kompensasi apabila terbukti lalai.

Tokopedia hanya memenuhi sebagian kecil dari kewajiban tersebut. Selain itu, mereka tidak pernah mempublikasikan hasil audit independen yang membuktikan apakah sistem keamanan mereka sebelumnya memang telah sesuai standar. Hal ini bertentangan dengan

prinsip *accountability* dalam Pasal 3 UU PDP. Tindakan Tokopedia yang tidak memberikan ganti rugi menunjukkan adanya kelemahan regulasi sebelum hadirnya UU PDP. Polisi dan Kominfo pun hanya sebatas memberikan imbauan, tanpa menjatuhkan denda atau sanksi. Dengan demikian, kasus Tokopedia menjadi contoh nyata ketidakseimbangan kekuasaan antara konsumen dan perusahaan digital raksasa, di mana perusahaan tidak menanggung konsekuensi hukum meskipun kerugiannya sangat besar bagi publik.

3. Kasus Denny Siregar

Kebocoran data pribadi Denny Siregar terjadi pada 5 Juli 2020, ketika gambar berisi data pribadinya tersebar di akun Twitter @Opposite6891. Data tersebut diperoleh dari seorang karyawan outsourcing Telkomsel di Surabaya, dan mencakup nama, alamat, NIK, KK, IMEI, OS, serta jenis perangkat. Denny Siregar kemudian mengajukan tuntutan kepada Telkomsel.

Kebocoran data pribadi ini memiliki dampak serius bagi konsumen, seperti risiko menjadi korban penipuan dan phishing, menerima spam berlebihan, penyalahgunaan identitas, serta pembobolan rekening bank. Bagi perusahaan, dampaknya meliputi kehilangan reputasi dan kepercayaan pelanggan, sanksi dan denda, serta biaya besar untuk pemulihan. Dari sudut pandang teori tanggung jawab hukum, yang menilai kemampuan subjek hukum untuk menanggung biaya atau kerugian, bentuk tanggung jawab yang diberikan oleh Bukalapak dan Tokopedia dalam kasus-kasus ini belum memadai. Tanggung jawab mereka terbatas pada pernyataan kesadaran dan upaya perbaikan sistem, tanpa memberikan ganti rugi kepada konsumen. Jika merujuk pada teori hukum pidana minimalis Douglas Husak, yang menekankan bahwa kriminalisasi harus menjadi pilihan terakhir ketika mekanisme lain gagal, maka masalah kebocoran data pribadi sebaiknya diselesaikan melalui jalur perdata atau privat, bukan pidana, selama masih memungkinkan.

Kebocoran data Denny Siregar pada 2020 merupakan contoh lain yang memperlihatkan kelemahan perlindungan data pribadi oleh operator telekomunikasi. Kasus ini berbeda karena pelaku bukan peretas eksternal, melainkan karyawan outsourcing yang memiliki akses internal terhadap sistem Telkomsel. Data yang bocor bukan data umum, melainkan data sensitif seperti NIK, KK, IMEI, dan data perangkat, yang seharusnya mendapatkan perlindungan paling tinggi.

Dari sudut pandang tanggung jawab hukum, kasus ini menunjukkan adanya kelalaian dalam pengawasan internal (internal control). Pengendali data memiliki kewajiban memastikan bahwa hanya pihak yang berwenang (authorized personnel) yang dapat mengakses data pribadi pelanggan. Pelanggaran ini termasuk kategori insider threat, yang secara hukum tetap menjadi tanggung jawab penuh perusahaan sebagai pengendali data.

Tindakan Telkomsel yang meminta maaf dan memecat pelaku tidak cukup memenuhi standar tanggung jawab hukum. Seharusnya, Telkomsel menyediakan kompensasi serta jaminan perlindungan lanjutan kepada korban. Kebocoran data semacam ini dapat memicu risiko doxing, pembuntutan, dan pencurian identitas yang membahayakan keselamatan fisik seseorang, sehingga dampaknya jauh lebih besar dibanding kasus e-commerce.

KESIMPULAN

Dalam konteks pengaturan perlindungan data pribadi di Indonesia, meskipun sudah diatur melalui berbagai peraturan perundang-undangan, kenyataannya aturan tersebut belum sepenuhnya mampu melindungi hak-hak konsumen atau menjamin keamanan data pribadi mereka dalam transaksi perdagangan elektronik. Ada beberapa alas an dibalik hal ini. Pertama, Undang-Undang Perlindungan Data Pribadi tidak memberikan penjelasan lebih rinci mengenaik bentuk tanggung jawab pengendali data terhadap konsumen, termasuk kondisi-kondisi yang memungkinkan penolakan atau pemberian ganti rugi kepada subjek data pribadi. Kedua, lembaga khusus untuk Perlindungan Data Pribadi yang seharusnya terbentuk masih belum terealisasi hingga saat ini. Ketiga, undang-undang tersebut juga tidak secara tegas memisahkan apakah sanksi administrasi atau perdata harus didahulukan dalam menyelesaikan sengketa pengelolaan data pribadi, dibandingkan dengan sanksi pidana.

Sementara itu, tanggung jawab pelaku usaha telah diatur dalam Pasal 47 Undang-Undang Perlindungan Data Pribadi, yang menyatakan bahwa pengendali data bertanggung jawab atas pemrosesan data dan harus menunjukkan pertanggungjawaban berdasarkan prinsip-prinsip perlindungan data pribadi. Konsumen juga diberikan hak untuk menuntut ganti rugi kepada pengendali data sesuai Pasal 12. Namun, dalam praktiknya, pelaku usaha belum sepenuhnya memenuhi bentuk pertanggungjawaban seperti yang dipersyaratkan undang-undang. Misalnya, dalam kasus Bukalapak, tanggung jawab yang diberikan hanya berupa pernyataan bahwa sistem keamanan marketplace telah diperketat dan ditingkatkan. Begitu pula dengan Tokopedia, di mana mereka hanya memberitahukan konsumen tentang kebocoran data pribadi dan memperkuat sistem keamanan, tanpa memberikan kompensasi berupa ganti kerugian kepada konsumen.

Saran

Berdasarkan temuan-temuan tersebut, beberapa saran dapat diajukan untuk meningkatkan perlindungan data pribadi konsumen. Pertama, kepada pelaku usaha marketplace, diharapkan agar mereka lebih serius dalam memperketat, memperkuat, dan membangun sistem perlindungan data pribadi yang lebih aman, sehingga tidak mudah diretas atau disalahgunakan. Meskipun aturan perlindungan data sudah ada, masih sering terjadi kelalaian dari pihak pelaku usaha yang perlu diatasi.

Kedua, kepada pemerintah perlu dilakukan penguatan keamanan siber dengan fokus pada pengawasan khusus dan berkelanjutan terhadap perlindungan data pribadi konsumen. Selain itu, penting untuk mengadakan edukasi dan sosialisasi kepada konsumen serta pelaku usaha mengenai hak dan kewajiban mereka dalam konteks ini. Adapun kepada jajaran legislatif dan eksekutif pemerintah, diharapkan agar segera membentuk lembaga perlindungan data pribadi dan menyempurnakan Undang-Undang Perlindungan Data Pribadi yang ada, sehingga menjadi undang-undang yang lebih komprehensif. Tak kalah pentingnya, perlu dilakukan evaluasi terhadap regulasi terkait perlindungan data pribadi aga**r** tercipta keselarasan antar peraturan yang membahas isu ini.

DAFTAR PUSTAKA BUKU :

Hans Kelsen, sebagaimana diterjemahkan oleh Somardi, General Theory Of law and State , Teori Umum Hukum dan Negara, Dasar-Dasar Ilmu Hukum Normatif Sebagai Ilmu Hukum Deskriptif Empirik, (Jakarta: BEE Media Indonesia, 2007), hlm. 81

Kurniawan, A. (2021). Ethical Hacker–Menjadi Peretas yang Beretika. PENERBIT KBM INDONESIA.

Mangesti, Y. A., SH, M., Slamet Suhartono, S. H., Asmara, G. Y. P., & SH, M. (2021). Mengenal Audit Hukum (Legal Audit). CV. Cipta Mandiri Solusindo.

Rohendi, H. A. (2025). Hukum Bisnis Digital Regulasi, Etika, dan Perlindungan di Era Ekonomi Digital. PT KIMHSAFI ALUNG CIPTA.

Santoso, R. A., Pawitri, W., Mennita, R., Meliawati, R., Puspasari, M., Subagdja, A., ... & Huda, M. N. (2024). Fraud: definisi, strategi, dan tren masa depan. Azzia Karya

Bersama.
Sayidah, N., & Hartati, S. J. (2019). Akutansi forensik dan audit investigatif. Zifatama Jawara.
Titik Triwulan dan Shinta, Perlindungan Hukum Bagi Pasien, (Jakarta : Prestasi Pustaka, 2010), hlm.
48.
Zainal Asikin dan Amirudin, Pengantar Metode Penelitian Hukum, (JakartaL:Raja Grafindo Persada, 2004), hlm. 118.
JURNAL :
Kehista, Adisya Poeja, Achmad Fauzi, Annisa Tamara, Ivanida Putri, Nurul Afni Fauziah, Salma Klarissa, and Vivi Bunga Damayanti. "Analisis Keamanan Data Pribadi Pada Pengguna E- Commerce: Ancaman, Risiko, Strategi Kemanan (Literature Review)." Jurnal Ilmu Manajemen Terapan 4, no. 5 (2023): 625–32.
Kornelius Benus, Siti Mahmudah, dan Ery Agus Priyono, Perlindungan hukum terhadap Keamanan Data Konsumen Financial Technology di Indonesia, Jurnal ilmu Hukum, Vol.3 No.2, April, 2019, hlm 155.
SIMANJORANG, N. (2024). REKONSTRUKSI REGULASI PERTANGGUNGJAWABAN PIDANA PEMILIK MANFAAT (BENEFICIAL OWNERSHIP) DALAM PERSEROAN TERBATAS BERBASIS NILAI KEADILAN (Doctoral dissertation, Universitas Islam Sultan Agung Semarang).
Sinaga, J. A. D. (2025). TANGGUNG JAWAB HUKUM PERUSAHAAN TOKOPEDIA DALAM PERLINDUNGAN DATA KONSUMEN DI ERA DIGITAL MENURUT UNDANG-UNDANG NO 27 TAHUN 2022.
Wiraguna, S. A. (2025). Tanggung Jawab Hukum Platform E-Commerce atas Kebocoran Data Pribadi dalam Perspektif UU No. 27 Tahun 2022. Jurnal Kajian Hukum Dan Kebijakan Publik| E-ISSN: 3031-8882, 2(2), 1089-1096.
Yuniarti, Siti. "Perlindungan Hukum Data Pribadi Di Indonesia." Business Economic, Communication, and Social Sciences Journal (BECOSS) 1, no. 1 (2019): 147–54.
ARTIKEL :
APJII. "APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang." Apjii.or.Id, 2024. https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet- indonesia-tembus-221-juta-orang.
———. "Survei APJII Pengguna Internet Di Indonesia Tembus 215 Juta Orang." Apjii.or.Id, 2023. https://apjii.or.id/berita/d/survei-apjii-pengguna-internet-di-indonesia-tembus-215-juta-orang.
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), 11-11.
Bernie, Muhammad. "91 Juta Data Pengguna Tokopedia Bocor Dan Disebar Di Forum Internet." Tirto.Id, 2020. https://tirto.id/91-juta-data-pengguna-tokopedia- bocor-dan-disebar-di-forum- internet-fNH1.
Daeng, Y., Linra, N., Darham, A., Handrianto, D., Sianturi, R. R., Martin, D., ... & Saputra, H. (2023). Perlindungan Data Pribadi dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi. Innovative: Journal Of Social Science Research, 3(6), 2898-2905.
Deon, Dugaan Pembobolan Data Pelanggan Bukalapak: UU Perlindungan Data Pribadi Mendesak, https://www.kominfo.go.id, diakses pada tanggal 16 April 2024
Desi Kris, Kronologi Lengkap Bocornya Data Denny Siregar, Pelaku Ditangkap hingga Motif Kejahatan, https://jatimtimes.com. Diakses pada tanggal 16 April 2024.
Dewi, A. K., Sibarani, B. K., Saputra, E., Norazlina, N., Susanti, S., & Syafira, Y. (2025). Strategi Efektif Pengendalian Internal dalam Keamanan Sistem Informasi Akuntansi untuk Perlindungan Data Keuangan. Jurnal Ilmiah Raflesia Akuntansi, 11(1), 138-148.

Fallahnda, Balqis. “Kronologi LockBit Diduga Curi Data Nasabah BSI & Update Terkini.” Tirto.Id, 2023.

Firdaus, Achmad. “Kasus Kebocoran Data Pribadi Di Indonesia: 10 Kejadian Terbesar Yang Perlu Diketahui.” Medcom.Id, 2024.

Hidayat, R. S. (2025). Transformasi hukum bisnis di ekosistem digital: Studi atas perlindungan data pribadi konsumen. RIGGS: Journal of Artificial Intelligence and Digital Business, 3(4), 46-52. https://www.medcom.id/teknologi/news-teknologi/8koPDdWK-kasus- kebocoran-data-pribadi-di- indonesia-10-kejadian-terbesar-yang-perlu-diketahui.

Kurnianingrum, T. P. (2020). Urgensi pelindungan data pribadi konsumen di era ekonomi digital. Kajian, 25(3), 197-216.

Mahmud Ashari, Belajar Dari Kebocoran Data Kredensial: Data Yang Paling Berharga adalah Data Pribadi, https://www.djkn.kemenkeu.go.id. Diakses pada tanggal 28 Mei 2024

Rahmadani, A. E., Pangestu, Y., & Halizhah, N. (2024). Perlindungan Data Pribadi di Era Digital: Tantangan dan Solusi Dalam Sistem Perbankan. Media Hukum Indonesia (MHI), 2(4), 180-186.

Rita Puspita Sari, RI Siapkan Lembaga Pengawas Perlindungan Data Pribadi, https://www.cloudcomputing.id. Diakses pada tanggal 28 Mei 2024.

Suari, K. R. A., & Sarjana, I. M. (2023). Menjaga privasi di era digital: Perlindungan data pribadi di Indonesia. Jurnal Analisis Hukum, 6(1), 132-142.

Widiartanto, Yoga Hasyadi, and Reska K Nisntanto. “Skandal Pencurian Data Facebook Bikin Cambridge Analytica Bangkrut Dan Ditutup.” Tekno.Kompas.Com,2018. https://tekno.kompas.com/read/2018/05/03/08450037/skandal-pencurian-data-facebook-bikin- cambridge-analytica-bangkrut-dan-ditutup

Wildan, M., Ramadhan, D. R. C., & Wijayanti, Z. R. (2024). Analisis Tanggung Jawab Bank Terhadap Kebocoran Data Nasabah: Ditinjau Dalam Perspektif Hukum Perbankan. Media Hukum Indonesia (MHI), 2(4