Rechtsregel
Jurnal Ilmu Hukum
Vol 8, No. 1 Agustus| 2025
P-ISSN 2622-6235, E-ISSN 2622-6243
rjih_fh@unpam.ac.id

ANALISIS YURIDIS PERLINDUNGAN KONSUMEN ATAS KEBOCORAN DATA PRIBADI DALAM TRANSAKSI JUAL BELI AKUN DOMPET DIGITAL

Bintang Mahacakri Lisan Putri, Rohaini, Ria Wierma Putri
Universitas Lampung
bintangmlp@gmail.com, rohainiariefien@gmail.com, ria.wierma@fh.unila.ac.id

ABSTRAK

Perlindungan konsumen di era digital merupakan tantangan besar yang dihadapi oleh Indonesia seiring dengan pesatnya perkembangan teknologi dan transaksi elektronik. Meskipun sudah ada regulasi seperti Undang-Undang Perlindungan Konsumen dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), peraturan yang ada saat ini masih belum mampu mengatasi masalah baru yang muncul akibat digitalisasi, seperti kebocoran data pribadi, penipuan online, serta kesulitan dalam menegakkan hukum terhadap platform digital lintas negara. Penelitian ini bertujuan untuk mengeksplorasi urgensi pembaruan hukum untuk memperkuat perlindungan konsumen di era digital. Melalui pendekatan kualitatif, penelitian ini mengidentifikasi berbagai tantangan yang dihadapi konsumen digital, termasuk kurangnya transparansi dalam layanan digital, rendahnya literasi digital, serta pengawasan yang kurang terhadap pelaku usaha di sektor digital. Temuan penelitian ini menunjukkan bahwa pembaruan hukum yang menyeluruh sangat diperlukan untuk memperkuat transparansi, keamanan data, serta mempermudah akses konsumen dalam menuntut hak-hak mereka. Pembaruan ini juga harus mencakup pembentukan lembaga mediasi dan arbitrase khusus untuk sektor digital, penguatan pengawasan terhadap pelaku usaha, serta harmonisasi antara regulasi domestik dan standar internasional. Penelitian ini menyimpulkan bahwa dengan pembaruan hukum yang lebih responsif dan berkelanjutan, Indonesia dapat menciptakan lingkungan digital yang lebih aman, adil, dan dapat diandalkan bagi konsumen.

Kata Kunci: Perlindungan konsumen, pembaruan hukum, transaksi digital, transparansi, keamanan data, literasi digital

ABSTRACT

Consumer protection in the digital era is a major challenge faced by Indonesia along with the rapid development of technology and electronic transactions. Despite the existence of regulations such as the Consumer Protection Law and the Electronic Information and Transaction Law (ITE Law), the current regulations are still unable to address new problems arising from digitalization, such as personal data leakage, online fraud, as well as difficulties in enforcing laws against cross-border digital platforms. This research aims to explore the urgency of law reform to strengthen consumer protection in the digital era. Through a qualitative approach, this research identifies various challenges faced by digital consumers, including a lack of transparency in digital services, low digital literacy, and insufficient supervision of businesses in the digital sector. The findings show that comprehensive legal reforms are needed to strengthen transparency, data security, and make it easier for consumers to access their rights. This reform should also include the establishment of special mediation and arbitration institutions for the digital sector, strengthening supervision of business actors, and harmonization between domestic regulations and international standards. This research concludes that with more responsive and sustainable legal reforms, Indonesia can create a safer, fairer and more reliable digital environment for consumers.

Keywords: *Consumer protection, law reform, digital transactions, transparency, data security, digital literacy*

PENDAHULUAN

Perkembangan ekonomi digital di Indonesia memberikan peluang besar bagi pertumbuhan ekonomi, tetapi juga menghadirkan tantangan signifikan, terutama dalam hal perlindungan konsumen. Laporan *e-Conomy SEA 2021* mencatat bahwa nilai ekonomi digital Indonesia melonjak dari US$40 miliar pada 2019 menjadi US$70 miliar pada 2021, menunjukkan percepatan yang luar biasa. Namun, akselerasi ini tidak sejalan dengan kesiapan regulasi yang mampu melindungi konsumen, khususnya dalam aspek keamanan data pribadi. Yayasan Lembaga Konsumen Indonesia (YLKI) menerima 535 aduan terkait layanan digital pada 2021, di mana sebagian besar berkaitan dengan kebocoran data pribadi dan pelanggaran privasi. Fenomena ini menjadi bukti nyata perlunya pembaruan hukum yang adaptif dan progresif dalam menghadapi era digital (Hezkiel Bram Setiawan dan Fatma Najicha,2022).

Kasus kebocoran data pribadi terus meningkat dan menyebabkan kerugian besar bagi konsumen. Pada Mei 2020, data pribadi 91 juta pengguna Tokopedia bocor dan dijual di forum daring, mengekspos informasi seperti nama, alamat, dan nomor telepon. Insiden serupa menimpa BPJS Kesehatan pada 2021, di mana data 279 juta peserta diduga diperjualbelikan di *dark web*. Kejadian-kejadian ini tidak hanya menimbulkan kerugian finansial tetapi juga menciptakan ketidakpercayaan terhadap ekosistem digital di Indonesia. Dalam laporan IBM Security 2021, rata-rata kerugian global akibat kebocoran data mencapai US$4,24 juta per insiden, sementara di Indonesia, total kerugian akibat kejahatan siber melonjak dari Rp61,71 miliar pada 2020 menjadi Rp3,88 triliun pada 2021.

Dampak kebocoran data tidak hanya bersifat finansial tetapi juga melibatkan konsekuensi psikologis yang signifikan. Konsumen yang datanya disalahgunakan sering menghadapi pencurian identitas, pemerasan, atau bahkan penipuan, yang dapat menyebabkan tekanan emosional yang mendalam. Pelaku sering memanfaatkan informasi yang diperoleh untuk berbagai kejahatan, seperti mengajukan pinjaman atas nama korban. Dalam kondisi ini, konsumen merasa tidak berdaya karena proses hukum untuk melindungi hak-hak mereka sering kali rumit dan memakan waktu. Akibatnya, perlindungan hukum yang lemah menciptakan rasa ketidakamanan dalam bertransaksi secara digital (Aulia Alayna Suvil, 2024).

Kerangka hukum yang ada belum mampu menjawab tantangan perlindungan data pribadi dengan efektif. Sebelum diberlakukannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), isu perlindungan data hanya diatur secara parsial melalui UU ITE dan beberapa peraturan sektoral. Ketiadaan regulasi khusus membuat mekanisme pengawasan dan penegakan hukum menjadi lemah. Banyak perusahaan digital yang gagal memprioritaskan keamanan data karena kurangnya insentif hukum atau sanksi yang signifikan. Dengan UU PDP, harapannya adalah adanya kerangka hukum yang lebih terintegrasi, namun tantangan implementasi tetap membutuhkan perhatian serius.

UU PDP diharapkan menjadi landasan kuat dalam memperbaiki tata kelola data pribadi di Indonesia. UU ini mengatur kewajiban penyedia layanan digital untuk menjaga kerahasiaan data konsumen, meliputi penerapan teknologi keamanan yang memadai dan pemberian kompensasi kepada konsumen yang dirugikan. Namun, keberhasilan UU ini sangat bergantung pada kesiapan teknis dari perusahaan dan kesadaran konsumen terhadap hak-hak mereka. Sayangnya, survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) menunjukkan bahwa lebih dari 60% pengguna internet di Indonesia tidak memahami pentingnya perlindungan data pribadi, yang menjadi tantangan besar dalam penerapan aturan tersebut.

Penyedia layanan dompet digital menghadapi tekanan besar untuk mengamankan data pengguna mereka. Platform seperti OVO, GoPay, dan Dana harus mengatasi serangan siber yang semakin kompleks, sementara di sisi lain, mereka harus meningkatkan literasi digital pengguna. Banyak pengguna masih lengah terhadap ancaman seperti *phishing* atau peretasan melalui perangkat yang tidak aman. Selain itu, beberapa kasus kebocoran data yang melibatkan kesalahan internal menunjukkan perlunya pelatihan intensif bagi staf di perusahaan-perusahaan tersebut. Untuk memitigasi risiko ini, investasi dalam teknologi keamanan mutakhir, seperti enkripsi end-to-end dan sistem autentikasi multi-faktor, menjadi suatu keharusan.

Mekanisme penyelesaian sengketa terkait kebocoran data juga masih memerlukan perbaikan yang signifikan. Konsumen sering menghadapi kesulitan dalam menuntut hak mereka karena rumitnya proses hukum dan rendahnya transparansi dari penyedia layanan. Dalam banyak kasus, perusahaan yang bertanggung jawab atas kebocoran data tidak memberikan kompensasi yang memadai atau bahkan tidak mengakui kesalahan mereka. Pembentukan lembaga pengawasan khusus untuk menangani pelanggaran data pribadi dapat menjadi solusi untuk memastikan bahwa hak-hak konsumen ditegakkan dengan lebih baik (Althea Serafim Kriswandaru, 2024).

Pemerintah memiliki peran penting dalam menciptakan ekosistem digital yang lebih aman dan terpercaya. Selain memperkuat regulasi, diperlukan upaya untuk meningkatkan pengawasan terhadap perusahaan digital. Audit keamanan secara berkala dan penerapan sanksi tegas terhadap pelanggaran dapat memberikan efek jera. Di sisi lain, kerja sama antara pemerintah, sektor swasta, dan lembaga internasional juga diperlukan untuk menangani kasus-kasus lintas negara, seperti pelanggaran yang melibatkan perusahaan asing.

Edukasi dan literasi digital menjadi langkah fundamental dalam melindungi konsumen di era digital. Konsumen harus diberikan pemahaman yang lebih baik tentang bagaimana menjaga data pribadi mereka, misalnya melalui penggunaan autentikasi dua faktor atau menghindari membagikan informasi sensitif secara daring. Kampanye literasi digital yang melibatkan pemerintah, penyedia layanan, dan komunitas masyarakat dapat meningkatkan kesadaran publik dan mengurangi risiko kebocoran data.

Dalam jual beli akun dompet digital, risiko kebocoran data semakin meningkat, menunjukkan perlunya regulasi yang lebih tegas dan pengawasan yang lebih baik. Proses ini sering kali melibatkan

transfer akses akun yang berisi informasi pribadi, yang dapat dengan mudah disalahgunakan oleh pihak yang tidak bertanggung jawab. Dengan regulasi yang lebih komprehensif, pengawasan yang ketat, dan investasi dalam teknologi keamanan, ekosistem digital Indonesia dapat berkembang menjadi lebih aman dan mampu memberikan perlindungan yang lebih baik bagi konsumen.

Penelitian ini menggunakan pendekatan kualitatif deskriptif untuk menganalisis urgensi pembaruan hukum dalam perlindungan konsumen di era digital. Data dikumpulkan melalui studi pustaka dengan mengkaji berbagai sumber hukum, literatur yang relevan, serta laporan dari lembaga-lembaga resmi seperti Badan Siber dan Sandi Negara (BSSN) dan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). Penelitian ini juga menganalisis regulasi yang berlaku, seperti Undang-Undang Perlindungan Konsumen dan UU ITE, untuk mengidentifikasi kesenjangan dalam perlindungan konsumen di dunia digital. Selain itu, penelitian ini memanfaatkan data sekunder yang diperoleh dari survei dan laporan terkait untuk menilai tantangan yang dihadapi oleh konsumen digital.

PEMBAHASAN

1. Bentuk perlindungan hukum terhadap konsumen yang mengalami kebocoran data pribadi akibat jual beli akun dompet digital (e-wallet) menurut peraturan perundang-undangan di Indonesia

Perlindungan hukum terhadap konsumen yang mengalami kebocoran data pribadi akibat jual beli akun dompet digital di Indonesia menjadi isu yang semakin mendesak, seiring dengan meningkatnya aktivitas ekonomi digital (Andri Soemitra dan Adlina Hasan, 2024). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) hadir sebagai upaya memberikan kerangka hukum komprehensif untuk melindungi data pribadi konsumen. Undang-undang ini menetapkan bahwa data pribadi adalah hak fundamental yang harus dijaga, dengan memberikan konsumen kendali penuh atas data mereka (Danil Erlangga Mahameru, 2023). Selain itu, UU PDP mewajibkan pelaku usaha yang mengelola data pribadi untuk mematuhi prinsip-prinsip perlindungan data, seperti transparansi, keamanan, dan akuntabilitas. Namun, implementasi UU PDP masih menghadapi tantangan berupa kurangnya kesadaran publik dan kesiapan teknis banyak penyedia layanan digital dalam mematuhi standar yang ditetapkan.

Selain UU PDP, konsumen juga dilindungi oleh Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UU Perlindungan Konsumen), yang memberikan landasan hukum bagi hak-hak konsumen dalam transaksi digital. Pasal 7 UU ini menegaskan bahwa pelaku usaha wajib menjamin keamanan dan kerahasiaan data pribadi konsumen serta memberikan kompensasi jika terjadi pelanggaran. Dalam konteks dompet digital, kewajiban ini meliputi penerapan teknologi keamanan tingkat tinggi, pemberitahuan kepada konsumen dalam kasus kebocoran data, dan kompensasi yang adil bagi konsumen yang dirugikan. Namun, pelanggaran terhadap kewajiban ini sering kali tidak direspon dengan tegas, baik oleh penyedia layanan maupun pihak berwenang, sehingga memunculkan keraguan terhadap efektivitas perlindungan hukum tersebut.

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) juga memiliki peran penting dalam melindungi data pribadi konsumen. Pasal 26 UU ITE secara eksplisit menyebutkan bahwa penggunaan data pribadi harus berdasarkan persetujuan pemilik data, dan pelanggaran terhadap prinsip ini dapat dikenai sanksi administratif maupun pidana (Erna Priliasari, 2023). Dalam kasus kebocoran data akibat jual beli akun dompet digital, penyedia layanan dapat dimintai pertanggungjawaban hukum jika terbukti lalai dalam melindungi data pribadi pengguna. Namun, tantangan utama dalam penegakan UU ITE adalah rendahnya kapasitas teknis aparat penegak hukum dalam menangani kasus-kasus siber yang kompleks, sehingga banyak kasus kebocoran data berakhir tanpa penyelesaian yang memadai.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE) memberikan pedoman teknis yang lebih rinci terkait tanggung jawab penyelenggara sistem elektronik. Dalam PP PSTE, penyelenggara sistem diwajibkan untuk menjamin keandalan sistem yang digunakan, melindungi data pribadi dari akses tidak sah, dan melaporkan insiden kebocoran data kepada pihak berwenang dalam waktu 14 hari. Aturan ini juga mengharuskan penyedia layanan untuk melakukan audit keamanan data secara berkala. Namun, laporan dari Kominfo pada 2023 menunjukkan bahwa hanya sekitar 40% penyedia layanan digital yang memenuhi kewajiban ini, menunjukkan masih rendahnya tingkat kepatuhan terhadap PP PSTE, yang pada akhirnya memperbesar risiko kebocoran data.

Konsumen yang dirugikan akibat kebocoran data juga memiliki jalur hukum melalui asas perbuatan melawan hukum sebagaimana diatur dalam Pasal 1365 Kitab Undang-Undang Hukum Perdata (KUHPerdata). Jalur ini memungkinkan konsumen untuk menggugat pelaku usaha yang dianggap lalai dalam melindungi data pribadi. Namun, proses ini sering kali

menghadapi kendala, terutama dalam hal pembuktian dan biaya yang harus dikeluarkan oleh konsumen. Dalam kasus jual beli akun dompet digital, misalnya, konsumen harus mampu membuktikan adanya hubungan kausal antara kebocoran data dan kerugian yang dialami, yang sering kali sulit dilakukan tanpa dukungan ahli forensik digital atau perangkat hukum yang memadai.

Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI) juga memiliki peran strategis dalam mengawasi praktik keamanan data oleh penyedia layanan dompet digital. Sebagai regulator sektor keuangan, kedua lembaga ini telah mengeluarkan berbagai regulasi terkait tata kelola data, seperti kewajiban penerapan prinsip *know your customer* (KYC) dan audit berkala terhadap sistem keamanan. Namun, laporan OJK pada 2022 menunjukkan bahwa masih banyak penyedia layanan yang gagal memenuhi standar keamanan ini, terutama penyedia kecil yang memiliki keterbatasan sumber daya. Hal ini menciptakan celah yang dapat dimanfaatkan oleh pelaku kejahatan siber untuk mencuri atau menyalahgunakan data pribadi konsumen (Diva Salsabila Ferdiansyah, 2024).

Tantangan dalam penerapan perlindungan hukum ini tidak hanya berasal dari rendahnya tingkat kepatuhan pelaku usaha, tetapi juga literasi digital yang rendah di kalangan masyarakat. Banyak konsumen tidak menyadari hak-hak mereka terkait data pribadi, sehingga cenderung pasif ketika mengalami pelanggaran. Sebagai contoh, survei yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada 2023 menunjukkan bahwa hanya 30% pengguna internet di Indonesia yang memahami pentingnya pengaturan privasi dalam aplikasi digital. Rendahnya literasi ini membuat konsumen rentan terhadap eksploitasi data dan memperbesar risiko kebocoran informasi (Linda Kurniawati, 2024).

Koordinasi antar lembaga pemerintah dalam menangani kebocoran data pribadi juga menjadi tantangan besar. Kasus kebocoran data sering kali melibatkan berbagai pihak, seperti Kementerian Komunikasi dan Informatika (Kominfo), OJK, dan pihak kepolisian. Namun, kurangnya sinergi antara lembaga-lembaga ini sering kali menyebabkan proses penanganan menjadi lambat dan tidak efektif. Dalam beberapa kasus, seperti kebocoran data BPJS Kesehatan pada 2021, koordinasi yang buruk menyebabkan ketidakpastian hukum dan menimbulkan ketidakpercayaan masyarakat terhadap kemampuan pemerintah dalam melindungi data pribadi mereka.

Pemerintah perlu mempertimbangkan pembentukan lembaga independen yang khusus menangani perlindungan data pribadi, seperti Data Protection Authority (DPA) di Uni Eropa. Lembaga ini dapat berfungsi sebagai regulator dan pengawas dalam penerapan UU PDP, memberikan sanksi kepada pelanggar, dan menyediakan saluran pengaduan yang efektif bagi konsumen. Keberadaan lembaga semacam ini juga dapat mendorong peningkatan kepatuhan pelaku usaha terhadap regulasi dan menciptakan kepercayaan konsumen terhadap ekosistem digital.

Dalam konteks jual beli akun dompet digital, pendekatan perlindungan hukum harus mencakup pengawasan yang lebih ketat dan edukasi konsumen tentang risiko yang mereka hadapi. Penyedia layanan dompet digital perlu berperan aktif dalam mencegah praktik-praktik yang berpotensi membahayakan data pribadi, seperti dengan meningkatkan teknologi keamanan dan menyediakan informasi yang transparan kepada pengguna. Dengan pendekatan yang terintegrasi antara regulasi, edukasi, dan pengawasan, perlindungan hukum terhadap konsumen dapat berjalan lebih efektif, menciptakan ekosistem digital yang aman dan terpercaya.

2. Tanggung jawab perusahaan penyedia layanan dompet digital terhadap kebocoran data pribadi konsumen dalam praktik jual beli akun dompet digital

Perusahaan penyedia layanan dompet digital memiliki tanggung jawab hukum yang sangat besar terhadap kebocoran data pribadi konsumen, terutama terkait dengan praktik jual beli akun dompet digital yang kerap melibatkan penyalahgunaan data sensitif. Dalam konteks ini, tanggung jawab perusahaan untuk melindungi data pribadi konsumen diatur secara tegas dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). UU ini mewajibkan penyelenggara layanan digital untuk menjamin keamanan data pribadi konsumen dan melakukan upaya pencegahan terhadap potensi akses tidak sah. Tanggung jawab ini mencakup pengimplementasian berbagai langkah teknis, seperti enkripsi data tingkat lanjut, autentikasi ganda, dan pemantauan aktivitas secara berkala guna mendeteksi potensi ancaman. Meskipun aturan ini dirancang untuk memberikan perlindungan maksimal kepada konsumen, banyak perusahaan yang masih belum sepenuhnya mematuhi standar yang ditetapkan, yang menyebabkan kerentanannya terhadap kebocoran data yang dapat merugikan banyak pihak. Selain itu, ketidakpatuhan terhadap kebijakan ini sering kali terhambat oleh ketidaksiapan infrastruktur teknologi di banyak perusahaan, yang menjadikannya lebih rentan terhadap serangan siber yang berbahaya.

Kewajiban perlindungan data pribadi juga diatur dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UU Perlindungan Konsumen), yang menjadi landasan hukum bagi para pelaku usaha dalam menjamin keamanan dan kerahasiaan data konsumen. Pasal 7 dalam UU ini dengan jelas menekankan bahwa pelaku usaha harus memastikan bahwa data pribadi konsumen tidak disalahgunakan oleh pihak ketiga dan harus bertanggung jawab atas segala kerugian yang timbul akibat kelalaian mereka. Hal ini mengharuskan perusahaan penyedia dompet digital untuk tidak hanya menjaga keamanan data dari segi teknis tetapi juga untuk memiliki prosedur darurat yang cepat dan efektif apabila terjadi kebocoran data. Tanggung jawab ini mencakup pengaturan sistem yang dapat segera menangani insiden kebocoran data dan memastikan konsumen yang terdampak mendapatkan kompensasi yang layak. Namun, data yang dirilis oleh Yayasan Lembaga Konsumen Indonesia (YLKI) pada 2023 menunjukkan bahwa banyak perusahaan hanya memberikan respons minimalis ketika kebocoran data terjadi, dan sering kali tidak memberikan kompensasi yang cukup kepada konsumen yang mengalami kerugian (Andri Soemitra dan Adlina Hasan, 2022).

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE) memberikan rincian teknis mengenai tanggung jawab perusahaan dalam menjaga keamanan data konsumen. Peraturan ini mewajibkan penyelenggara sistem elektronik untuk memastikan bahwa sistem mereka bebas dari celah keamanan yang bisa dieksploitasi oleh pihak yang tidak bertanggung jawab. Selain itu, PP PSTE juga mengatur kewajiban bagi perusahaan untuk melaporkan insiden kebocoran data kepada otoritas terkait, seperti Kementerian Komunikasi dan Informatika (Kominfo), serta untuk memberikan notifikasi kepada pengguna yang terdampak dalam waktu 14 hari sejak insiden terjadi. Meskipun regulasi ini terkesan ketat, survei yang dilakukan oleh Kominfo pada 2023 mengungkapkan bahwa lebih dari separuh perusahaan teknologi di Indonesia masih tidak melaporkan insiden keamanan dengan tepat waktu, yang mengarah pada ketidakmampuan dalam mitigasi risiko dan peningkatan kerugian bagi konsumen. Keadaan ini menunjukkan adanya celah besar dalam penerapan regulasi yang seharusnya melindungi konsumen (Tiara Shafa Putri, 2025).

Dalam kasus jual beli akun dompet digital, perusahaan penyedia layanan harus mengambil langkah-langkah tegas untuk mencegah penyalahgunaan akun yang melibatkan pihak ketiga yang tidak sah. Tanggung jawab perusahaan dalam hal ini mencakup penerapan sistem keamanan yang ketat, seperti sistem anti-penipuan berbasis kecerdasan buatan yang mampu mendeteksi pola transaksi yang mencurigakan serta metode autentikasi biometrik yang jauh lebih sulit untuk dipalsukan. Perusahaan juga diwajibkan menyediakan mekanisme pelaporan yang memungkinkan konsumen untuk segera melaporkan akun mereka jika dicurigai disalahgunakan, sehingga perusahaan dapat segera mengambil langkah mitigasi yang diperlukan. Namun, laporan dari IBM Security pada 2022 menunjukkan bahwa lebih dari 60% perusahaan di kawasan Asia Tenggara, termasuk Indonesia, masih menggunakan sistem keamanan yang usang, yang semakin meningkatkan kerentanannya terhadap ancaman dunia maya yang terus berkembang (Dewi Puspita Sari, 2023).

Selain itu, tanggung jawab perusahaan juga mencakup kewajiban untuk memberikan kompensasi yang setimpal kepada konsumen yang dirugikan akibat kebocoran data. Pasal 19 UU Perlindungan Konsumen secara jelas mengatur bahwa pelaku usaha wajib memberikan ganti rugi kepada konsumen yang mengalami kerugian, yang bisa berupa pengembalian dana, penggantian barang atau jasa, atau bentuk kompensasi lainnya yang disepakati antara kedua belah pihak. Namun, mekanisme kompensasi ini sering kali tidak berjalan efektif. Studi yang dilakukan oleh Indonesian Cyber Security Forum pada 2023 menunjukkan bahwa hanya 20% dari kasus kebocoran data yang dilaporkan mendapatkan respons yang memadai dari perusahaan, sementara sisanya berakhir tanpa solusi yang memuaskan bagi konsumen. Hal ini menunjukkan perlunya pengawasan yang lebih ketat terhadap implementasi kewajiban kompensasi ini agar konsumen dapat memperoleh hak mereka dengan adil (Eko Nurhadi, 2019).

Edukasi konsumen mengenai risiko kebocoran data pribadi juga merupakan bagian dari tanggung jawab yang harus dipikul oleh perusahaan penyedia layanan dompet digital. Banyak konsumen yang tidak sepenuhnya memahami potensi risiko yang bisa timbul akibat penyalahgunaan akun digital, seperti penipuan, pencurian identitas, atau bahkan kerugian finansial yang besar. Survei yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada 2023 menunjukkan bahwa hanya 29% pengguna dompet digital yang memiliki pemahaman yang memadai tentang pentingnya menjaga kerahasiaan data pribadi mereka. Oleh karena itu, perusahaan perlu mengambil peran aktif dalam memberikan informasi yang mudah diakses dan dimengerti mengenai cara-cara untuk melindungi data pribadi mereka, baik melalui kampanye edukasi publik, pemberian informasi yang jelas pada saat registrasi, maupun menyediakan fitur keamanan dalam aplikasi yang dapat memperingatkan pengguna mengenai potensi ancaman.

Dari sisi teknologi, perusahaan harus mengadopsi infrastruktur keamanan yang sesuai dengan standar global untuk melindungi data pribadi pengguna mereka. Teknologi seperti enkripsi end-to-end, firewall tingkat lanjut, dan pengelolaan akses berbasis peran (role-based access control) harus menjadi standar operasional. Namun, banyak perusahaan kecil dan menengah menghadapi tantangan besar dalam mengimplementasikan teknologi ini karena keterbatasan anggaran dan kurangnya tenaga ahli di bidang keamanan siber. Pemerintah dapat membantu dengan memberikan insentif bagi perusahaan yang berinvestasi dalam penguatan sistem keamanan mereka, seperti pengurangan pajak atau subsidi untuk pengembangan teknologi yang lebih canggih dan aman.

Secara hukum, perusahaan dapat dimintai pertanggungjawaban pidana apabila terbukti melakukan kelalaian atau kesengajaan yang menyebabkan kebocoran data pribadi. Pasal 48 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) memberikan ancaman hukuman hingga enam tahun penjara atau denda maksimal Rp1 miliar bagi pelanggaran yang melibatkan kebocoran data pribadi. Meskipun ketentuan ini sudah cukup tegas, implementasinya masih menghadapi banyak kendala, seperti kompleksitas dalam pembuktian kasus kejahatan siber serta keterbatasan kapasitas penegak hukum dalam menangani kasus-kasus yang melibatkan teknologi informasi. Kasus kebocoran data Tokopedia pada 2020 adalah contoh nyata dari lambatnya proses hukum yang justru merugikan konsumen yang berharap segera mendapatkan keadilan. Proses hukum yang memakan waktu lama menciptakan ketidakpastian yang menambah beban bagi korban kebocoran data.

Reputasi perusahaan juga menjadi taruhan besar dalam kasus kebocoran data pribadi. Kehilangan kepercayaan konsumen dapat berdampak langsung pada penurunan jumlah pengguna layanan dan pendapatan perusahaan. Perusahaan-perusahaan besar, seperti GoPay dan OVO, telah mulai mengadopsi kebijakan transparansi dengan melaporkan secara terbuka langkah-langkah yang mereka ambil untuk memperbaiki sistem keamanan mereka setelah insiden kebocoran data. Langkah transparansi ini sangat penting untuk membangun kembali kepercayaan konsumen, namun perusahaan-perusahaan kecil sering kali tidak memiliki kapasitas yang sama untuk melakukan hal tersebut, yang membuat mereka lebih rentan terhadap kerugian reputasi yang besar.

Untuk memastikan bahwa tanggung jawab perusahaan berjalan efektif, diperlukan pengawasan yang lebih ketat dari regulator yang berwenang, seperti Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI). Kedua lembaga ini memiliki peran penting dalam memberlakukan audit keamanan wajib, memberikan sanksi administratif bagi perusahaan yang tidak mematuhi standar perlindungan data, dan memfasilitasi koordinasi antara berbagai pihak terkait dalam menangani insiden kebocoran data. Selain itu, pembentukan lembaga independen khusus yang mengawasi perlindungan data pribadi, seperti Data Protection Authority (DPA), dapat memperkuat sistem pengawasan ini. Dengan adanya lembaga pengawasan yang independen, tanggung jawab perusahaan dalam melindungi data pribadi konsumen dapat dioptimalkan, yang pada gilirannya akan menciptakan ekosistem digital yang lebih aman dan terpercaya di Indonesia.

Melalui langkah-langkah ini, diharapkan bahwa setiap pelaku usaha yang menyediakan layanan dompet digital akan lebih memperhatikan aspek keamanan data pribadi konsumen mereka, sehingga dapat mengurangi potensi kebocoran yang dapat merugikan masyarakat secara luas. Tanggung jawab ini tidak hanya terbatas pada sisi teknis tetapi juga mencakup aspek etis dan transparansi dalam menjalankan bisnis digital yang bertanggung jawab.

3. Urgensi pembaruan hukum untuk memperkuat perlindungan konsumen di era digital

Urgensi pembaruan hukum untuk memperkuat perlindungan konsumen di era digital semakin nyata, terutama mengingat pesatnya perkembangan teknologi dan tingginya intensitas transaksi elektronik yang terjadi di seluruh dunia, termasuk di Indonesia. Fenomena ini menciptakan tantangan besar bagi konsumen, yang harus menghadapi risiko baru yang sebelumnya tidak ada dalam ekosistem ekonomi tradisional. Di Indonesia, meskipun sudah ada Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UU Perlindungan Konsumen) dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), regulasi yang ada masih belum mampu mengatasi kompleksitas yang muncul akibat digitalisasi. Fenomena kebocoran data pribadi, penipuan berbasis online, serta penyalahgunaan informasi pribadi menunjukkan bahwa perlindungan hukum yang ada sudah ketinggalan zaman. Berdasarkan laporan dari Badan Siber dan Sandi Negara (BSSN) pada tahun 2023, tercatat lebih dari 1,2 juta insiden siber yang terjadi di Indonesia, dan sebagian besar insiden tersebut berhubungan dengan pelanggaran data konsumen. Hal ini menegaskan bahwa kerangka hukum yang ada belum dapat memberikan rasa aman bagi konsumen, dan perlunya pembaruan hukum yang menyeluruh sudah sangat mendesak (Abdurrahman Mazli, 2021).

Transformasi digital yang pesat telah mengubah interaksi antara pelaku usaha dan konsumen, dengan platform online menjadi saluran utama transaksi barang dan jasa. Namun, banyak perusahaan digital yang beroperasi di Indonesia tanpa pengawasan memadai, menciptakan celah hukum yang merugikan konsumen. Survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada 2023 menunjukkan bahwa 72% pengguna dompet digital tidak memahami syarat dan ketentuan layanan mereka, termasuk pengelolaan data pribadi. Hal ini mengindikasikan perlunya pembaruan hukum yang lebih tegas dalam mengatur kewajiban pelaku usaha serta memperkuat pengawasan untuk menjamin perlindungan konsumen (Yustina Dhian Novita, 2021). Pembaruan ini penting agar konsumen dapat membuat keputusan yang lebih bijak dan terlindungi.

Tantangan yurisdiksi lintas negara juga menunjukkan pentingnya pembaruan hukum yang komprehensif. Banyak perusahaan teknologi besar yang beroperasi di luar negeri namun melayani konsumen Indonesia, sehingga penegakan hukum terhadap pelanggaran mereka sering terkendala. Sebagai contoh, Indonesia kesulitan menindaklanjuti kasus kebocoran data dari platform seperti Facebook pada 2021. Untuk itu, Indonesia perlu mengadopsi peraturan yang mewajibkan perusahaan teknologi asing mematuhi hukum Indonesia dan memperkuat perjanjian internasional untuk penegakan hukum lintas negara. Dengan cara ini, perlindungan hukum bagi konsumen Indonesia akan lebih terjamin (Sri Yulianingsih, 2024).

Masalah lainnya yang harus diatasi melalui pembaruan hukum adalah kurangnya akses konsumen terhadap informasi yang jelas dan transparan mengenai risiko yang terkandung dalam penggunaan layanan digital. Sering kali, platform digital menyembunyikan atau membuat kebijakan privasi dan syarat penggunaan yang terlalu rumit dan sulit dipahami oleh konsumen. Hal ini menambah ketidakpastian bagi konsumen yang tidak memiliki pengetahuan yang cukup tentang hak-hak mereka. Menurut data dari Lembaga Riset Siber Indonesia (CISSReC), 64% konsumen mengaku tidak membaca kebijakan privasi sebelum menggunakan layanan online karena isinya dianggap terlalu teknis dan sulit dipahami. Situasi ini menciptakan ketidakseimbangan informasi yang dapat dimanfaatkan oleh pelaku usaha untuk meraih keuntungan sepihak. Oleh karena itu, pembaruan hukum harus mencakup kewajiban bagi penyedia layanan digital untuk menyederhanakan kebijakan privasi mereka, serta memastikan bahwa informasi yang disampaikan kepada konsumen mudah dimengerti dan cukup jelas. Dengan demikian, konsumen akan lebih mudah untuk membuat keputusan yang terinformasi mengenai penggunaan layanan digital.

Ancaman serangan siber yang semakin meningkat dalam beberapa tahun terakhir juga menunjukkan perlunya pembaruan hukum yang lebih kuat untuk melindungi konsumen dari kerugian akibat serangan tersebut. Laporan dari BSSN pada tahun 2023 menunjukkan bahwa sektor keuangan digital, termasuk dompet digital dan layanan pembayaran online, menjadi target utama serangan siber. Kerugian yang ditimbulkan dari serangan ini diperkirakan mencapai lebih dari Rp18 triliun. Namun, regulasi yang ada saat ini belum sepenuhnya mengatur kewajiban perusahaan untuk mengadopsi teknologi keamanan yang memadai, seperti autentikasi berbasis biometrik atau enkripsi data yang lebih kuat. Oleh karena itu, pembaruan hukum yang diperlukan harus mencakup standar keamanan digital minimum yang harus dipatuhi oleh setiap pelaku usaha, serta menetapkan sanksi yang lebih tegas bagi perusahaan yang gagal dalam melindungi data konsumen mereka. Penerapan teknologi keamanan yang canggih harus menjadi kewajiban yang tidak dapat ditawar untuk memastikan data konsumen terlindungi dari ancaman dunia maya yang semakin kompleks (Ika Atikah, 2020).

Selain itu, konsumen sering kali kesulitan dalam menuntut hak mereka atas kompensasi apabila dirugikan dalam transaksi digital. Hal ini disebabkan oleh prosedur hukum yang rumit, memakan waktu, dan mahal, yang membuat akses ke keadilan sulit bagi konsumen yang tidak memiliki sumber daya hukum yang memadai. Pembaruan hukum yang mendalam harus memberikan mekanisme penyelesaian sengketa yang lebih efektif, misalnya dengan membentuk lembaga mediasi atau arbitrase khusus untuk sektor digital yang bisa membantu konsumen menyelesaikan sengketa dengan pelaku usaha secara cepat, efisien, dan biaya yang lebih rendah. Selain itu, lembaga ini juga bisa berfungsi sebagai pusat pengaduan yang memantau dan mengevaluasi kepatuhan perusahaan terhadap peraturan yang ada. Lembaga semacam ini akan sangat membantu konsumen dalam memperjuangkan hak mereka tanpa harus melalui proses pengadilan yang panjang dan mahal.

Edukasi digital yang memadai juga merupakan elemen penting dalam pembaruan hukum yang harus diperhatikan. Konsumen yang memahami hak-hak mereka dalam dunia digital akan lebih mampu melindungi diri mereka dari berbagai risiko, seperti penyalahgunaan data pribadi atau penipuan online. Data dari survei APJII menunjukkan bahwa literasi digital di Indonesia masih sangat rendah, dengan hanya 38% pengguna yang memahami bagaimana cara melindungi data pribadi mereka saat bertransaksi online. Untuk itu, pembaruan hukum harus mewajibkan

pelaku usaha untuk menyediakan materi edukasi digital yang efektif dan mudah diakses oleh konsumen, baik melalui kampanye publik maupun fitur-fitur edukasi di platform mereka. Dengan meningkatkan pemahaman masyarakat tentang risiko digital dan cara mengamankan data pribadi mereka, konsumen akan lebih siap menghadapi tantangan yang ada di dunia maya (Rizkita Dinar Anggraini, 2024).

Pentingnya pengawasan terhadap pelaku usaha di sektor digital juga tidak bisa diabaikan dalam pembaruan hukum. Banyak pelaku usaha merasa tidak terawasi dengan ketat, sehingga mereka cenderung mengabaikan kewajiban hukum yang berlaku. Misalnya, meskipun ada kewajiban bagi platform e-commerce untuk mendaftar di Kementerian Komunikasi dan Informatika, hanya sekitar 40% dari platform tersebut yang benar-benar terdaftar, sebagaimana diwajibkan oleh Peraturan Pemerintah Nomor 71 Tahun 2019. Pembaruan hukum harus memperkenalkan mekanisme pengawasan yang lebih ketat, seperti melalui audit wajib, serta memberikan wewenang tambahan kepada regulator seperti Otoritas Jasa Keuangan (OJK) untuk melakukan pengawasan yang lebih menyeluruh terhadap sektor digital. Pengawasan yang lebih intensif akan meningkatkan kepatuhan pelaku usaha terhadap peraturan yang ada, dan pada gilirannya akan melindungi konsumen dari praktik bisnis yang merugikan.

Harmonisasi antara regulasi domestik dan standar internasional juga menjadi aspek penting yang harus diperhatikan dalam pembaruan hukum perlindungan konsumen digital. Dalam era globalisasi, transaksi lintas negara sudah menjadi hal yang sangat umum, dan karena itu regulasi domestik perlu selaras dengan standar internasional. Sebagai contoh, General Data Protection Regulation (GDPR) yang diterapkan di Uni Eropa dapat dijadikan acuan bagi Indonesia dalam memperkuat aturan mengenai pengelolaan data pribadi. Pembaruan hukum di Indonesia dapat mengadopsi beberapa elemen dari GDPR, seperti prinsip pengendalian data yang lebih ketat dan hak konsumen untuk menghapus data mereka dari sistem. Melalui harmonisasi ini, Indonesia dapat lebih efektif dalam melindungi konsumen, sekaligus mendukung integrasi Indonesia ke dalam pasar digital global (Rizky Amelia, 2023).

Dengan tantangan yang semakin kompleks di era digital, pembaruan hukum yang menyeluruh menjadi keharusan untuk menciptakan ekosistem digital yang lebih aman, adil, dan dapat diandalkan. Pembaruan ini harus melibatkan revisi terhadap regulasi yang sudah ada, pengesahan aturan baru, serta penguatan mekanisme penegakan hukum yang lebih efektif. Namun, yang tidak kalah penting adalah partisipasi aktif dari semua pemangku kepentingan, termasuk pemerintah, pelaku usaha, organisasi konsumen, dan masyarakat luas, dalam merumuskan dan mengimplementasikan pembaruan hukum ini. Hanya dengan kolaborasi yang baik antara semua pihak, perlindungan konsumen di era digital dapat ditingkatkan secara signifikan, sekaligus mendukung pertumbuhan ekonomi digital yang berkelanjutan di Indonesia.

Perlindungan konsumen di era digital bukanlah tugas yang dapat diselesaikan dalam waktu singkat. Namun, dengan pembaruan hukum yang responsif dan berkelanjutan, Indonesia dapat menciptakan lingkungan digital yang lebih aman bagi konsumen. Regulasi yang jelas dan pengawasan yang ketat akan menciptakan ekosistem yang sehat bagi industri digital, sekaligus memastikan bahwa konsumen tetap terlindungi dari potensi risiko yang dapat merugikan mereka. Melalui langkah-langkah ini, Indonesia dapat menjadi negara yang berhasil melindungi hak-hak konsumen, sekaligus memajukan sektor digital secara berkelanjutan.

KESIMPULAN

Perlindungan konsumen di era digital menjadi isu yang sangat penting di tengah pesatnya perkembangan teknologi dan transaksi elektronik yang semakin kompleks. Meskipun regulasi seperti Undang-Undang Perlindungan Konsumen dan UU ITE sudah ada, namun keduanya belum mampu mengatasi tantangan baru yang muncul akibat digitalisasi. Terlebih dengan adanya kebocoran data pribadi, penipuan online, dan transaksi lintas negara yang sulit diawasi, menunjukkan bahwa kerangka hukum yang ada perlu diperbarui. Pembaruan hukum diperlukan untuk memberikan perlindungan yang lebih baik bagi konsumen, dengan memperketat kewajiban transparansi bagi pelaku usaha, memperkenalkan standar keamanan digital yang lebih ketat, serta mempermudah akses konsumen dalam menuntut hak-hak mereka. Melalui pembaruan hukum yang menyeluruh, Indonesia dapat menciptakan lingkungan digital yang lebih aman dan adil, serta mendukung pertumbuhan ekonomi digital yang berkelanjutan.

SARAN

Pembaruan hukum yang mendalam dan menyeluruh harus segera dilakukan untuk memperkuat perlindungan konsumen di era digital. Salah satu langkah penting adalah memperkenalkan peraturan yang mewajibkan perusahaan digital untuk memberikan informasi yang

jelas dan transparan mengenai layanan mereka, termasuk pengelolaan data pribadi. Selain itu, hukum juga perlu mengatur kewajiban perusahaan dalam menerapkan teknologi keamanan yang canggih, seperti enkripsi data dan autentikasi biometrik, untuk melindungi konsumen dari serangan siber. Dalam hal penyelesaian sengketa, pembaruan hukum harus memungkinkan pembentukan lembaga mediasi atau arbitrase digital yang dapat menyelesaikan sengketa dengan biaya yang lebih rendah dan prosedur yang lebih cepat. Pemerintah juga perlu memperkuat pengawasan terhadap pelaku usaha digital dan menjalin kerja sama dengan regulator internasional untuk menanggulangi masalah lintas negara. Di samping itu, penting untuk meningkatkan literasi digital konsumen agar mereka lebih memahami hak-hak mereka dan dapat melindungi diri dari risiko digital. Sebagai langkah akhir, pembaruan hukum ini harus disusun dengan melibatkan berbagai pihak, termasuk pemerintah, pelaku usaha, dan masyarakat, agar bisa mewujudkan sistem perlindungan konsumen yang lebih efektif dan berkelanjutan.

DAFTAR PUSTAKA

Buku

Ferdiansyah, D. S., Ameeralia, N. V., Kresna Putri, A. A., & Fikrie, S. N. (2024). Peran OJK dalam perlindungan konsumen terhadap kebocoran data pada konsumen jasa keuangan Indonesia. *Media Hukum Indonesia, 2*(3), 45–60.

Abdurrahman, M. (2021). Urgensi pembaharuan Undang-Undang perlindungan konsumen Indonesia di era e-commerce. *Lex Renaissance, 6*(2), 299–300.

Priliasari, E. (2023). Perlindungan data pribadi konsumen dalam transaksi e-commerce. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional, 12*(2), 210–225.

Jurnal

Alayna Suvil, A., Firdaus, F., Ramadhan, M. A., Darma Putra, W., & Lestarika, D. P. (2024). Implementasi perlindungan data pribadi berdasarkan Undang-Undang Nomor 11 Tahun 2020. *Jurnal Hukum, Politik dan Ilmu Sosial, 3*(4), 70–80.

Anggraini, R. D., & Hartantien, S. K. (2024). Perlindungan konsumen atas hak informasi dalam melakukan transaksi online. *Jurnal Hukum dan Keadilan, 13*(1), 104–112.

Amelia, R., Sarbini, I., Adnan, & Sukirman. (2023). Penyelesaian sengketa konsumen dalam e-commerce di Indonesia. *Fundamental: Jurnal Ilmiah Hukum, 12*(1), 199–210.

Erlangga Mahameru, D., Nurhalizah, A., Badjeber, H., Wildan, A., & Rahmadia, H. (2023). Implementasi UU perlindungan data pribadi terhadap keamanan informasi identitas di Indonesia. *Jurnal Esensi Hukum, 5*(2), 45–60.

Kriswandaru, A. S., Pratiwi, B., & Suwardi, S. (2024). Efektivitas kebijakan perlindungan data pribadi di Indonesia: Analisis hukum perdata dengan pendekatan studi kasus. *Hakim: Jurnal Ilmu Hukum dan Sosial, 2*(4), 740–756.

Kurniawati, L., Pratitis, N. T., & Arifiana, I. Y. (2024). Literasi digital dengan perilaku konsumtif pada generasi Z. *JIWA: Jurnal Psikologi Indonesia, 2*(4), 210–225.

Mazli, A. (2021). Urgensi pembaharuan Undang-Undang perlindungan konsumen Indonesia di era e-commerce. *Lex Renaissance, 6*(2), 299–300.

Nurhadi, E. (2019). Perlindungan data pribadi dalam transaksi elektronik di Indonesia. *Jurnal Hukum dan Pembangunan, 49*(2), 234–249.

Putri, T. S., & Putra, M. R. S. (2025). Implementasi Undang-Undang pelindungan data pribadi: Peran manajemen risiko hukum bagi prosesor data pribadi. *Jurnal Hukum Lex Generalis, 5*(4), 123–138.

Setiawan, H. B., & Najicha, F. (2022). Perlindungan data pribadi warga negara Indonesia terkait perkembangan ekonomi digital. *Jurnal Pembangunan Hukum Indonesia, 3*(1), 1–15.

Sari, D. P. (2023). Literasi digital dan perlindungan konsumen dompet digital di Indonesia. *Jurnal Komunikasi Indonesia, 10*(1), 75–90.

Soemitra, A., & Hasan, A. (2022). Perlindungan konsumen terhadap kebocoran data pada jasa keuangan di Indonesia. *Juripol (Jurnal Institusi Politeknik Ganesha Medan, 5*(1), 290–302.

Yulianingsih, S., & Putra, R. K. (2024). Analisis yuridis tentang perlindungan konsumen pada e-commerce di Indonesia: Pendekatan yuridis-normatif. *Hakim: Jurnal Ilmu Hukum dan Sosial, 2*(4), 842–856.

Novita, Y. D., & Santoso, B. (2021). Urgensi pembaharuan regulasi perlindungan konsumen di era bisnis digital. *Jurnal Pembangunan Hukum Indonesia, 3*(1), 46–58.