

MENGUNGKAP KASUS KEBOCORAN DATA PADA PLATFORM E-COMMERCE: ANALISIS DAN MITIGASI RISIKO

Ratri Syawalina¹⁾, Nurwati²⁾, Teguh Rama Prasja³⁾, M. Rendi Aridhayandi⁴⁾

¹Universitas Djuanda, e.2310517@unida.ac.id

²Universitas Djuanda, nurwati@unida.ac.id

³Universitas Islam Riau, teguhramaprasja@law.uir.ac.id

⁴Universitas Djuanda, rendi.aridhayandi@unida.ac.id

ABSTRAK

E-commerce telah menjadi bagian penting dalam kehidupan modern yang mana sudah banyak yang menggunakan elektronik dalam banyak kegiatan, mempermudah transaksi global dan akses ke berbagai produk, tetapi pertumbuhan ini menimbulkan risiko keamanan data yang signifikan. Kebocoran data pada platform e-commerce dapat menyebabkan kerugian finansial, pencurian identitas, dan hilangnya kepercayaan konsumen. Hal ini tentu berkaitan erat dengan UU No. 11 tahun 2008 yang mengatur tentang pemanfaatan informasi dan transaksi elektronik di Indonesia, sudah tercatat didalamnya ketentuan ketentuan elektornik. Tujuan penelitian ini adalah untuk mengkaji kasus kebocoran data pada platform e-commerce, mengidentifikasi penyebabnya, dan mengevaluasi strategi mitigasi risiko yang efektif. Melalui studi kasus dan tinjauan literatur, Dengan ini mengkaji dampak kebocoran data terhadap konsumen, perusahaan e-commerce, dan regulator. Hasil penelitian menunjukkan bahwa kerentanan sistem, kurangnya perhatian terhadap keamanan, dan pengelolaan data yang tidak memadai menjadi penyebab utama kebocoran data. Strategi mitigasi risiko yang dapat diterapkan meliputi peningkatan enkripsi data, penerapan otentikasi multi-faktor, pelatihan keamanan siber bagi karyawan, dan peningkatan kepatuhan terhadap regulasi perlindungan data. Penelitian ini memberikan wawasan berharga bagi industri e-commerce untuk memahami risiko kebocoran data dan mengambil tindakan proaktif untuk melindungi informasi sensitif. Dengan menerapkan strategi mitigasi risiko yang tepat, platform e-commerce dapat meningkatkan keamanan data, membangun kepercayaan konsumen, dan memastikan keberlanjutan bisnis di era digital.

Kata Kunci : Kebocoran data, Data Pribadi, E-Commerce

PENDAHULUAN

Kemajuan pesat dalam teknologi informasi dan komunikasi (TIK) mendorong perubahan yang cepat dalam berbagai bidang, seperti sosial, ekonomi, dan budaya. Internet, sebagai contoh utama dari kemajuan TIK, memudahkan berbagai aspek kehidupan dan mengubah gaya hidup manusia menjadi lebih efisien¹. Dalam kehidupan sosial dan bernegara, hukum dapat berfungsi sebagai standar untuk memastikan terwujudnya keadilan². Sistem teknologi informasi dirancang untuk memperbaiki berbagai aspek pengelolaan sistem informasi, seperti yang tercermin dalam kecepatan, ketepatan waktu, serta pemrosesan dan akurasi sistem, termasuk dalam pelayanan³. Namun, kemudahan ini juga dapat menimbulkan dampak negatif seperti kurangnya interaksi sosial langsung dan potensi penyalahgunaan informasi. Oleh karena itu, penting untuk bijak dalam memanfaatkan teknologi agar dampak positifnya lebih terasa. Perkembangan tersebut terus berjalan pesat, sehingga dibutuhkan regulasi yang mampu mengakomodasi perkembangan tersebut. Salah satu aspek yang berkembang adalah merek, khususnya terkait dengan merek dagang⁴. Di era perkembangan teknologi digital saat ini, kegiatan sehari-hari manusia mengalami kemajuan yang sangat signifikan. Proses digitalisasi di Indonesia semakin cepat selama pandemi COVID-19, terlihat dari perubahan perilaku masyarakat dalam bertransaksi secara online atau e-commerce. Era digital, dengan platform *e-commerce* sebagai garda depan, telah mengubah lanskap konsumsi dan interaksi ekonomi. Konsumen tertarik pada kemudahan akses, pilihan produk

¹ Sujana, K. C., & Suprpti, N. W. S. (2016). Peran Kepercayaan Dalam Memediasi Pengaruh Kualitas Terhadap Niat Konsumen Untuk Berbelanja di Situs Zalora. *Jurnal Manajemen Dan Kewirausahaan*, 5(1), 595–622.

² Esy Kurniasih, Teguh Rama Prasja, dan Anggraini Dwi Milandry, "Perlindungan Konsumen Dalam Hal Pelaksanaan Tanggung Jawab Pengusaha Travel Tanpa Izin Operasional," *Jurnal Akuntansi dan Hukum* (tanggal akses, <https://journal.undiknas.ac.id/index.php/JAH/article/view/3741>).

³ Salsabila, Adinda, Nurwati Nurwati, and Maulana Dwi Sena. 2024. "Implementation of Geographic Information System for Hotels and Lodging in Asahan Regency." *Journal Name (Please Fill In)* 13, no. 2. <https://doi.org/10.32520/stmsi.v13i2.4020>.

⁴ Achmad, Qorie Claudi, Nurwati, and Dadang Suprijatna. 2024. "Penyelesaian Sengketa Merek 'Strong' Dalam Perspektif Prinsip Konstitutif (Studi Putusan Mahkamah Agung Nomor 332K/Pdt.Sus.HKI/Merek/2021)". *Karimah Tauhid* 3 (1):63-79. <https://doi.org/10.30997/karimahtauhid.v3i1.10858>.

beragam, dan harga yang lebih kompetitif. Indonesia mencatat angka kepesatan perdagangan online tertinggi di dunia, mencapai 78%. Pesatnya teknologi informasi ini membuat perlindungan data pribadi atau *privacy* menjadi sangat penting. Perkembangan teknologi informasi mempermudah pekerjaan,

Perkembangan teknologi dan berbagai faktor pendorong telah memainkan peran penting dalam mempercepat pertumbuhan e-commerce dalam dua dekade terakhir.

Beberapa faktor yang mempengaruhinya antara lain:

- a. Perkembangan Infrastruktur Internet
Peningkatan akses dan kecepatan internet mempermudah akses ke platform *e-commerce*, sehingga mendorong pertumbuhannya.
- b. Peningkatan Kepercayaan Konsumen
Keamanan transaksi *online* dan layanan pelanggan yang lebih baik meningkatkan kepercayaan konsumen terhadap *e-commerce*. Ulasan dan testimoni dari pengguna sebelumnya juga berperan penting dalam membangun kepercayaan.
- c. Kemudahan dan Kepuasan Konsumen
E-commerce menawarkan kenyamanan berbelanja 24/7 dari mana saja, dengan beragam produk dan layanan, serta jangkauan yang dapat dipilih sesuai preferensi konsumen
- d. Penetrasi Perangkat Seluler
Munculnya *smartphone* dan tablet mengubah cara konsumen berinteraksi dengan *e-commerce*. Transaksi melalui perangkat seluler atau *mobile commerce* menjadi tren utama dalam industri ini, namun juga meningkatkan risiko kejahatan seperti pencurian data pribadi, termasuk kata sandi, alamat email, nomor kartu kredit, dan informasi lainnya.⁵

⁵ Ayu, S. S., & Nasution, M. I. P. (2023). Analisis Kebocoran Data Privacy Pada E-Commerce Tokopedia. *JUEB: Jurnal Ekonomi dan Bisnis*, 2(3).

Sejalan dengan pertumbuhan *e-commerce*, terjadi segmentasi dan diversifikasi yang signifikan dalam industri ini. Awalnya, *e-commerce* berfokus pada penjualan produk fisik seperti buku, elektronik, dan pakaian. Namun, kini *e-commerce* telah merambah berbagai sektor, termasuk perjalanan (pemesanan tiket pesawat dan hotel), makanan dan minuman (layanan pengantaran makanan), hiburan (streaming musik dan film), dan lain-lain. Perkembangan *e-commerce* saat ini sangat dipengaruhi oleh inovasi dan kemajuan teknologi. Beberapa terobosan yang telah mengubah industri *e-commerce* antara lain adalah:

- (a) AI telah menjadi kekuatan transformatif dalam *e-commerce*, mengubah interaksi bisnis dengan pelanggan dan pengelolaan operasional. Penerapan AI dalam *e-commerce* sangat luas, mulai dari personalisasi pengalaman berbelanja hingga pencarian produk yang lebih akurat dan peningkatan layanan pelanggan. Salah satu aplikasi AI yang paling umum adalah rekomendasi produk yang dipersonalisasi. Dengan menganalisis data dari perilaku pelanggan sebelumnya, riwayat penjelajahan, dan riwayat pembelian, AI dapat menyarankan produk yang relevan dan menarik bagi setiap individu. Fitur-fitur bertenaga AI seperti "Pelanggan juga membeli" atau "Pelanggan juga melihat" dapat menyarankan produk pelengkap berdasarkan ukuran, warna, bentuk, kain, dan merek.

Selain itu, *chatbot* dan asisten virtual telah menjadi alat penting untuk meningkatkan layanan pelanggan. *Chatbot* yang didukung oleh AI, Pemrosesan Bahasa Alami (NLP), dan *Generative AI* dapat memahami dan menanggapi pertanyaan pelanggan secara instan, memberikan dukungan 24/7, memproses pesanan, dan menawarkan penawaran yang dipersonalisasi. Mereka juga dapat mengumpulkan data pelanggan, seperti ukuran dan alasan pertanyaan, yang dapat membantu menginformasikan pengembangan produk dan meningkatkan layanan pelanggan.

AI juga berperan penting dalam mendeteksi dan mencegah penipuan. Dengan menganalisis data, mendeteksi anomali, dan memantau transaksi secara *real*

time, AI dapat mengidentifikasi transaksi yang mencurigakan, seperti transfer bernilai tinggi atau beberapa transaksi dalam waktu singkat dari lokasi yang tidak dikenal, dan menandainya untuk penyelidikan lebih lanjut.

Selain itu, AI dapat membantu dalam manajemen inventaris dengan menganalisis data penjualan historis dan memprediksi permintaan di masa depan. AI dapat mengotomatiskan proses pengisian ulang inventaris dengan berintegrasi dengan pemasok untuk memastikan pengisian ulang tepat waktu, dan memprediksi waktu transit dan penundaan pengiriman, serta mengomunikasikan pembaruan ini dengan pemangku kepentingan, termasuk pelanggan. AI juga memungkinkan penetapan harga dinamis, yang memungkinkan bisnis untuk menyesuaikan harga dan penawaran berdasarkan perilaku pengguna *real-time*, penawaran, dan pesaing. Dengan kekuatan AI, bisnis dapat mengantisipasi peluang diskon optimal dan secara dinamis menentukan diskon minimum yang diperlukan untuk mendorong penjualan yang sukses.

(b) Augmented Reality (AR) dan Virtual Reality (VR):

AR dan VR menawarkan cara inovatif untuk meningkatkan pengalaman berbelanja *online* dengan memberikan gambaran yang lebih nyata tentang produk dan fitur-fiturnya. Teknologi ini memungkinkan pelanggan untuk memvisualisasikan produk dalam lingkungan mereka sendiri sebelum melakukan pembelian, sehingga mengurangi risiko ketidakpuasan dan pengembalian.

Dengan AR, pelanggan dapat menggunakan *smartphone* atau tablet mereka untuk memposisikan versi virtual produk di dalam ruang fisik mereka. Sebagai contoh, konsumen dapat memanfaatkan aplikasi AR untuk melihat bagaimana furnitur akan tampak di ruang tamu mereka atau mencoba pakaian secara virtual sebelum memutuskan untuk membeli.

VR membawa pengalaman berbelanja selangkah lebih maju dengan menciptakan lingkungan virtual yang imersif di mana pelanggan dapat berinteraksi dengan produk dengan cara yang lebih realistis. Misalnya, pelanggan dapat menggunakan *headset* VR untuk menjelajahi toko virtual, memeriksa produk dari semua sudut, dan bahkan berinteraksi dengan perwakilan penjualan virtual.

(c) Internet of Things (IoT):

IoT menghubungkan perangkat rumah pintar dengan platform e-commerce, memungkinkan konsumen untuk melakukan pembelian secara otomatis sesuai dengan kebutuhan mereka. Misalnya, kulkas pintar dapat mendeteksi ketika persediaan makanan rendah dan secara otomatis memesan lebih banyak dari toko *online* pilihan pelanggan.

IoT juga dapat digunakan untuk melacak pengiriman dan memantau kondisi produk selama transit. Sensor IoT dapat memberikan informasi *real-time* tentang lokasi, suhu, dan kelembaban produk, memastikan bahwa mereka dikirimkan dalam kondisi optimal. Selain itu, IoT dapat memungkinkan pengalaman berbelanja yang lebih personal dengan mengumpulkan data tentang preferensi dan perilaku pelanggan. Data ini dapat digunakan untuk memberikan rekomendasi produk yang dipersonalisasi, menawarkan diskon yang ditargetkan, dan meningkatkan layanan pelanggan.

E-commerce menghadapi sejumlah tantangan penting, termasuk memastikan hak-hak konsumen terlindungi, menjaga privasi, mengamankan data, mempertahankan standar mutu produk, serta menyediakan sistem penyelesaian sengketa yang efisien. Perlindungan konsumen menjadi krusial mengingat banyaknya kasus penipuan dan ketidaksesuaian produk. Keamanan data dan privasi juga menjadi perhatian utama. krusial karena platform digital menyimpan dan memproses semakin banyak informasi pribadi. Selain itu, e-commerce juga perlu meningkatkan perlindungan transaksi, mengatasi tantangan logistik dan pengiriman,

serta melindungi konsumen dari kebocoran data, yang dapat menjadi ancaman besar bagi perusahaan dan pelanggan. Masalah kebocoran data konsumen dan penjualan data oleh pihak yang tidak bertanggung jawab juga menjadi isu yang perlu ditangani. Keamanan data dan privasi pun menjadi perhatian utama, mengingat semakin banyak data pribadi yang disimpan dan diproses oleh platform digital. Kebocoran data konsumen dalam e-commerce menjadi salah satu risiko yang sangat serius bagi perusahaan maupun konsumen.

METODE PENELITIAN

Penelitian ini mengadopsi pendekatan kualitatif dengan metode studi pustaka (library research) untuk menganalisis perlindungan data pribadi dalam konteks e-commerce. Pendekatan kualitatif dipilih karena memungkinkan pemahaman yang lebih mendalam terhadap konsep, isu, dan perspektif yang ada yang berkaitan dengan perlindungan data pribadi melalui telaah berbagai sumber tertulis yang relevan. Data dikumpulkan melalui studi literatur yang sistematis dan komprehensif. Studi literatur ini melibatkan pengumpulan dan analisis berbagai sumber sekunder, seperti: Buku teks dan referensi ilmiah yang membahas teori dan konsep terkait data pribadi, privasi, dan perlindungan data. Jurnal ilmiah dan artikel penelitian yang memuat hasil studi empiris, analisis kasus, atau tinjauan teoritis tentang isu-isu perlindungan data pribadi. Peraturan perundang-undangan, kebijakan pemerintah, dan standar industri yang relevan dengan perlindungan data pribadi, termasuk Undang-Undang No. 27 Tahun 2022 yaitu Perlindungan Data Pribadi (UU PDP), UU ITE, dan peraturan turunannya. Laporan penelitian, survei, dan studi kasus yang diterbitkan oleh lembaga pemerintah, organisasi non-pemerintah, atau perusahaan swasta yang berkaitan dengan perlindungan data pribadi. Artikel berita, opini, dan publikasi populer lainnya yang membahas isu-isu perlindungan data pribadi di media massa dan platform online.

HASIL DAN PEMBAHASAN

Perubahan pola hidup masyarakat sejalan dengan berkembangnya dan meluasnya kebiasaan, budaya, serta pengetahuan baru⁶. Dengan Indonesia yang semakin mengalami erosi⁷ tersebut maka Pertumbuhan e-commerce di Indonesia terjadi dengan pesat, didorong oleh meningkatnya jumlah pengguna internet dan semakin meluasnya penerapan teknologi. Indonesia telah memasuki era Industri 4.0, yang ditandai dengan digitalisasi dan otomatisasi di berbagai sektor⁸. Transformasi signifikan dalam lanskap e-commerce mencakup peningkatan penggunaan perangkat seluler untuk berbelanja, diversifikasi layanan yang ditawarkan oleh platform e-commerce, implementasi Strategi pemasaran yang disesuaikan dengan preferensi dan kebutuhan lokal, serta kemajuan dalam infrastruktur logistik yang mendukung efisiensi pengiriman barang. Perubahan dalam praktik e-commerce meliputi peningkatan penggunaan perangkat seluler, keragaman layanan yang tersedia, penerapan strategi pemasaran yang sesuai dengan kebutuhan lokal, serta perkembangan infrastruktur yang mendukung logistik⁹.

Transformasi dalam lanskap e-commerce ini mencakup beberapa aspek penting:

1. Peningkatan Pemanfaatan Perangkat Seluler: Semakin banyak konsumen yang memanfaatkan perangkat seluler. (smartphone dan

⁶ Hidayat, Husain Rahmat, Nurwati, and Dadang Suprijatna. 2024. "Peran Kepolisian Dalam Penanggulangan Tindak Pidana Perjudian Online Studi Kasus : Wilayah Kepolisian Resor Subang, Jawa Barat". *Karimah Tauhid* 3 (3):3050-66. <https://doi.org/10.30997/karimahtauhid.v3i3.12481>.

⁷ Utami, Tanti Kirana, and M Rendi Aridhayandi. 2020. "Regulasi Pendidikan Karakter Bagi Mahasiswa di Fakultas Hukum Universitas Suryakencana dalam Rangka Meningkatkan Softskill dan Literasi Keuangan." *Jurnal Hukum Mimbar Justitia* 6, no. 1: 71-89.

⁸ Aridhayandi, M. Rendi, Achmad Rifqi Nurghi Fari, Usamah Habiburrachman, and Jajang Jajang. 2020. "Optimalisasi Fungsi Kepala Desa Dalam Pelayanan Publik Di Era Revolusi Industri 4.0". *Jurnal MSDA (Manajemen Sumber Daya Aparatur)* 8 (1), 28-38.

⁹ Rohmana, D. W. (2023). Peranan Ekonomi Digital dalam Peningkatan Pertumbuhan UMKM: Peluang Dan Tantangan. In *Indonesian Proceedings and Annual Conference of Islamic Law And Sharia Economic (IPACILSE)*, 1(1), 42–48

tablet) untuk berbelanja online, menjadikan mobile commerce sebagai tren utama dalam industri e-commerce.

2. Diversifikasi Layanan: Platform e-commerce menawarkan berbagai jenis layanan, tidak hanya penjualan produk fisik, tetapi juga layanan digital, seperti pemesanan tiket pesawat dan hotel, pengantaran makanan, streaming musik dan film, dan lain-lain.
3. Personalisasi Pemasaran: Strategi pemasaran semakin disesuaikan dengan preferensi dan kebutuhan lokal konsumen, dengan memanfaatkan data dan analisis untuk menargetkan audiens yang tepat dengan pesan yang relevan.
4. Kemajuan Logistik: Infrastruktur logistik terus ditingkatkan untuk mendukung pengiriman barang yang lebih cepat, efisien, dan terjangkau, termasuk pengembangan ¹⁰sistem pelacakan (tracking) yang memberikan kemudahan bagi konsumen untuk melacak status pengiriman barang mereka secara langsung.

Insiden kebocoran data yang terjadi pada platform pada tahun 2020, yang melibatkan sekitar 91 juta akun pengguna, merupakan contoh nyata dari risiko yang dihadapi oleh konsumen dalam dunia e-commerce¹¹. Peristiwa ini menyoroti kelemahan dalam sistem keamanan yang diterapkan oleh perusahaan, serta minimnya tanggung jawab dalam pengelolaan data pribadi. Pelanggaran semacam ini menegaskan betapa pentingnya adanya perlindungan hukum yang kokoh untuk mencegah terjadinya insiden serupa di masa mendatang.

Peristiwa ini menunjukkan kelemahan dalam sistem keamanan yang diterapkan oleh perusahaan, serta minimnya akuntabilitas dalam pengelolaan data pribadi

¹⁰ Shona Azi, RR. Desy Priatni, Indah Pujiati, Aria Wijaya, Aditya Dinda Rahmani, Josuhua Gumanti, ... Elli Ruslina. (2024). Peran UU ITE dalam Regulasi E-Commerce di Era Digital. *Jurnal Ilmu Hukum, Humaniora Dan Politik*, 5(1), 258–267. <https://doi.org/10.38035/jihhp.v5i1.2900>

¹¹ Mahfudin, T. (2024). ANALISA KASUS KEBOCORAN DATA PENGGUNA TOKOPEDIA. *Jurnal Hukum Progresif*, XI(2), 1928–1940.

pengguna. Pelanggaran seperti ini menekankan pentingnya adanya perlindungan hukum yang efektif dan kuat untuk mencegah kejadian serupa di masa yang akan datang. Perlindungan hukum adalah upaya untuk menjaga masyarakat agar tidak menjadi korban tindakan penguasa yang bertentangan dengan aturan hukum, yang dalam konteks ini mencakup perlindungan hukum dalam e-commerce melalui UU ITE dan UU Perlindungan Konsumen¹².

Di Indonesia, ada dua aturan penting yang melindungi konsumen, terutama saat belanja *online*. rangka untuk mewujudkan keadaan yang aman dan tentram dalam kehidupan bermasyarakat¹³. Aturan pertama adalah Perlindungan Konsumen (UU No. 8 Tahun 1999). Aturan kedua adalah (UU ITE) (UU No. 19 Tahun 2016). UU Perlindungan Konsumen bilang bahwa konsumen punya hak untuk dapat informasi yang benar dan jujur soal barang atau jasa yang dijual, termasuk kalau belinya lewat internet. UU ini juga melindungi privasi konsumen, misalnya bagaimana toko *online* mengumpulkan, memakai, dan menyimpan informasi pribadi kita. Selain itu, UU Perlindungan Konsumen juga mengakui kalau transaksi *online* itu sah. Jadi, ada aturan khusus buat melindungi hak-hak konsumen saat belanja *online*, seperti hak untuk dapat informasi yang jelas soal transaksi, termasuk bagaimana toko *online* menjaga privasi kita.¹⁴

Perlindungan hukum berperan vital dalam melindungi kepentingan masyarakat dari tindakan sewenang-wenang penguasa atau pihak lain yang melanggar ketentuan hukum yang berlaku. kepastian serta keuntungan dari hukum, dimana hukum harus

¹² Kurniasih, Esy, Teguh Rama Prasja, and Anggraini Dwi Milandry. 2022. "Perlindungan Konsumen Dalam Hal Pelaksanaan Tanggung Jawab Pengusaha Travel Tanpa Izin Operasional". Jurnal Analisis Hukum 5 (2):231-44. <https://doi.org/10.38043/jah.v5i2.3741>.

¹³ Kurniasih, Esy, Teguh Rama Prasja, and Anggraini Dwi Milandry. 2022. "Perlindungan Konsumen Dalam Hal Pelaksanaan Tanggung Jawab Pengusaha Travel Tanpa Izin Operasional". Jurnal Analisis Hukum 5 (2):231-44. <https://doi.org/10.38043/jah.v5i2.3741>.

¹⁴ Devi, R. S., & Simarsoit, F. (2020). Perlindungan Hukum Bagi Konsumen E-Commerce Menurut Undang – Undang No.8 Tahun 1999 Tentang Perlindungan Konsumen. JURNAL RECTUM: Tinjauan Yuridis Penanganan Tindak Pidana, 2(2), 119. <https://doi.org/10.46930/jurnalrectum.v2i2.644>

memberikan manfaat dan dapat didayagunakan¹⁵. Dalam konteks e-commerce, perlindungan hukum mencakup berbagai aspek esensial, antara lain perlindungan data pribadi, pemenuhan hak konsumen, keamanan transaksi, dan mekanisme penyelesaian sengketa. UU ITE merupakan salah satu instrumen hukum yang relevan dalam mengatur kegiatan e-commerce di Indonesia. UU ITE mengatur berbagai aspek terkait informasi elektronik dan transaksi elektronik, termasuk ketentuan mengenai perlindungan data pribadi, tanda tangan elektronik, dan perbuatan yang dilarang dalam dunia siber. Selain UU ITE, terdapat pula peraturan perundang-undangan lain yang terkait dengan e-commerce, seperti Undang-Undang Perlindungan Konsumen dan peraturan-peraturan sektoral lainnya¹⁶.

Pemerintah Indonesia telah mengesahkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) No. 1 Tahun 2024 yang diatur dan dilaksanakan secara adil¹⁷ Sebagai respons terhadap pesatnya perkembangan industri e-commerce, pemerintah Indonesia telah mengesahkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) No. 1 Tahun 2024. Tujuan utama dari UU ini adalah memperkuat regulasi untuk melindungi hak konsumen dan menciptakan iklim persaingan usaha yang sehat. UU ITE No. 1 Tahun 2024 menyediakan kerangka hukum yang lebih menyeluruh untuk mengatur kegiatan e-commerce, yang meliputi transaksi elektronik, perlindungan data pribadi, tanggung jawab hukum para pelaku usaha, serta pengawasan dan pemberian sanksi.

uang lingkupnya mencakup e-commerce, media sosial, penyedia layanan aplikasi dan konten, sistem pembayaran elektronik, serta pemasaran digital.

¹⁵ Nur, Nurwati, Adi Sulistiyono, and Martin Roestamy. 2020. "MODEL PENGEMBANGAN JAMINAN FIDUSIA BAGI PEMILIK HAK CIPTA KARYA MUSIK DAN LAGU SEBAGAI OBJEK JAMINAN UNTUK MENDAPATKAN KREDIT PERBANKAN DI INDONESIA". *Jurnal Sosial Humaniora* 11 (2):190-202. <https://doi.org/10.30997/jsh.v11i2.3123>.

¹⁶ Dewa Gede Ananta Prasetya, Anak Agung Sagung Laksmi Dewi, dan Ni Made Puspasutari Ujjianti, "Tinjauan Yuridis Industri E-Commerce Dalam Melakukan Kegiatan Transaksi Online," *Jurnal Konstruksi Hukum* 3, no. 2 (April 2022): 365-370, <https://doi.org/10.22225/jkh.3.2.4838.365-370>.

¹⁷ Aridhayandi, M. Rendi, Achmad Rifqi Nurchi Fari, Usamah Habiburrahman, and Jajang Jajang. 2020. "Optimalisasi Fungsi Kepala Desa Dalam Pelayanan Publik Di Era Revolusi Industri 4.0". *Jurnal MSDA (Manajemen Sumber Daya Aparatur)* 8 (1), 28-38.

Implementasi UU ITE No. 1 Tahun 2024 memiliki dampak signifikan terhadap industri e-commerce. Para pelaku usaha e-commerce kini memiliki tanggung jawab hukum yang lebih besar, termasuk kewajiban untuk memastikan keamanan data konsumen, keabsahan transaksi, serta kualitas produk dan layanan yang ditawarkan. Selain itu, terdapat kewajiban bagi seluruh pelaku usaha e-commerce, termasuk toko online individu dan UMKM, untuk melakukan registrasi dan memperoleh izin guna meningkatkan transparansi dan akuntabilitas. Pelanggaran terhadap ketentuan dapat dikenai sanksi pidana maupun administratif yang cukup berat. Bagi pelaku usaha yang tidak memenuhi kewajiban registrasi dan perizinan, UU ini menerapkan sanksi yang cukup serius, mulai dari denda hingga penutupan sementara atau permanen platform digital. Penerapan UU ITE No. 1 Tahun 2024 turut berkontribusi dalam menciptakan keseimbangan antara hukum konvensional dan digital¹⁸. Undang-undang ini mewajibkan setiap pelaku usaha e-commerce untuk menjamin kerahasiaan dan keamanan informasi sensitif milik konsumen, termasuk data pribadi, riwayat transaksi, serta detail pembayaran.

Penegakan hukum merujuk pada tindakan yang dilakukan oleh aparat penegak hukum untuk menerapkan ketentuan peraturan perundang-undangan, menindak pelaku tindak pidana, serta memberikan sanksi kepada mereka yang melanggar hukum. Pemerintah Indonesia, melalui Kementerian Komunikasi dan Informatika (Kemkominfo), menegaskan bahwa perlindungan konsumen dalam transaksi digital sudah diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Peraturan Pemerintah No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE). Konsumen yang merasa dirugikan dalam transaksi online dapat merujuk pada Pasal 28 ayat 1 UU ITE yang mengatur tentang kerugian

¹⁸ Shona Azi, RR. Desy Priatni, Indah Pujiati, Aria Wijaya, Aditya Dinda Rahmani, Josuhua Gumanti, Wawan Kustiawan, and Elli Ruslina. 2024. "Peran UU ITE Dalam Regulasi E-Commerce Di Era Digital". *Jurnal Ilmu Hukum, Humaniora Dan Politik* 5 (1):258-67. <https://doi.org/10.38035/jihhp.v5i1.2900>.

konsumen. Pasal ini melarang penyebaran berita bohong dan menyesatkan yang dapat merugikan konsumen dalam transaksi elektronik. Pelanggaran terhadap ketentuan ini dapat dikenakan sanksi pidana.

Selain UU ITE, Undang-Undang Perlindungan Konsumen (UU PK) juga memiliki peran penting dalam melindungi hak-hak konsumen dalam transaksi e-commerce. UU PK mengatur tentang hak dan kewajiban antara konsumen dan pelaku usaha, serta mekanisme penyelesaian sengketa konsumen. UU PK memberikan perlindungan kepada konsumen yang merasa hak-haknya dilanggar atau dirugikan oleh pelaku usaha. Dalam UU PK, terdapat pengaturan yang rinci mengenai hak-hak konsumen, yang juga berlaku bagi konsumen yang terlibat dalam transaksi elektronik atau e-commerce. Beberapa hak konsumen yang diatur dalam UU PK antara lain:

- Hak atas Informasi yang Akurat, Lengkap, dan Jujur: Konsumen berhak menerima informasi yang jelas, tepat, dan tidak menyesatkan mengenai produk atau layanan yang ditawarkan dalam e-commerce. Ini termasuk informasi terkait harga, spesifikasi, kualitas, dan kondisi barang/layanan.
- Hak atas Keamanan dan Perlindungan: Konsumen berhak mendapatkan jaminan keselamatan dan perlindungan dalam menggunakan produk atau layanan yang dibeli melalui e-commerce, yang mencakup perlindungan dari risiko yang dapat membahayakan kesehatan, keselamatan, atau harta benda konsumen.
- Hak untuk Memilih Produk atau Layanan: Konsumen berhak memilih produk atau layanan yang sesuai dengan kebutuhan, preferensi, dan kemampuan finansial mereka dalam transaksi e-commerce.

- Hak untuk Menyampaikan Pendapat dan Keluhan: Konsumen berhak mengajukan pendapat, keluhan, atau umpan balik kepada pelaku usaha terkait pengalaman mereka dalam menggunakan barang atau jasa yang dibeli secara online. Pelaku usaha wajib merespons dan menangani keluhan konsumen dengan baik.

Peraturan perundang-undangan yang dapat digunakan sebagai acuan, antara lain regulasi-regulasi berikut ini.

- a. UU No. 10 Tahun 1998 tentang Perbankan. Mengatur Privacy dan data pribadi mengenai nasabah penyimpan dan simpanannya.
- b. UU No. 36 Tahun 1999 tentang Telekomunikasi.
- c. UU No. 39 Tahun 1999 tentang Hak Asasi Manusia. Yaitu perlindungan privasi
- d. UU No. 23 Tahun 2006 tentang Administrasi Kependudukan (telah diubah dengan Undang-Undang No. 24 Tahun 2013).
- e. UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (telah diubah dengan UndangUndang Nomor 19 Tahun 2016),¹⁹melarang penggunaan informasi diperoleh melalui media elektronik yang memuat privasi pada data pribadi yang terkait dengan sebuah individu tanpa persetujuan tersebut orang.

Konsep regulasi yang baik terkait dengan keamanan privasi data harus mencakup hal-hal berikut:

¹⁹ UU No. 36 Tahun 2009 tentang Kesehatan., Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi. Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia. Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (telah diubah dengan Undang-Undang No. 24 Tahun 2013). Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (telah diubah dengan UndangUndang Nomor 19 Tahun 2016)

- a. Prinsip privasi data yang terkandung dalam UUD 1945, khususnya pada Pasal 28G, yang secara eksplisit menyatakan bahwa hak atas perlindungan keamanan data pribadi harus dijaga.
- b. Prinsip keadilan informasi, yang bertujuan memastikan bahwa entitas yang mengumpulkan dan menggunakan data pribadi melakukannya dengan cara yang memadai untuk melindungi data tersebut.
- c. Definisi istilah-istilah substansial yang harus jelas dan tertera dalam regulasi.
- d. Untuk mencapai regulasi yang efektif, diperlukan keterlibatan kedua lembaga dan proses yang saling mendukung (Dewi, 2015).

Kesalahan yang terjadi dalam E-Commerce

1. Sistem Keamanan yang Lemah dan Rentan Terhadap Serangan Siber²⁰
 - Deskripsi: Tidak menerapkan langkah-langkah keamanan yang memadai untuk melindungi data pribadi pelanggan dan informasi transaksi.
 - Implikasi:
 - Kebocoran Data: Peretas dapat mengakses dan mencuri data sensitif seperti nama, alamat, nomor telepon, alamat email, informasi kartu kredit, dan riwayat pembelian.
 - Kerugian Finansial: Konsumen dapat mengalami kerugian finansial akibat penyalahgunaan informasi kartu kredit atau identitas mereka.
 - Kerusakan Reputasi: Kehilangan kepercayaan pelanggan dan citra negatif bagi bisnis e-commerce.
 - Tuntutan Hukum: Potensi tuntutan hukum dari konsumen yang dirugikan.

²⁰ Nia Ramadhani dan Muhammad Irwan Padli Nasution, "Tantangan Dan Solusi Keamanan Siber Dalam Transaksi E-Commerce," *Jurnal Penelitian Sistem Informasi* 2, no. 2 (Mei 2024): 134-144, <https://doi.org/10.54066/jpsi.v2i2.1930>

- Hubungan dengan UU ITE:
 - Pasal 29 UU ITE: Mewajibkan penyelenggara sistem elektronik (termasuk platform e-commerce) untuk melindungi data pribadi pengguna. Kegagalan dalam melindungi data pribadi dapat dianggap sebagai pelanggaran terhadap pasal ini.
 - Ancaman Pidana: Jika kebocoran data disebabkan oleh tindakan sengaja atau kelalaian yang berat, pelaku dapat dijerat dengan pasal-pasal pidana dalam UU ITE yang mengatur tentang akses ilegal ke sistem elektronik dan pencurian data.

- 2. Penyimpanan Data Pribadi yang Tidak Aman
 - Deskripsi: Menyimpan data pribadi pelanggan dalam format yang tidak terenkripsi atau menggunakan sistem penyimpanan yang rentan terhadap akses tidak sah.
 - Implikasi:
 - Peningkatan Risiko Kebocoran Data: Data yang tidak terenkripsi lebih mudah dicuri dan disalahgunakan jika terjadi pelanggaran keamanan.
 - Pelanggaran Privasi: Data pribadi yang bocor dapat digunakan untuk tujuan yang tidak diinginkan, seperti penipuan, spam, atau pencurian identitas.
 - Hubungan dengan UU ITE:
 - Pasal 29 UU ITE: Menekankan kewajiban untuk menjaga kerahasiaan data pribadi. Penyimpanan data yang tidak aman dapat dianggap sebagai pelanggaran terhadap prinsip kerahasiaan ini.
 - Peraturan Pelaksanaan Undang-Undang ITE: Peraturan pemerintah yang mengatur penyelenggaraan sistem elektronik (PP PSTE) memberikan panduan lebih mendetail mengenai cara data pribadi harus disimpan dan dilindungi.

3. Transfer Data Pribadi yang Tidak Terenkripsi

- Deskripsi: Mengirimkan data pribadi pelanggan melalui jaringan internet tanpa menggunakan enkripsi yang kuat.
- Implikasi:
 - Pencegatan Data: Pihak ketiga yang tidak berwenang dapat mencegat dan mencuri data pribadi selama proses transfer.
- Hubungan dengan UU ITE:
 - Prinsip Keamanan: UU ITE dan peraturan pelaksanaannya menekankan pentingnya menggunakan teknologi yang aman untuk melindungi data selama transmisi. Enkripsi adalah salah satu teknologi yang direkomendasikan.

4. Kurangnya Transparansi dalam Penggunaan Data Pribadi

- Deskripsi: Tidak menyediakan informasi yang jelas dan mudah dimengerti kepada pelanggan mengenai cara pengumpulan, penggunaan, dan pembagian data pribadi mereka.
- Implikasi:
 - Kehilangan Kepercayaan: Pelanggan mungkin merasa tidak nyaman atau curiga jika mereka tidak tahu bagaimana data mereka digunakan.
 - Potensi Pelanggaran Privasi: Penggunaan data pribadi yang tidak sesuai dengan harapan pelanggan dapat dianggap sebagai pelanggaran privasi.
- Hubungan dengan UU ITE:
 - Hak Atas Informasi: UU ITE dan Undang-Undang Perlindungan Konsumen memberikan hak kepada konsumen untuk memperoleh informasi yang akurat, transparan, dan jujur mengenai produk dan layanan yang mereka konsumsi, termasuk informasi tentang bagaimana data pribadi mereka dikelola.

5. Tidak Memperbarui Perangkat Lunak dan Sistem Keamanan

- Deskripsi: Tidak secara teratur memperbarui perangkat lunak, sistem operasi, dan aplikasi keamanan yang digunakan oleh platform e-commerce.
- Implikasi:
 - Kerentanan Terhadap Serangan: Perangkat lunak yang tidak diperbarui seringkali memiliki celah keamanan yang dapat dieksploitasi oleh peretas.
- Hubungan dengan UU ITE:
 - Kewajiban Pemeliharaan Sistem: Sebagai penyelenggara sistem elektronik, platform e-commerce memiliki kewajiban untuk memelihara sistem mereka agar tetap aman dan berfungsi dengan baik. Ini termasuk memperbarui perangkat lunak dan sistem keamanan secara teratur.

6. Tidak Melakukan Audit Keamanan Secara Berkala

- Deskripsi: Tidak melaksanakan audit keamanan secara rutin untuk mendeteksi dan memperbaiki potensi kerentanannya dalam sistem.
- Implikasi:
 - Risiko Keamanan yang Tidak Terdeteksi: Tanpa audit keamanan, kerentanan dalam sistem dapat tetap tidak terdeteksi dan menjadi target potensial bagi peretas.

7. Kurangnya Kesadaran dan Pelatihan Keamanan bagi Karyawan

- Deskripsi: Tidak memberikan pelatihan yang memadai kepada karyawan tentang praktik keamanan yang baik, seperti cara mengenali serangan phishing, membuat kata sandi yang kuat, dan melindungi data pribadi pelanggan.
- Implikasi:

- Kesalahan Manusia: Karyawan yang tidak terlatih dapat melakukan kesalahan yang membahayakan keamanan sistem, seperti mengklik tautan berbahaya atau mengungkapkan informasi sensitif kepada pihak yang tidak berwenang.

8. Penggunaan Kata Sandi yang Lemah

- Deskripsi: Pelanggan menggunakan kata sandi yang mudah ditebak atau menggunakan kata sandi yang sama untuk beberapa akun.
- Implikasi:
 - Akses Tidak Sah: Peretas dapat dengan mudah menebak atau memecahkan kata sandi yang lemah dan mendapatkan akses tidak sah ke akun pelanggan.

9. Tidak Menggunakan Otentikasi Dua Faktor (2FA)

- Deskripsi: Tidak mengaktifkan atau menawarkan opsi otentikasi dua faktor (2FA) kepada pelanggan.
- Implikasi:
 - Kurangnya Lapisan Keamanan Tambahan: 2FA memberikan lapisan keamanan tambahan dengan meminta pengguna untuk memberikan kode verifikasi selain kata sandi saat masuk ke akun mereka. Tanpa 2FA, akun lebih rentan terhadap peretasan.

contoh kasus *e-commerce* terkait data pribadi yang diambil dari jurnal-jurnal penelitian, dengan deskripsi yang jelas:

1. **Bukalapak (2020):** Pada November 2020, Bukalapak mengumumkan terjadinya kebocoran data yang melibatkan informasi pribadi sekitar 13 juta pengguna. Data yang bocor mencakup nama lengkap, alamat email, nomor telepon, dan alamat pengiriman. Kebocoran ini terjadi akibat serangan siber

yang memanfaatkan celah keamanan dalam sistem Bukalapak. Dampaknya berpotensi membahayakan privasi dan keamanan pengguna, dengan risiko penipuan dan spam.

2. **Tokopedia (2020):** Pada 2 Mei 2020, Tokopedia mengalami kebocoran data yang mempengaruhi 91 juta akun pengguna. Informasi yang bocor mencakup nama, alamat email, nomor telepon, tanggal lahir, dan password yang di-hash. Data ini kemudian diperjualbelikan di dark web. Kasus ini menimbulkan kekhawatiran publik dan perbincangan mengenai keamanan data serta perlindungan privasi pengguna e-commerce. Tokopedia dinilai gagal dalam menyediakan sistem elektronik yang aman, andal, dan bertanggung jawab.
3. **Lazada (Tidak ada tanggal spesifik):** Kasus yang melibatkan Amir Salim dan Lazada Indonesia, di mana pelaku usaha di platform Lazada Indonesia melakukan kelalaian yang menyebabkan kebocoran data pengguna.
4. **eBay (2014):** Pada 2014, situs lelang online eBay mengalami kebocoran data besar-besaran. Hacker berhasil mengakses basis data pengguna dan mencuri informasi pribadi lebih dari 145 juta akun pengguna, termasuk nama, alamat, nomor telepon, dan data login. Meskipun kata sandi yang bocor terenkripsi, sebagian besar kata sandi lemah dapat dengan mudah dipecahkan. Insiden ini menyebabkan hilangnya kepercayaan konsumen terhadap eBay dan menyoroti pentingnya perlindungan data pribadi yang lebih baik oleh perusahaan.
5. **Target (2013):** Pada 2013, Target, jaringan toko ritel di Amerika Serikat, mengalami kebocoran data besar. Hacker berhasil mencuri informasi kartu kredit dan debit dari lebih dari 40 juta pelanggan Target.
6. **Home Depot (2014):** Pada 2014, Home Depot, peritel peralatan rumah tangga, menjadi korban serangan siber yang mengakibatkan kebocoran data

pelanggan. Peretas berhasil mencuri informasi dari sekitar 56 juta kartu kredit dan debit yang digunakan di toko mereka di Amerika Serikat dan Kanada. Serangan ini terjadi antara April dan September 2014, dengan para peretas memperoleh akses melalui kredensial vendor pihak ketiga, lalu mengeksploitasi kerentanan zero-day di Microsoft Windows untuk meningkatkan hak akses dan menyebar di seluruh jaringan. Mereka juga memasang malware khusus di sistem self-checkout. yang dirancang untuk mencuri informasi kartu pembayaran dan alamat *email* pelanggan²¹.

Contoh-contoh kasus ini menggambarkan pentingnya keamanan data dan perlindungan privasi dalam ekosistem *e-commerce*. Pelanggaran data tidak hanya merugikan konsumen tetapi juga dapat merusak reputasi perusahaan dan melanggar regulasi yang berlaku

Pada tahun 2023, nilai transaksi *e-commerce* mencapai Rp 453 triliun dan diproyeksikan tumbuh 2,8 persen menjadi Rp 487 triliun pada tahun 2024 yang berarti naik 2,5%²². Untuk mendukung pertumbuhan ini, Kementerian Perdagangan (Kemendag) telah mengeluarkan berbagai regulasi, termasuk Permendag No. 31/2023 yang mengatur tentang Perizinan Berusaha, Periklanan, Pembinaan, dan Pengawasan Pelaku Usaha dalam Perdagangan Melalui Sistem Elektronik. Regulasi ini bertujuan menciptakan ekosistem *e-commerce* yang sehat dan adil, serta melindungi konsumen dan UMKM. UU ITE, UU Perlindungan Konsumen (UU PK), dan peraturan terkait lainnya menjadi dasar hukum penting dalam mengatur dan melindungi konsumen serta pelaku usaha di ekosistem *e-commerce* yang terus berkembang di Indonesia. Pemerintah dan pihak terkait terus berupaya memperkuat regulasi, meningkatkan pengawasan, serta membangun kesadaran masyarakat tentang pentingnya

²¹ Erna Priliasari, "Perlindungan Data Pribadi Konsumen dalam Transaksi E-Commerce Menurut Peraturan Perundang-Undangan di Indonesia," *Volume 12 Nomor 2* (Agustus 2023)

²² Budi sebagai Menteri Perdagangan (Mendag) dalam rapat bersama Komisi VI DPR RI di Kompleks Parlemen, Senayan, Jakarta, Rabu (20/11/2024). <https://www.tribunnews.com/bisnis/2024/11/20/nilai-transaksi-e-commerce-indonesia-tahun-ini-diproyeksikan-tembus-rp-487-triliun>.

perlindungan data pribadi dan keamanan di era digital. Dengan pengakuan terhadap transaksi elektronik dan dokumen elektronik dalam UU ITE, e-commerce kini memiliki kepastian hukum. Selain itu, untuk memperbaiki pemantauan dan penegakan hukum di dunia digital, kerjasama antara pemerintah, lembaga penegak hukum, dan platform bisnis online sangat diperlukan.

Bisnis e-commerce diatur oleh berbagai perangkat hukum, di antaranya adalah Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

Aktivitas e-commerce di Indonesia berada dalam lingkup pengaturan yang kompleks, melibatkan berbagai peraturan perundang-undangan yang saling terkait. Kerangka hukum ini mencakup aspek perdagangan secara umum, transaksi elektronik, perlindungan konsumen, dan keamanan data pribadi.

1. Undang-Undang Nomor 7 Tahun 2014 tentang Perdagangan (UU Perdagangan)

- Fokus: UU Perdagangan mengatur tata cara kegiatan yang berkaitan dengan transaksi barang dan/atau jasa, baik di dalam negeri maupun lintas negara, dengan tujuan untuk mengalihkan hak atas barang dan/atau jasa sebagai bentuk imbalan atau kompensasi²³.
- Definisi E-commerce: UU ini "Perdagangan melalui Sistem Elektronik" didefinisikan sebagai kegiatan perdagangan yang transaksinya dilakukan melalui berbagai perangkat dan prosedur elektronik.
- Relevansi: UU Perdagangan memberikan landasan hukum bagi pengaturan e-commerce sebagai bagian dari sistem perdagangan nasional. Meskipun demikian, UU ini lebih berfokus pada aspek perdagangan secara umum dan belum secara spesifik mengatur isu-isu

²³ Johannes Johny Koynja, Sofwan, Rusnan, dan Erlies Septiana Nurbani, "Transaksi Perdagangan Melalui Sistem Elektronik Oleh Pelaku Usaha E-Commerce Dalam Memenuhi Target Penerimaan Perpajakan," *Jurnal Kompilasi Hukum* 4, no. 2 (Desember 2019).

yang unik dalam e-commerce, seperti perlindungan data pribadi dan keamanan transaksi elektronik.

2. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP STE)

- Fokus: PP STE mengatur penyelenggaraan sistem dan transaksi elektronik, termasuk aspek keamanan, perlindungan data pribadi, dan tanda tangan elektronik.
- Transaksi Elektronik: Peraturan Pemerintah ini mengartikan transaksi elektronik sebagai tindakan hukum yang dilakukan dengan memanfaatkan komputer, jaringan komputer, dan/atau media elektronik lainnya.
- Relevansi: PP STE memberikan kerangka hukum yang lebih rinci tentang bagaimana transaksi elektronik harus dilakukan secara aman dan terpercaya. PP ini juga mengatur tanggung jawab Penyelenggara Sistem Elektronik (PSE), termasuk platform e-commerce, dalam melindungi data pribadi pengguna.

3. Rancangan Peraturan Pemerintah tentang Transaksi Elektronik (RPP E-commerce)

- Status: Kementerian Perdagangan (Kemendag) telah mewacanakan pembentukan RPP E-commerce selama beberapa tahun terakhir. Namun, hingga saat ini, RPP tersebut belum disahkan menjadi peraturan pemerintah.
- Tujuan: RPP E-commerce bertujuan untuk memberikan pengaturan yang lebih komprehensif dan spesifik terhadap transaksi e-commerce, mencakup aspek perizinan, perlindungan konsumen, keamanan data, dan persaingan usaha yang sehat.
- Potensi Dampak: Jika disahkan, RPP E-commerce diharapkan dapat memberikan kepastian hukum yang lebih besar bagi pelaku usaha dan konsumen dalam ekosistem e-commerce.

4. Kitab Undang-Undang Hukum Perdata (KUH Perdata)

- Fokus: KUH Perdata mengatur berbagai aspek hukum perdata, termasuk hukum perjanjian, perikatan, dan jual beli.
- Relevansi: Ketentuan dalam KUH Perdata mengenai perjanjian jual beli berlaku secara umum untuk transaksi e-commerce. Prinsip-prinsip seperti kebebasan berkontrak, itikad baik, dan ganti rugi dapat diterapkan dalam sengketa yang timbul dalam transaksi e-commerce.

Dalam Kitab Undang-Undang Hukum Perdata (KUHPer) Pasal 1457, jual beli diartikan sebagai suatu perjanjian di mana salah satu pihak berkomitmen untuk menyerahkan barang, sementara pihak lainnya berjanji untuk membayar harga yang disepakati. Dalam konteks tradisional, seperti di supermarket, jual beli terjadi saat pembeli melakukan pembayaran di kasir; tindakan penjual yang menampilkan barang dengan harga tertentu dianggap sebagai komitmen untuk menyerahkan barang tersebut setelah pembayaran. Pembayaran oleh pembeli dianggap sebagai persetujuan terhadap harga, sehingga perjanjian jual beli pun sah. Jika terjadi insiden kebocoran data pribadi pada platform e-commerce, konsumen yang terdampak memiliki beberapa pilihan untuk menuntut keadilan dan mendapatkan ganti rugi atas kerugian yang dialami.

Upaya hukum ini diatur dalam berbagai peraturan perundang-undangan di Indonesia, termasuk UU PDP dan KUH Perdata.

1. Pengaduan kepada Menteri Komunikasi dan Informatika

- Dasar Hukum: Pasal 26 huruf b UU PDP memberikan hak kepada pemilik data pribadi (dalam hal ini, konsumen) untuk mengajukan pengaduan kepada Menteri Komunikasi dan Informatika apabila terjadi kegagalan dalam perlindungan data pribadi mereka. Pengaduan ini ditujukan kepada pemerintah sebagai regulator untuk melakukan investigasi dan memberikan sanksi kepada pihak yang lalai dalam melindungi data pribadi konsumen.

- **Prosedur:** Konsumen dapat mengajukan pengaduan secara tertulis kepada Menteri Komunikasi dan Informatika dengan menyertakan bukti-bukti yang relevan, seperti tangkapan layar (screenshot) notifikasi kebocoran data, bukti transaksi di platform e-commerce, dan/atau dokumen identitas diri.
 - **Tindak Lanjut:** Setelah menerima pengaduan, Menteri Komunikasi dan Informatika akan melakukan investigasi terhadap platform e-commerce yang diduga melakukan pelanggaran. Jika terbukti bersalah, platform e-commerce dapat dikenakan sanksi administratif berupa teguran tertulis, denda, atau bahkan pencabutan izin usaha.
2. Gugatan Perdata atas Dasar Kelalaian
- **Dasar Hukum:** Pasal 1366 KUH Perdata mengatur tentang tanggung jawab atas kerugian yang disebabkan oleh kelalaian. Dalam konteks kebocoran data, konsumen dapat mengajukan gugatan perdata kepada platform e-commerce dengan dasar bahwa platform tersebut telah lalai dalam menjaga keamanan data pribadi konsumen, sehingga menyebabkan terjadinya kebocoran data.
 - **Unsur Kelalaian:** Untuk memenangkan gugatan perdata, konsumen harus membuktikan adanya unsur kelalaian dari pihak platform e-commerce. Beberapa indikator kelalaian antara lain:
 - **Sistem keamanan yang tidak memadai:** Platform e-commerce tidak menerapkan standar keamanan yang tinggi untuk melindungi data pribadi konsumen.
 - **Tidak melakukan audit keamanan secara berkala:** Platform e-commerce tidak melakukan pemeriksaan rutin terhadap sistem keamanan mereka untuk mengidentifikasi dan mengatasi potensi kerentanan.
 - **Kurangnya pengawasan terhadap karyawan:** Platform e-commerce tidak memberikan pelatihan yang cukup kepada karyawan mengenai pentingnya keamanan data dan cara mencegah kebocoran data.
 - **Ganti Rugi:** Jika gugatan dikabulkan oleh pengadilan, platform e-commerce wajib membayar ganti rugi kepada konsumen yang dirugikan. Ganti rugi

dapat berupa penggantian biaya yang telah dikeluarkan, ganti rugi atas kerugian materiil (misalnya, kerugian akibat penyalahgunaan informasi kartu kredit), dan/atau ganti rugi atas kerugian immateriil (misalnya, ganti rugi atas rasa malu atau stres yang dialami akibat kebocoran data).

3. Penyelesaian Sengketa Alternatif

- Dasar Hukum: Pasal 64 UU PDP memberikan opsi bagi konsumen dan platform e-commerce untuk menyelesaikan sengketa melalui mekanisme penyelesaian sengketa alternatif, seperti arbitrase, mediasi, atau konsiliasi.
- Keuntungan: Penyelesaian sengketa alternatif umumnya lebih cepat, lebih murah, dan lebih fleksibel dibandingkan dengan proses pengadilan. Selain itu, penyelesaian sengketa alternatif juga dapat menjaga hubungan baik antara konsumen dan platform e-commerce.
- Lembaga Penyelesaian Sengketa: Konsumen dan platform e-commerce dapat memilih lembaga penyelesaian sengketa yang terpercaya dan memiliki reputasi baik. Beberapa lembaga penyelesaian sengketa yang ada di Indonesia antara lain Badan Arbitrase Nasional Indonesia (BANI) dan Badan Mediasi Nasional (BMN).

Alat Bukti yang Sah Dalam mengajukan upaya hukum terkait kebocoran data pribadi, konsumen perlu melengkapi diri dengan alat bukti yang sah. Beberapa contoh alat bukti yang dapat digunakan antara lain:

- Tangkapan layar (screenshot) notifikasi kebocoran data dari platform e-commerce atau media massa.
- Bukti transaksi di platform e-commerce yang menunjukkan bahwa konsumen pernah memberikan data pribadi kepada platform tersebut.
- Surat elektronik (e-mail) atau pesan teks (SMS) dari pihak yang tidak dikenal yang mencurigakan (misalnya, upaya penipuan atau phishing).
- Laporan dari bank atau lembaga keuangan yang menunjukkan adanya transaksi yang tidak sah atau mencurigakan setelah terjadinya kebocoran data.

- Surat keterangan dari dokter atau psikolog yang menyatakan bahwa konsumen mengalami gangguan kesehatan akibat kebocoran data.

KESIMPULAN (PALATINO LINOTYPE, 12, BOLD, SPASI 1.5)

Pesatnya perkembangan e-commerce di Indonesia menghadirkan kemudahan bagi konsumen dan peluang bisnis yang luas, namun juga memunculkan tantangan serius terkait perlindungan data pribadi. Insiden kebocoran data yang berulang kali terjadi mengindikasikan adanya kerentanan dalam sistem keamanan platform e-commerce serta minimnya akuntabilitas dalam pengelolaan data. Indonesia telah memiliki kerangka hukum yang mengatur perlindungan data pribadi, termasuk di dalamnya. UU ITE, UU Perlindungan Konsumen, dan terutama UU PDP yang menjadi tonggak penting dalam menciptakan aturan komprehensif terkait pengumpulan, penggunaan, dan pengungkapan data pribadi. UU Perlindungan Data Pribadi (PDP) menjamin hak setiap warga negara untuk melindungi data pribadinya dan meningkatkan kesadaran masyarakat mengenai pentingnya perlindungan data pribadi. Efektivitas perlindungan hukum sangat bergantung pada implementasi yang kuat dan penegakan hukum yang tegas. Beberapa tantangan utama meliputi sistem keamanan yang lemah pada platform e-commerce, kurangnya transparansi informasi mengenai penggunaan data pribadi konsumen, rendahnya kesadaran konsumen mengenai hak-hak mereka, serta penegakan hukum yang belum optimal. Untuk meningkatkan perlindungan data pribadi, diperlukan upaya bersama dari berbagai pihak:

- **Peningkatan Keamanan:** Platform e-commerce harus meningkatkan sistem keamanan dengan standar yang tinggi, audit berkala, dan pelatihan karyawan.
- **Peningkatan Transparansi:** Platform harus memberikan informasi yang jelas mengenai kebijakan privasi dan bagaimana data dikelola.
- **Peningkatan Kesadaran:** Pemerintah, organisasi konsumen, dan platform e-commerce perlu meningkatkan kesadaran konsumen tentang hak-hak mereka.

- **Penegakan Hukum yang Lebih Efektif:** Aparat penegak hukum harus meningkatkan kemampuan dalam menangani kasus pelanggaran data.
- **Penguatan Regulasi:** Pemerintah perlu memperkuat regulasi dan memberikan kewenangan lebih besar kepada lembaga pengawas.

Konsumen juga harus aktif dalam menjaga keamanan data pribadi dengan menggunakan kata sandi yang kuat, mengaktifkan otentikasi dua faktor, dan berhati-hati saat memberikan informasi secara online. Perlindungan data pribadi merupakan tanggung jawab bersama untuk menciptakan ekosistem e-commerce yang aman, tepercaya, dan menguntungkan bagi semua pihak.

REFERENSI

- Achmad, Qorie Claudi, Nurwati, and Dadang Suprijatna. 2024. "Penyelesaian Sengketa Merek 'Strong' Dalam Perspektif Prinsip Konstitutif (Studi Putusan Mahkamah Agung Nomor 332K/Pdt.Sus.HKI/Merek/2021)". *Karimah Tauhid* 3 (1):63-79. <https://doi.org/10.30997/karimahtauhid.v3i1.10858>.
- Ardika, I Wayan Cenic. 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. <https://doi.org/10.47134/ijlj.v2i3.3601>.
- Aridhayandi, M. Rendi, Achmad Rifqi Nurchi Fari, Usamah Habiburrachman, and Jajang Jajang. 2020. "Optimalisasi Fungsi Kepala Desa Dalam Pelayanan Publik Di Era Revolusi Industri 4.0". *Jurnal MSDA (Manajemen Sumber Daya Aparatur)* 8 (1), 28-38.
- Ayu, S. S., & Nasution, M. I. P. (2023). Analisis Kebocoran Data Privacy Pada E-Commerce Tokopedia. *JUEB: Jurnal Ekonomi dan Bisnis*, 2(3).

Budi sebagai Menteri Perdagangan (Mendag) dalam rapat bersama Komisi VI DPR RI di Kompleks Parlemen, Senayan, Jakarta, Rabu (20/11/2024).

<https://www.tribunnews.com/bisnis/2024/11/20/nilai-transaksi-e-commerce-indonesia-tahun-ini-diproeksikan-tembus-rp-487-triliun>.

Devi, R. S., & Simarsoit, F. (2020). Perlindungan Hukum Bagi Konsumen E-Commerce Menurut Undang – Undang No.8 Tahun 1999 Tentang Perlindungan Konsumen. JURNAL RECTUM: Tinjauan Yuridis Penanganan Tindak Pidana, 2(2), 119. <https://doi.org/10.46930/jurnalrectum.v2i2.644>

Dewa Gede Ananta Prasetya, Anak Agung Sagung Laksmi Dewi, dan Ni Made Puspasutari Ujianti, "Tinjauan Yuridis Industri E-Commerce Dalam Melakukan Kegiatan Transaksi