

PERLINDUNGAN HUKUM ATAS DATA PRIBADI DALAM PERJANJIAN ELEKTRONIK PADA PLATFORM E-COMMERCE: STUDI KASUS TOKOPEDIA

Fakhri Mujahidi ; Indah Maulani, SH.,MH.
Program Ilmu Hukum, Fakultas Hukum Dan Ilmu Politik
Universitas Muhammdiyah Surakarta

Abstrak

Perkembangan teknologi informasi mendorong pesatnya penggunaan e-commerce, namun juga menimbulkan permasalahan terkait perlindungan data pribadi konsumen. Kasus kebocoran data pada platform Tokopedia menunjukkan adanya kesenjangan antara pengaturan hukum dan implementasinya, sehingga menimbulkan keraguan terhadap efektivitas perlindungan hukum dalam perjanjian elektronik. Penelitian ini bertujuan untuk menganalisis bentuk pelanggaran dalam praktik perjanjian elektronik pada Tokopedia serta mengkaji perlindungan hukum terhadap data pribadi konsumen berdasarkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Pelindungan Data Pribadi (UU PDP). Metode yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan dan bersifat deskriptif, menggunakan data sekunder yang dianalisis secara kualitatif. Hasil penelitian menunjukkan bahwa pelanggaran meliputi akses ilegal terhadap data pribadi, kegagalan perlindungan dan keamanan sistem elektronik, serta kebocoran dan penyebaran data pribadi, yang tidak hanya disebabkan oleh pihak eksternal tetapi juga kelemahan internal penyelenggara sistem elektronik. Perlindungan hukum dilakukan secara preventif melalui kewajiban penyedia sistem dalam menjamin keamanan data, serta secara represif melalui sanksi administratif dan pidana serta hak ganti rugi bagi korban. Namun, pelaksanaannya belum optimal karena kendala pembuktian, keterbatasan penelusuran pelaku lintas negara, serta penegakan hukum yang masih reaktif, sehingga efektivitas perlindungan data pribadi sangat bergantung pada implementasi dan sinergi antar pihak.

Kata Kunci: *perlindungan hukum, data pribadi, perjanjian elektronik, Tokopedia*

Abstract

The evolution of information technology encourages the rapid use of e-commerce, but it also raises problems related to the protection of consumers' personal data. The case of data leak on the Tokopedia platform shows that there is a gap between legal regulation and its implementation, thus casting doubt on the effectiveness of legal protection in electronic agreements. This study aims to analyze the form of violations in the practice of electronic agreements on Tokopedia and examine the legal protection of consumer personal data based on the Electronic Information and Transaction Law (ITE Law) and the Personal Data Protection Law (PDP Law). The method used is normative legal research with a statutory and descriptive approach, using secondary data that is analyzed qualitatively. The results of the study show that violations include illegal access to personal data, failure to protect and secure electronic systems, as well as leakage and dissemination of personal data, which are not only caused by external parties but also internal weaknesses of electronic system operators. Legal protection is carried out preventively through the obligation of the system provider to ensure data security, as well as repressively through administrative and criminal sanctions and the right to compensation for victims. However, its implementation is not optimal due to evidentiary constraints, limited cross-border tracing of perpetrators, and law enforcement that is still reactive, so the effectiveness of personal data protection is highly dependent on implementation and synergy between parties.

Keywords: *legal protection, personal data, electronic agreements, Tokopedia*

1. PENDAHULUAN

Perdagangan merupakan aktivitas ekonomi yang berpengaruh besar terhadap distribusi barang dan jasa, sekaligus menjadi salah satu faktor utama yang mendorong perubahan dalam kehidupan masyarakat modern¹. Melalui kegiatan perdagangan, tingkat kemakmuran dan stabilitas ekonomi suatu negara dapat tercermin. Seiring dengan kemajuan teknologi informasi dan komunikasi, aktivitas perdagangan kini tidak lagi terbatas pada interaksi konvensional, melainkan telah bertransformasi ke dalam bentuk digital yang lebih cepat dan efisien. Perkembangan ini semakin didorong oleh pesatnya kemajuan internet di Indonesia, terutama dengan dukungan pemerintah yang terus memperluas infrastruktur digital hingga menjangkau berbagai daerah, termasuk wilayah pedesaan. Akses internet yang semakin merata menjadikan teknologi digital sebagai bagian penting dalam kehidupan masyarakat dan membuka peluang besar bagi pemanfaatannya dalam berbagai sektor, termasuk perdagangan yang kini semakin mengandalkan platform daring sebagai sarana utama transaksi². Evolusi teknologi tersebut kemudian melahirkan sistem perdagangan elektronik atau *electronic commerce (e-commerce)*.

E-commerce adalah kegiatan transaksi perdagangan yang mencakup barang, jasa, maupun informasi yang dilakukan melalui jaringan internet secara daring. Perkembangan *e-commerce* sebagai bentuk modernisasi perdagangan digital telah menciptakan pola interaksi ekonomi yang berbeda dari sistem konvensional. Sistem ini memiliki karakteristik tersendiri dibandingkan perdagangan konvensional karena menciptakan ruang interaksi tanpa batas antara penjual dan pembeli³. Melalui *e-commerce*, proses transaksi dapat dilakukan tanpa adanya pertemuan langsung, dengan memanfaatkan jaringan internet yang dapat diakses dari berbagai waktu dan lokasi.

Perkembangan pesat *e-commerce* menjadi bukti bahwa teknologi telah menjadi bagian penting dalam kehidupan ekonomi masyarakat. Perkembangan tersebut dapat dilihat secara nyata melalui peningkatan jumlah pengguna platform *e-commerce* di Indonesia dalam beberapa tahun ke belakang. Data menunjukkan bahwa tren pengguna *e-commerce* terus mengalami pertumbuhan signifikan setiap tahunnya, sejalan dengan meningkatnya penetrasi internet dan

¹ Tia Deja Pohan and others, 'Perlindungan Hukum Data Pribadi Konsumen Dalam', 1.3 (2023), 42–48.

² S. Abidin, Z., Thoif, M., & Marwiyah, 'Perlindungan Hukum Konsumen Atas Ketidakjelasan Informasi Oleh Pelaku Usaha Dalam Perjanjian E-Commerce Menurut Hukum Perdata Dan Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen', *Paper Knowledge . Toward a Media History of Documents*, 7.2 (2025), 107–15 <<https://aksiologi.org/index.php/courtreview/article/view/2079>>.

³ David Banjarhanor, 'Konsepsi Perlindungan Hukum Konsumen Anak Yang Masuk Dalam Segmentasi Pasar Digital (E-Commerce)', *Gorontalo Law Review*, 5.1 (2022), 27–40 <<https://jurnal.unigo.ac.id/index.php/golrev/article/view/2036/918>>.

perubahan perilaku konsumsi masyarakat menuju transaksi digital⁴.

Namun, seiring dengan meningkatnya intensitas transaksi digital, interaksi ekonomi masyarakat di dunia maya juga menimbulkan konsekuensi baru yang berkaitan dengan penggunaan dan penyimpanan data pribadi. Masyarakat sebagai pengguna sering memberikan data pribadi saat bertransaksi jual beli. Salah satu data yang diberikan adalah alamat IP (*Internet Protocol*). Alamat IP ini berfungsi sebagai identitas unik untuk membedakan pengguna internet satu dengan yang lainnya di seluruh dunia. Kondisi ini berpotensi menimbulkan berbagai bentuk kejahatan di dunia maya (*cybercrime*), terutama yang berkaitan dengan pelanggaran terhadap perlindungan data pribadi (*the protection of privacy rights*).

Menurut data Kementerian Komunikasi dan Informatika (Kominfo), periode 2019–Juni 2023 mencatat 94 kasus kebocoran data, dengan puncak 35 kasus pada 2022; sekitar 28 kasus disebabkan kelemahan sistem atau keamanan siber. Hal ini menunjukkan bahwa kebocoran data merupakan masalah nyata yang terus meningkat, sehingga pengaturan perlindungan data pribadi dalam transaksi elektronik menjadi sangat penting.

Salah satu contoh nyata adalah kebocoran data pengguna Tokopedia pada 2020. Sebagai pelopor e-commerce di Indonesia, platform ini menyediakan berbagai produk dengan harga kompetitif serta fitur pencarian dan katalog yang memudahkan konsumen berbelanja⁵. Pada peristiwa tersebut, sekitar 91 juta akun pengguna dilaporkan terdampak kebocoran data yang kemudian diperjualbelikan di forum daring, meliputi informasi penting seperti nama, alamat email, dan nomor telepon pengguna⁶. Kasus ini memicu gugatan hukum terhadap Tokopedia karena dinilai tidak menjalankan kewajiban perlindungan data konsumen secara optimal.

Kasus serupa juga terjadi pada platform Bukalapak, di mana seorang anggota forum peretas mengklaim memiliki data sekitar 13 juta akun pengguna yang bocor dan dijual di forum online pada tahun 2019. Dalam postingannya, pelaku melampirkan contoh data yang dijual, berisi informasi nama lengkap pengguna, alamat *e-mail*, dan tanggal lahir. Penjual menawarkan *database* ini kepada siapa saja yang tertarik dengan cara menghubunginya secara pribadi melalui

⁴ Kuan Maharani and Nur Hidayah, 'ANALISIS FAKTOR YANG MEMENGARUHI PERILAKU IMPULSIVE BUYING PADA PENGGUNAAN E-COMMERCE', *Jurnal Akuntansi*, 5.2 (2025), 505–19.

⁵ Fadel Retzen Lupi and Nurdin, 'Analisis Strategi Pemasaran Dan Penjualan', *Jurnal Elektronik Sistem Informasi Dan Komputer*, 2.1 (2016), 20–31.

⁶ Lia Santosa, 'Kominfo Tangani 94 Kasus Kebocoran Data Pribadi Dalam Tiga Tahun', *ANTARA*, 2023 <<https://www.antaraneews.com/berita/3584103/kominfo-tangani-94-kasus-kebocoran-data-pribadi-dalam-tiga-tahun>>.

pesan langsung (*personal message/PM*)⁷. Kedua kasus ini menegaskan bahwa masih terdapat kerentanan signifikan dalam keamanan *cyber* di Indonesia, sekaligus menyoroti urgensi penerapan regulasi yang efektif dan komprehensif guna memberikan perlindungan hukum yang pasti terhadap data pribadi konsumen di ranah digital.

Pemerintah Indonesia telah menetapkan regulasi terkait transaksi elektronik dan perlindungan data pribadi, terutama melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan UU No. 19 Tahun 2016, yang mengatur keabsahan transaksi elektronik dan penggunaan data pribadi harus atas persetujuan pemiliknya. Selain itu, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi hadir sebagai kerangka hukum yang lebih komprehensif dalam pengelolaan data pribadi, termasuk hak subjek data, kewajiban pengendali data, serta sanksi atas pelanggaran⁸⁹.

Meskipun telah terdapat pengaturan dalam Undang-Undang Informasi dan Transaksi Elektronik serta Undang-Undang Pelindungan Data Pribadi, dalam praktiknya masih ditemukan ketidaksesuaian antara norma hukum dengan realitas, khususnya dalam kasus kebocoran data pada platform *e-commerce* seperti Tokopedia. Keberadaan regulasi yang secara normatif telah mengatur kewajiban perlindungan data pribadi belum sepenuhnya mampu menjamin keamanan data konsumen dalam praktik penyelenggaraan sistem elektronik. Di samping itu, penerapan klausula baku dalam perjanjian elektronik juga memiliki potensi mengalihkan atau membatasi tanggung jawab pelaku usaha terhadap perlindungan data pribadi konsumen. Kondisi ini menunjukkan adanya persoalan yuridis terkait efektivitas perlindungan data pribadi dalam perjanjian elektronik, sehingga perlu dianalisis kesesuaiannya antara norma hukum dan praktik di lapangan..

2. METODE

Penelitian ini merupakan penelitian hukum normatif dengan pendekatan perundang-undangan (*statute approach*) yang berfokus pada pengkajian norma, asas, dan doktrin hukum terkait perlindungan data pribadi dalam perjanjian elektronik. Metode yang digunakan bersifat deskriptif untuk memberikan gambaran secara sistematis dan komprehensif mengenai ketentuan hukum yang berlaku serta penerapannya. Data yang digunakan adalah data sekunder yang terdiri

⁷ Wahyunanda Pertiwi and Oik Yusuf, 'Anggota Forum Hacker Klaim Punya Data 13 Juta Akun Bukalapak Sumber: <https://Tekno.Kompas.Com/Read/2020/05/06/09390047/Anggota-Forum-Hacker-Klaim-Punya-Data-13-Juta-Akun-Bukalapak>. Membership: <https://Kmp.Im/Plus6> Download Aplikasi: <https://Kmp.Im/App6>', *Kompas.Com*.

⁸ Indonesia, *Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik* (Indonesia: Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952, Pasal 26 ayat (1), 2016).

⁹ Indonesia, *Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi*, 2022.

dari: (1) bahan hukum primer meliputi Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta KUHP; dan (2) bahan hukum sekunder berupa jurnal, buku, dan pendapat ahli. Pengumpulan data dilakukan melalui studi kepustakaan (library research) dengan menelaah berbagai sumber hukum yang relevan. Analisis data dilakukan secara kualitatif melalui pendekatan normatif dengan penafsiran peraturan perundang-undangan, serta menggunakan pola pikir deduktif untuk menarik kesimpulan dari ketentuan umum ke dalam kasus konkret yang diteliti.

3. HASIL DAN PEMBAHASAN

3.1 Bentuk Pelanggaran dalam Praktik Perjanjian Elektronik pada Platform Tokopedia

3.1.1 Akses Ilegal terhadap Data Pribadi (*Unauthorized Access*)

Kejahatan *illegal access* (akses ilegal) merupakan tindakan memasuki atau menembus sistem keamanan milik individu maupun korporasi tanpa hak, baik untuk memperoleh informasi maupun keuntungan tertentu.¹⁰ Dalam konteks kebocoran data pada platform Tokopedia, dapat diidentifikasi ke dalam dua bentuk pelanggaran utama. Pertama, peretasan (*unauthorized access*) terhadap sistem elektronik, yaitu tindakan menembus sistem keamanan sehingga pelaku dapat masuk ke dalam sistem yang seharusnya dilindungi. Kedua, penguasaan data pribadi tanpa hak oleh pihak yang tidak berwenang, yang ditunjukkan dari keberhasilan pelaku memperoleh dan mengendalikan data pengguna dalam jumlah besar, meliputi alamat email, nama pengguna, serta kata sandi yang telah dienkripsi. Kedua bentuk pelanggaran ini terlihat dari keberhasilan pelaku mengakses sistem elektronik secara tidak sah hingga mengakibatkan terbukanya data pribadi pengguna dalam jumlah besar.

Selaras dengan ketentuan Pasal 65 Undang-Undang Perlindungan Data Pribadi (UU PDP) yang menegaskan larangan terhadap setiap tindakan memperoleh, mengakses, maupun menggunakan data pribadi tanpa dasar hak atau persetujuan yang sah dari subjek data. Larangan tersebut tidak hanya mencakup pengumpulan dan pengungkapan data tanpa kewenangan, tetapi juga pemanfaatannya untuk tujuan tertentu, termasuk memperoleh keuntungan ekonomi bagi diri sendiri maupun pihak lain.¹¹ Dalam konteks kebocoran data Tokopedia, ketentuan ini menjadi sangat relevan karena

¹⁰ Aplikasi Angkutan and others, 'Peretasan Terhadap Sistem Elektronik Pada Aplikasi Angkutan Umum', *Qawanin Jurnal Ilmu Hukum*, 1.1 (2020), 59–71.

¹¹ Komang Arundati and others, 'PELINDUNGAN HUKUM DATA PRIBADI DALAM TRANSAKSI NON FUNGIBLE TOKEN (NFT) BERDASARKAN UNDANG- UNDANG NOMOR 27 TAHUN 2022 PELINDUNGAN HUKUM DATA PRIBADI DALAM TRANSAKSI NON FUNGIBLE TOKEN (NFT) BERDASARKAN UNDANG- UNDANG NOMOR 27 TAHUN 2022', 4.2 (2026).

tindakan peretasan tidak hanya berhenti pada akses ilegal, tetapi juga berlanjut pada penyebaran serta komersialisasi data di ruang siber. Secara substantif, peristiwa ini mencerminkan adanya pelanggaran berlapis, yakni pelanggaran terhadap hak privasi akibat akses tanpa persetujuan, serta penyalahgunaan data yang kemudian diperjualbelikan sebagai komoditas ilegal di forum *dark web*. Hal tersebut menandakan bahwa aspek keamanan dan privasi pemilik data pribadi masih belum mendapatkan perlindungan yang memadai.¹² Kondisi ini sekaligus mengindikasikan bahwa pelanggaran data pribadi telah berkembang menjadi kejahatan yang kompleks dan sistematis, dengan dampak yang luas, baik bagi individu maupun terhadap tingkat kepercayaan publik dalam ekosistem digital. Penurunan kepercayaan ini pada akhirnya memengaruhi hak konsumen atas rasa aman dan perlindungan dalam bertransaksi secara elektronik¹³.

Dalam perspektif Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), tindakan peretasan dalam kasus kebocoran data Tokopedia dapat dikualifikasikan sebagai pelanggaran terhadap Pasal 30 ayat (1), (2), dan (3), yang secara tegas melarang setiap bentuk pengaksesan secara tidak berwenang terhadap sistem elektronik milik pihak lain.¹⁴ Ketentuan ini menegaskan bahwa setiap upaya memasuki atau menguasai sistem elektronik tanpa kewenangan merupakan perbuatan yang dilarang secara hukum. Fakta bahwa pelaku berhasil menembus sistem dan memperoleh puluhan juta data pengguna menunjukkan telah terjadinya akses ilegal terhadap sistem yang seharusnya dilindungi. Lebih lanjut, penyebaran dan praktik penjualan data hasil peretasan di forum *dark web* memperlihatkan bahwa akses tersebut tidak hanya dilakukan secara tidak sah, tetapi juga dimanfaatkan untuk tujuan tertentu yang berpotensi menimbulkan kerugian bagi pihak lain.

3.1.2 Kegagalan Perlindungan dan Keamanan Sistem Elektronik

Kebocoran data yang terjadi akibat peretasan hingga berujung pada praktik penjualan data pribadi menunjukkan bahwa Tokopedia belum sepenuhnya menjalankan prinsip perlindungan data pribadi, khususnya dalam mencegah akses dan pengungkapan data secara tidak sah.¹⁵ Kondisi ini mengindikasikan adanya kelemahan mendasar dalam sistem perlindungan data pribadi yang dikelola oleh penyelenggara sistem elektronik. Skala kebocoran yang mencapai puluhan juta data pengguna menunjukkan adanya celah keamanan (*security vulnerability*) yang tidak mampu diantisipasi secara efektif, sehingga mencerminkan bahwa mekanisme pengamanan yang diterapkan belum didukung

¹² Hikmal Yusu Argiansyah and M. Rizki Yudha Prawira, 'Analisis Hukum Hak Atas Privasi Dan Perlindungan.Pdf', *JURNAL HUKUM PELITA*, 5.1 (2024), 61–75.

¹³ Mohamad Soleh and Zubakhrum Tjenreng, 'STRATEGI PENCEGAHAN KEBOCORAN DATA PELAYANAN PUBLIK', *Jurnal Kajian Pemerintah (JKP)*, 11.1 (2024), 1–10.

¹⁴ Rayhan Wira Sadewa and others, 'Arus Jurnal Sosial Dan Humaniora (AJSH) Analisis Yuridis Kebocoran Data Pelanggan Pada Platform Tokopedia Dan Tanggungjawab Terhadap Perlindungan Hukum Konsumen', 5.2 (2025).

¹⁵ Maichle Delpiero and others, 'Analisis Yuridis Kebijakan Privasi Dan Pertanggungjawaban Online Marketplace Dalam Perlindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data', 9 (2021).

oleh sistem perlindungan yang komprehensif, terutama dalam aspek pencegahan, deteksi dini, serta mitigasi terhadap serangan siber.

Selanjutnya, Tokopedia juga dapat dinilai tidak memenuhi ketentuan Pasal 2 ayat (2) dan Pasal 28 huruf C Permenkominfo Nomor 20 Tahun 2019, khususnya terkait kewajiban penyampaian informasi secara transparan dalam hal terjadinya kebocoran data pribadi. Pada tahap awal insiden, Tokopedia hanya mengumumkan adanya kebocoran data serta memberikan pernyataan bahwa keamanan kata sandi dan akun keuangan pengguna tetap terpelihara. Namun, fakta yang kemudian terungkap menunjukkan bahwa sekitar 91 juta akun pengguna, yang memuat berbagai data pribadi, telah diakses oleh pihak tidak berwenang. Kondisi ini mengindikasikan bahwa informasi yang disampaikan kepada publik belum sepenuhnya mencerminkan keadaan yang sebenarnya, sehingga menimbulkan pertanyaan terhadap tingkat transparansi dalam penanganan insiden tersebut.¹⁶

Dalam perspektif hukum, ketentuan Pasal 35 dan Pasal 36 Undang-Undang Perlindungan Data Pribadi (UU PDP) menempatkan tanggung jawab aktif pada pengendali data untuk menjamin keamanan informasi sejak tahap penyimpanan hingga perlindungan dari potensi ancaman eksternal. Apabila dikaitkan dengan fakta kebocoran data Tokopedia, terungkap bahwa jutaan data pengguna dapat diakses oleh pihak yang tidak sah dan kemudian tersebar di ruang siber, yang menunjukkan bahwa mekanisme pengamanan tidak mampu mencegah terjadinya penetrasi maupun membatasi dampaknya. Keberhasilan pelaku memperoleh data dalam jumlah besar sekaligus memperjualbelikannya di forum *dark web* menandakan bahwa sistem pengawasan dan pengendalian akses belum berjalan secara efektif, serta upaya pencegahan terhadap ancaman siber belum diterapkan secara optimal. Kondisi ini tidak hanya mencerminkan adanya pelanggaran oleh pihak luar, tetapi juga mengindikasikan bahwa tanggung jawab hukum dalam menjaga keamanan data belum dilaksanakan secara maksimal. Selain itu, kebocoran data pribadi juga menimbulkan dampak serius bagi individu yang datanya tersebar, baik dari segi keamanan, privasi, maupun potensi kerugian yang dapat ditimbulkan.¹⁷

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) memberikan landasan hukum bagi penyelenggara sistem elektronik untuk bertanggung jawab terhadap penyelenggaraan sistem yang aman dan andal tepatnya pada Pasal 15 ayat (1) UU ITE menegaskan bahwa setiap penyelenggara sistem elektronik wajib memastikan sistemnya

¹⁶ Sinta Sukma Ayu, Muhammad Irwan, and Padli Nasution, 'Analisis Kebocoran Data Privacy Pada E-Commerce Tokopedia', *Jurnal Ekonomi Dan Bisnis (JUEB)*, 2.3 (2023).

¹⁷ Lambok Tambunan, 'Urgensi Rancangan Undang-Undang (Ruu) Perlindungan Data Pribadi', *Jurnal Hukum UNISSULA*, 37.2 (2024), 119–33.

terlindungi dari segala bentuk gangguan, baik internal maupun eksternal.¹⁸ Dalam konteks ini, tingkat kepercayaan dalam dunia maya (*online trust*) sangat dipengaruhi oleh perlindungan terhadap privasi dan data pribadi, di mana lemahnya perlindungan berpotensi menyebabkan data jatuh ke pihak yang tidak bertanggung jawab, sehingga dapat menimbulkan kerugian finansial dan bahkan mengancam aspek keamanan pemilik data.¹⁹

Namun, kebocoran data skala besar pada kasus Tokopedia menunjukkan bahwa kewajiban perlindungan belum diimplementasikan secara optimal. Akses dan penyebaran data pengguna mengindikasikan kelemahan tidak hanya pada aspek teknis, tetapi juga pada tata kelola keamanan, termasuk identifikasi risiko, deteksi serangan, dan respons insiden. Hal ini menegaskan perlunya penguatan infrastruktur keamanan, manajemen risiko, dan konsistensi penerapan kewajiban hukum agar perlindungan data pribadi berjalan efektif.

3.1.3 Kebocoran dan Penyebaran Data Pribadi

Dalam praktik transaksi elektronik, penyelenggara sistem elektronik memiliki kewajiban hukum untuk menjamin keamanan, keandalan, dan perlindungan data pribadi pengguna. Kewajiban tersebut merupakan konsekuensi dari penguasaan dan pengendalian sistem elektronik yang digunakan dalam kegiatan perdagangan digital. Secara normatif, penyelenggara sistem elektronik dimaknai sebagai setiap individu, instansi pemerintah, badan usaha, maupun kelompok masyarakat yang bertindak secara individu atau berkelompok menyelenggarakan, mengatur, dan/atau mengoperasikan suatu sistem elektronik untuk dimanfaatkan oleh pengguna, baik untuk kepentingan sendiri maupun untuk kepentingan pihak lain²⁰. Dalam konteks platform perdagangan elektronik seperti Tokopedia, posisi tersebut menempatkan penyelenggara sebagai pihak yang berwenang dan bertanggung jawab dalam pengelolaan data pribadi konsumen.

Berdasarkan literatur, penyelenggara sistem elektronik wajib mematuhi ketentuan perlindungan data pribadi pada setiap tahap pengolahan, mulai dari pengumpulan dengan persetujuan pemilik data hingga pemrosesan yang akurat, bertanggung jawab, dan sesuai tujuan. Selain itu, pengelolaan data harus menjamin keamanan dari risiko seperti kehilangan, penyalahgunaan, dan akses tidak sah, serta dilakukan secara transparan terkait tujuan, proses, dan upaya perlindungannya. Di samping itu, penyelenggara juga wajib melakukan pengakhiran atau

¹⁸ Hidayat.

¹⁹ Andi Wahyuddin Nur and others, 'Tanggung Jawab Pelaksana Sistem Elektronik Dalam Melindungi Informasi Pemakai Media Sosial Menurut Undang-Undang Nomor 19 Tahun 2016 Mengenai Informasi Dan Transaksi Elektronik', *LEGAL: Journal of Law*, 3.1 (2024), 18–29.

²⁰ MENTERI KOMUNIKASI DAN DIGITAL REPUBLIK INDONESIA, *PERATURAN MENTERI KOMUNIKASI DAN DIGITAL REPUBLIK INDONESIA* (Indonesia, 2025), p. 2.

penghapusan data pribadi apabila data tersebut sudah tidak diperlukan lagi, kecuali terdapat kewajiban hukum yang mengharuskan penyimpanannya.²¹

Apabila dikaitkan dengan kasus kebocoran data Tokopedia, prinsip-prinsip tersebut menjadi parameter untuk menilai tingkat kepatuhan penyelenggara dalam melindungi data pribadi. Fakta menunjukkan bahwa terjadi akses tidak sah oleh pihak eksternal yang mengakibatkan terbukanya data pengguna dalam jumlah sangat besar, yang kemudian tidak hanya berhenti pada tahap penguasaan, tetapi berlanjut pada penyebaran serta praktik komersialisasi di ruang siber. Kondisi ini menunjukkan bahwa mekanisme perlindungan yang seharusnya mampu mencegah terjadinya pengungkapan data justru tidak berjalan secara efektif, sehingga membuka ruang bagi distribusi data secara luas tanpa kendali.

Secara yuridis, tindakan tersebut bertentangan dengan Pasal 65 Undang-Undang Perlindungan Data Pribadi (UU PDP) yang melarang setiap bentuk perolehan, akses, maupun pemanfaatan data pribadi tanpa dasar hak yang sah. Dalam konteks ini, pelanggaran tidak semata-mata terjadi pada tahap awal berupa akses ilegal, tetapi juga berlanjut pada pengungkapan dan pemanfaatan data yang diperoleh secara melawan hukum. Hal ini menunjukkan adanya pelanggaran berlapis terhadap rezim perlindungan data pribadi, di mana data yang seharusnya dilindungi justru berubah menjadi objek eksploitasi dalam ekosistem kejahatan siber.

Dalam perspektif Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), perbuatan tersebut juga memenuhi unsur pelanggaran sebagaimana diatur dalam Pasal 32 yang melarang setiap individu dengan sengaja dan tanpa izin memindahkan, mentransfer, atau menyebarkan informasi elektronik kepada pihak lain. Fakta bahwa data pengguna Tokopedia diperjualbelikan di forum *dark web* menunjukkan bahwa informasi elektronik yang bersifat privat telah didistribusikan secara luas tanpa otorisasi, sehingga memperbesar potensi penyalahgunaan oleh oknum yang tidak bertanggung jawab.

Apabila ditinjau dari efektivitas penerapan Pasal 32 UU ITE, terdapat beberapa faktor yang memengaruhi optimal atau tidaknya penegakan ketentuan tersebut. Mengacu pada konsep sistem hukum dalam pandangan Lawrence M. Friedman, keberhasilan hukum ditentukan oleh tiga aspek utama, yaitu substansi hukum, struktur hukum, dan budaya hukum.²² Dari sisi substansi, pengaturan

²¹ Rista Maharani and Andria Luhur Prakoso, 'Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital Protection of Consumer Personal Data by Electronic System Providers in Digital Peningkatan Substansial Dalam Penggunaan Platform E-Commerce Di Indonesia Telah', *USM Law Review*, 7.1 (2024), 333–47.

²² Aditya Sulisty Budhi and others, 'Implementasi Pasal 32 UU No. 11 Tahun 2008 Tentang Perlindungan Data Pribadi Dalam Transaksi Fintech', *Journal of New Trends in Sciences*, 3.3 (2025), 68–77.

dalam Undang-Undang Informasi dan Transaksi Elektronik masih bersifat umum dan belum sepenuhnya menjangkau kompleksitas penyebaran serta komersialisasi data pribadi di era digital, sebagaimana terlihat pada kasus Tokopedia. Dari sisi struktur, keterbatasan koordinasi dan kapasitas penegak hukum menghambat penanganan, terutama pada kasus lintas negara. Sementara dari sisi budaya hukum, rendahnya literasi digital dan kesadaran masyarakat dalam melaporkan pelanggaran turut memperluas dampak kebocoran data. Kondisi ini menunjukkan bahwa meskipun secara normatif Pasal 32 UU ITE telah melarang penyebaran informasi elektronik tanpa hak, dalam praktiknya pada kasus Tokopedia penegakan ketentuan tersebut masih menghadapi berbagai kendala yang menghambat efektivitas perlindungan data pribadi.

Lebih lanjut, kondisi ini menunjukkan bahwa kewajiban penyelenggara sistem elektronik dalam menjamin keamanan dan mencegah penyebaran data pribadi belum optimal, yang berdampak pada menurunnya kepercayaan dan rasa aman pengguna dalam bertransaksi digital. Dengan demikian, kasus ini tidak hanya mencerminkan pelanggaran hukum, tetapi juga lemahnya implementasi prinsip perlindungan data pribadi dalam praktik.. Perlu dipahami bahwa praktik perlindungan data yang diterapkan oleh Tokopedia dapat mengalami perkembangan sesuai dengan kebijakan internal perusahaan dan ketentuan peraturan perundang-undangan yang berlaku²³. Kebocoran dan penyebaran data pribadi dalam peristiwa ini menegaskan pentingnya penguatan sistem keamanan serta kepatuhan terhadap ketentuan hukum guna mencegah terulangnya pelanggaran serupa.

Kebocoran data yang terjadi akibat peretasan hingga berujung pada praktik penjualan data pribadi menunjukkan bahwa Tokopedia belum sepenuhnya menjalankan prinsip perlindungan data pribadi, khususnya dalam mencegah akses dan pengungkapan data secara tidak sah.²⁴ Kondisi ini menunjukkan adanya kelemahan mendasar dalam perlindungan data oleh penyelenggara sistem elektronik. Besarnya skala kebocoran mencerminkan adanya celah keamanan yang belum mampu diantisipasi, sehingga sistem pengamanan belum komprehensif, khususnya dalam aspek pencegahan, deteksi dini, dan mitigasi serangan siber.

Selanjutnya, Tokopedia juga dapat dinilai tidak memenuhi ketentuan Pasal 2 ayat (2) dan Pasal 28 huruf C Permenkominfo Nomor 20 Tahun 2019, khususnya terkait kewajiban penyampaian informasi secara transparan dalam hal terjadinya kebocoran data pribadi. Pada tahap awal insiden, Tokopedia hanya mengumumkan adanya kebocoran data serta memberikan pernyataan bahwa

²³ Husnul Khatimah, 'PERLINDUNGAN HUKUM TERHADAP KONSUMEN DALAM TRANSAKSI JUAL BELI ONLINE DI APLIKASI LAZADA DAN SHOPEE', *LEX LATA: Jurnal Ilmu Hukum*, 4.3 (2023), 384–404.

²⁴ Maichle Delpiero and others, 'Analisis Yuridis Kebijakan Privasi Dan Pertanggungjawaban Online Marketplace Dalam Perlindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data', 9 (2021).

keamanan kata sandi dan akun keuangan pengguna tetap terpelihara. Namun, fakta yang kemudian terungkap menunjukkan bahwa sekitar 91 juta akun pengguna, yang memuat berbagai data pribadi, telah diakses oleh pihak tidak berwenang. Kondisi ini mengindikasikan bahwa informasi yang disampaikan kepada publik belum sepenuhnya mencerminkan keadaan yang sebenarnya, sehingga menimbulkan pertanyaan terhadap tingkat transparansi dalam penanganan insiden tersebut.²⁵

3.2 Bentuk Perlindungan Hukum terhadap Data Pribadi Konsumen dalam Perjanjian Elektronik berdasarkan UU ITE dan UU PDP

3.2.1 Perlindungan Hukum terhadap Akses Ilegal Data Pribadi

Perlindungan data atau informasi berkaitan erat dengan konsep hak privasi sebagaimana menurut pendapat Alan Westin, yang memaknai *information privacy* sebagai hak individu, keluarga, maupun kelompok untuk menentukan batasan atas akses terhadap data pribadinya. Konsep ini kemudian dikembangkan oleh Arthur R. Miller yang menegaskan bahwa privasi data mencerminkan kemampuan seseorang untuk mengendalikan informasi mengenai dirinya, termasuk menentukan sejauh mana informasi tersebut dapat diketahui oleh pihak lain.²⁶ Dengan demikian, setiap bentuk akses terhadap data pribadi yang diakses tanpa persetujuan atau tanpa hak merupakan pelanggaran terhadap hak privasi tersebut.

Dalam perjanjian elektronik pada platform e-commerce, risiko akses ilegal terhadap data pribadi meningkat seiring digitalisasi transaksi. Akses ini umumnya terjadi melalui peretasan oleh pihak tidak berwenang yang memanfaatkan kelemahan sistem untuk memperoleh keuntungan²⁷, selain itu juga melalui pencurian akun maupun eksploitasi celah keamanan lainnya. Kebocoran data pada platform Tokopedia menunjukkan bahwa sistem elektronik yang tidak memiliki perlindungan optimal dapat membuka peluang bagi pihak tidak berwenang untuk mengakses data pengguna dalam jumlah besar. Kasus tersebut tidak hanya menunjukkan kelemahan aspek teknis, tetapi juga menegaskan bahwa perlindungan hak privasi dalam transaksi elektronik masih menghadapi tantangan serius dalam praktik.

Di Indonesia, perlindungan atas akses ilegal data pribadi diwujudkan dengan menggunakan dua pendekatan hukum, yaitu preventif dan represif. Perlindungan hukum preventif diarahkan untuk

²⁵ Sinta Sukma Ayu, Muhammad Irwan, and Padli Nasution, 'Analisis Kebocoran Data Privacy Pada E-Commerce Tokopedia', *Jurnal Ekonomi Dan Bisnis (JUEB)*, 2.3 (2023).

²⁶ Perlindungan Hukum and others, 'PERLINDUNGAN HUKUM POSITIF INDONESIA TERHADAP KEJAHATAN PENYALAHGUNAAN DATA PRIBADI', 2023, 369–92.

²⁷ Russel Butarbutar, 'Kejahatan Siber Terhadap Individu : Jenis , Analisis , Dan Kejahatan Siber Terhadap Individu : Jenis , Analisis , Dan Perkembangannya Fakultas Hukum Universitas Bung Karno', 2.2 (2023) <<https://doi.org/10.21143/TELJ.vol2.no2.1043>>.

melakukan pencegahan agar tidak terjadi pelanggaran yang dapat menimbulkan kerugian. Ketentuan ini secara normatif tercermin dalam Pasal 15 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, yang mewajibkan setiap Penyelenggara Sistem Elektronik untuk melaksanakan penyelenggaraan sistem secara andal, aman, dan bertanggung jawab atas beroperasinya sistem tersebut. Frasa “andal dan aman” mengharuskan penyelenggara menerapkan standar keamanan untuk mencegah akses tanpa hak, seperti keamanan berlapis, enkripsi, dan autentikasi ganda, serta didukung audit berkala, pengelolaan risiko siber, dan pembatasan akses internal.

Di luar aspek teknis, perlindungan preventif juga harus diwujudkan melalui pendekatan non-teknis, seperti edukasi dan sosialisasi kepada pengguna mengenai penggunaan teknologi informasi yang aman, etis, serta pentingnya menjaga kerahasiaan data pribadi.²⁸ Banyak kasus akses ilegal terjadi bukan hanya karena lemahnya sistem, tetapi juga karena rendahnya kesadaran dan pemahaman pengguna terhadap risiko keamanan digital²⁹, seperti membagikan kode OTP atau menggunakan kata sandi yang lemah. Oleh karena itu, tanggung jawab perlindungan data pribadi tidak hanya berada pada penyelenggara sistem elektronik, tetapi juga pada pengguna sebagai subjek data. Pada sisi represif, Pasal 30 dan Pasal 32 Undang-Undang Informasi dan Transaksi Elektronik mengatur larangan akses tanpa hak serta perbuatan pengambilan atau manipulasi data secara ilegal, yang disertai dengan ancaman pidana. Selain itu, Undang-Undang Pelindungan Data Pribadi juga memberikan dasar hukum berupa hukuman administratif maupun pidana terhadap pihak yang dengan melanggar hukum mengakses, mengungkapkan, atau memanfaatkan data pribadi.

Namun demikian, dalam praktik penegakan hukum, perlindungan represif tersebut masih menghadapi sejumlah hambatan. Pertama, kesulitan dalam pembuktian unsur “tanpa hak” dan “melawan hukum”, terutama ketika akses dilakukan melalui sistem elektronik yang kompleks dan melibatkan berbagai pihak. Selanjutnya, hambatan dalam penelusuran pelaku karena kejahatan siber seringkali bersifat lintas wilayah bahkan lintas negara, sehingga menyulitkan proses penegakan yurisdiksi. Pelaku kerap memanfaatkan teknologi untuk menyamarkan identitas atau beroperasi dari luar negeri, yang pada akhirnya menimbulkan kesulitan dalam menentukan hukum yang berlaku serta proses ekstradisi.³⁰ Hal ini menunjukkan bahwa pendekatan represif yang ada saat ini masih bersifat reaktif dan belum sepenuhnya mampu mengimbangi kompleksitas kejahatan siber yang terus berkembang.

²⁸ Mania and others, *ETIKA PROFESI TEKNOLOGI INFORMASI & KOMUNIKASI* (TOHAR MEDIA, 2022).

²⁹ Alieffia Nanda Ervian and Sepriyadi Adhan S, ‘Perlindungan Hukum Terhadap Nasabah Atas Kebocoran Data Pribadi Dalam Layanan Perbankan Digital Di Indonesia’, 2025, 8785–93.

³⁰ Djhpi Mei- and others, ‘The Crisis of Cybercrime Law Enforcement in Indonesia: Obstacles and Solutions’, 2024 <<https://doi.org/10.35905/delictum.v2i2.10613>>.

Kondisi tersebut menunjukkan adanya kesenjangan antara pengaturan normatif dan pelaksanaannya secara faktual di lapangan, khususnya yang berkaitan dengan akses ilegal data pribadi. Secara normatif, Indonesia telah memiliki landasan hukum yang relatif lengkap melalui Undang-Undang Informasi dan Transaksi Elektronik dan Undang-Undang Pelindungan Data Pribadi. Namun, efektivitas perlindungan hukum terhadap akses ilegal data pribadi masih sangat bergantung pada kapasitas penegak hukum, kesiapan infrastruktur keamanan siber, serta tingkat kesadaran masyarakat. Dengan demikian, perlindungan hukum terhadap akses ilegal data pribadi tidak cukup hanya mengandalkan regulasi, tetapi juga memerlukan penguatan implementasi, peningkatan literasi digital, serta koordinasi yang efektif antar lembaga dalam menangani kejahatan siber.

3.2.2 Perlindungan Hukum terhadap Kegagalan Keamanan Sistem Elektronik

Perlindungan hukum terhadap kegagalan keamanan sistem elektronik merupakan aspek krusial dalam memastikan keamanan serta kerahasiaan data pribadi dalam transaksi elektronik. Kegagalan sistem pada konteks ini tidak semata-mata dipahami sebagai gangguan teknis, tetapi juga sebagai bentuk ketidakmampuan penyelenggara sistem elektronik dalam memenuhi kewajiban hukumnya untuk menjaga keandalan dan keamanan sistem.³¹ Kondisi tersebut berdampak pada terganggunya kerahasiaan, integritas, dan ketersediaan data pribadi, sehingga berpotensi menimbulkan pelanggaran terhadap hak privasi, khususnya dalam konteks perlindungan terhadap akses tanpa hak.

Dalam praktik perjanjian elektronik, khususnya pada platform *e-commerce*, sistem elektronik menjadi sarana utama dalam pengelolaan dan penyimpanan data pribadi konsumen. Ketergantungan yang tinggi terhadap sistem ini menyebabkan risiko kegagalan keamanan menjadi semakin kompleks, baik yang berasal dari kelemahan teknis, kesalahan konfigurasi, maupun kurangnya pengawasan terhadap sistem. Oleh karena itu, keamanan sistem elektronik tidak terbatas aspek teknologi, tetapi juga menyangkut tanggung jawab hukum penyelenggara dalam menjamin perlindungan data pribadi pengguna.

Kegagalan keamanan sistem berkorelasi langsung dengan kebocoran data pribadi, sebagaimana terlihat pada kasus Tokopedia. Insiden kebocoran data yang terjadi menunjukkan bahwa kelemahan pada keamanan jaringan dan kontrol akses memungkinkan pihak tidak berwenang memperoleh data pengguna, termasuk *username*, alamat *email*, tanggal lahir, jenis kelamin, nomor telepon, serta kata sandi yang sudah melalui proses enkripsi. Kondisi ini mengindikasikan adanya celah dalam mekanisme perlindungan jaringan serta pengelolaan akses, sehingga membuka

³¹ Hal, Satria, and Ahyar.

kemungkinan bagi pihak ketiga untuk melakukan akses dan menyalahgunakan data pengguna tanpa persetujuan.

Dalam konteks tersebut, peningkatan kapasitas sistem harus diimbangi dengan penguatan keamanan jaringan secara menyeluruh. Perlindungan sistem elektronik tidak cukup hanya berfokus pada aspek pencegahan, tetapi juga harus mencakup kemampuan deteksi dan respons terhadap ancaman secara cepat dan tepat.³² Oleh karena itu, penerapan sistem keamanan yang terintegrasi, disertai dengan audit dan evaluasi keamanan jaringan secara rutin, menjadi langkah strategis untuk mengidentifikasi serta menutup celah yang berpotensi dimanfaatkan oleh pihak tidak bertanggung jawab.

Dari perspektif perlindungan hukum, kegagalan sistem keamanan tersebut menunjukkan adanya kelemahan baik dalam aspek preventif maupun represif. Secara preventif, kegagalan ini mencerminkan belum optimalnya penerapan standar keamanan oleh penyelenggara sistem elektronik, sehingga tidak mampu mencegah terjadinya akses ilegal terhadap data pribadi. Hal ini mengindikasikan adanya kelalaian dalam penerapan standar keamanan, sehingga jutaan data pengguna berisiko diakses dan diperjualbelikan secara tidak sah. Sementara itu, dari sisi represif, respons yang diberikan pasca insiden dinilai belum optimal, terutama dalam hal pemberitahuan kepada pengguna serta pemulihan kerugian yang ditimbulkan.³³ Kondisi ini menunjukkan bahwa perlindungan hukum terhadap subjek data belum terlaksana secara optimal, baik dari sisi pencegahan maupun pemulihan.

Secara yuridis, hubungan antara pengguna dan penyelenggara platform e-commerce didasarkan pada perjanjian yang termuat dalam *terms and conditions*, sehingga menimbulkan hubungan hukum kontraktual.³⁴ Dalam hal terjadi kebocoran data akibat kegagalan sistem, penyelenggara sistem elektronik wajib memberikan pemberitahuan kepada pemilik data sebagaimana diatur dalam Peraturan Pemerintah Nomor 71 Tahun 2019. Selain itu, pengguna memiliki hak untuk mengajukan tuntutan kompensasi atau ganti rugi berdasarkan Undang-Undang Informasi dan Transaksi Elektronik apabila data digunakan di luar kesepakatan. Tanggung jawab penyelenggara dalam hal ini dapat berasaskan wanprestasi maupun tindakan melawan hukum (*onrechtmatige daad*), khususnya apabila terdapat unsur kelalaian dalam menjaga keamanan sistem elektronik. Dengan

³² Business Technology, 'Keamanan Jaringan Komputer Dalam Bisnis E-Commerce (Studi Kasus : Kebocoran Data Tokopedia 2020)', 1.4 (2025), 73–77.

³³ Ragil Putri Anindya and Achmad Edi Subiyanto, 'Tanggung Jawab Platform Tokopedia Dalam Kasus Kebocoran Data Menurut Undang-Undang Tentang Perlindungan Data Pribadi', 4.3 (2025), 1105–12.

³⁴ Maldi Omar Muhammad and Lucky Dafira Nugroho, 'Perlindungan Hukum Terhadap Pengguna Aplikasi E-Commerce Yang Terdampak Kebocoran Data Pribadi', *Jurnal Pamator : Jurnal Ilmiah Universitas Trunojoyo*, 14.2 (2021), 165–74.

demikian, kegagalan dalam melindungi data pribadi akibat lemahnya sistem keamanan dapat menimbulkan konsekuensi hukum berupa kewajiban pertanggungjawaban terhadap kerugian yang dialami pengguna.

Lebih lanjut, secara normatif, perlindungan hukum terhadap kegagalan keamanan sistem elektronik diatur dalam Undang-Undang Informasi dan Transaksi Elektronik yang mewajibkan penyelenggara sistem elektronik untuk menjamin keandalan dan keamanan sistemnya, serta Undang-Undang Pelindungan Data Pribadi yang menetapkan kewajiban pengendali data dalam melindungi data pribadi serta memberikan konsekuensi administratif serta pidana atas pelanggaran yang terjadi. Ketentuan mengenai sanksi administratif diatur dalam Pasal 57, sedangkan sanksi pidana diatur dalam Pasal 67 hingga Pasal 73, yang memuat ketentuan pidana penjara dan/atau denda bagi pihak yang secara ilegal mengakses dan mengungkapkan data pribadi. Namun demikian, dalam kasus kebocoran data Tokopedia tahun 2020, penerapan sanksi berdasarkan Undang-Undang Pelindungan Data Pribadi belum dapat diberlakukan secara langsung karena terhalang oleh asas non-retroaktif, sehingga ketentuan tersebut tidak dapat diterapkan terhadap peristiwa yang terjadi sebelum undang-undang tersebut diundangkan.³⁵

Dalam praktiknya, perlindungan hukum masih menghadapi keterbatasan, terutama karena penyelenggara sistem elektronik cenderung hanya berfokus pada upaya internal dalam menjaga keamanan data.³⁶ Apabila terjadi kebocoran, mekanisme penyelesaian sengketa yang diinisiasi oleh penyelenggara belum berjalan secara optimal. Akibatnya, perlindungan hukum yang tersedia cenderung bersifat reaktif dan menempatkan konsumen sebagai pihak yang harus proaktif dalam memperjuangkan haknya melalui jalur hukum.

Dari uraian tersebut, dapat disimpulkan bahwa meskipun secara normatif Indonesia telah memiliki kerangka hukum yang cukup komprehensif, efektivitas perlindungan hukum terhadap kegagalan keamanan sistem elektronik masih menghadapi berbagai tantangan dalam implementasinya. Maka diperlukan penguatan dalam aspek pengawasan, peningkatan standar keamanan sistem, serta mekanisme penegakan hukum yang lebih responsif dan fleksibel terhadap perkembangan teknologi. Dengan adanya penguatan tersebut, diharapkan perlindungan data pribadi dalam sistem elektronik dapat terlaksana secara lebih efektif serta mampu meningkatkan kepercayaan masyarakat terhadap ekosistem digital.

³⁵ Anindya and Subiyanto.

³⁶ Journal Honeste Vivere, 'PERLINDUNGAN KONSUMEN ATAS RISIKO KEAMANAN INFORMASI DALAM TRANSAKSI E-COMMERCE', 32.2 (2022), 98–107.

3.2.3 Perlindungan Hukum terhadap Kebocoran dan Penyebaran Data Pribadi

Perlindungan data pribadi mencerminkan penghormatan terhadap privasi seseorang, baik individu maupun kelompok. Dalam perkembangannya, perlindungan data pribadi dipandang sebagai bagian dari hak asasi manusia yang mendasar, sehingga memerlukan kerangka hukum yang kuat dan komprehensif. Pembentukan Undang-Undang Pelindungan Data Pribadi didasarkan pada prinsip-prinsip utama, seperti perlindungan informasi pribadi, kepastian hukum, penghormatan terhadap hak subjek data, kehati-hatian, keseimbangan kepentingan, akuntabilitas, serta kerahasiaan.³⁷ Prinsip-prinsip tersebut menjadi landasan dalam menjamin bahwa setiap pengelolaan data pribadi dilakukan secara bertanggung jawab dan tidak merugikan pemilik data.

Dalam konteks transaksi elektronik, kebocoran dan penyebaran data pribadi dapat dipandang sebagai bentuk pelanggaran yang lebih serius dibandingkan sekadar akses ilegal. Hal ini karena pelanggaran tidak hanya berupa akses tanpa hak, tetapi juga mencakup penggunaan, pengungkapan, dan distribusi data kepada pihak lain tanpa persetujuan. Kondisi ini secara langsung melanggar hak privasi dan berpotensi menimbulkan kerugian, baik secara materiil maupun immateriil, seperti penyalahgunaan identitas, penipuan, hingga hilangnya kepercayaan pengguna terhadap platform digital. Kasus kebocoran data pada platform Tokopedia menjadi salah satu contoh konkret pelanggaran tersebut. Kebocoran yang melibatkan sekitar 91 juta data pengguna menunjukkan bahwa data pribadi seperti *username*, *e-mail*, nomor telepon, hingga kata sandi yang terenkripsi dapat diakses dan diduga diperjualbelikan melalui media ilegal seperti dark web tanpa persetujuan pemilik data. Hal ini menegaskan bahwa kebocoran data tidak hanya berhenti pada kegagalan sistem, tetapi juga berlanjut pada penyebaran data yang memperbesar risiko kerugian bagi pengguna.

Dari sisi hukum, respons terhadap kasus tersebut juga terlihat melalui Komunitas Konsumen Indonesia (KKI) yang mengajukan gugatan terhadap Menteri Komunikasi dan Informatika serta Tokopedia di Pengadilan Negeri Jakarta Pusat dengan nomor perkara 235/Pdt.G/PN.Jkt.Pst. Dalam putusan sela 21 Oktober 2020, majelis hakim menolak gugatan dan mengabulkan eksepsi tergugat karena tidak berwenang mengadili, serta menyatakan sengketa seharusnya diajukan ke PTUN akibat keterlibatan Kementerian Komunikasi dan Informatika.³⁸ Putusan ini menegaskan bahwa perlindungan hukum tidak sepenuhnya bergantung pada aturan yang ada, tetapi juga pada ketepatan pengadilan yang berwenang mengadili perkara.

³⁷ Ema Irmawati, John Pieries, and Wiwik Sri Widiarty, 'PERLINDUNGAN HUKUM ATAS DATA PRIBADI NASABAH BANK PENGGUNA MOBILE BANGKING DALAM PERSPEKTIF UU NO 27 TAHUN 2022 TENTANG KEBOCORAN DATA', 5.1 (2024).

³⁸ Tokopedia Studi and Normatif Dan, 'Kebocoran 91 Juta Data Pribadi Konsumen Aplikasi Tokopedia: Studi Normatif Dan Tanggungjawab', 13 (2025), 1–11.

Secara normatif, perlindungan terhadap kebocoran dan penyebaran data pribadi telah diatur dalam berbagai ketentuan peraturan perundang-undangan. Dalam Undang-Undang Informasi dan Transaksi Elektronik, Pasal 26 memberikan hak kepada pemilik data untuk mengajukan gugatan apabila data pribadinya digunakan tanpa izin. Sementara itu, Undang-Undang Pelindungan Data Pribadi secara lebih tegas mengatur larangan pengungkapan dan penyebaran data pribadi tanpa hak, serta menetapkan sanksi administratif dan pidana. Ketentuan sanksi administratif diatur dalam Pasal 57, sedangkan sanksi pidana diatur dalam Pasal 67 hingga Pasal 73, yang mencakup ancaman pidana penjara dan/atau denda dalam jumlah besar bagi pelaku pelanggaran.

Selain itu, pengendali data seperti Tokopedia bertanggung jawab memastikan keamanan data pribadi pengguna. Berdasarkan Pasal 47 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, pelanggaran kewajiban tersebut dapat dikenai sanksi administratif seperti denda hingga 2% dari penghasilan tahunan, peringatan tertulis, hingga penonaktifan sementara kegiatan. Ketentuan ini menunjukkan bahwa tanggung jawab pengendali data tidak hanya bersifat moral, tetapi juga berimplikasi secara hukum apabila terjadi kelalaian. Di sisi lain, prinsip akuntabilitas dalam Undang-Undang Pelindungan Data Pribadi menuntut pengendali data bertanggung jawab atas seluruh proses pengelolaan data. Dalam konteks ini, kebocoran data Tokopedia menunjukkan bahwa lemahnya penerapan prinsip kehati-hatian dan pengawasan dapat berujung pada pelanggaran hak subjek data.³⁹

Perlindungan hukum tidak hanya menjadi tanggung jawab penyelenggara sistem elektronik, tetapi juga membutuhkan peran aktif dari pengguna. Sebagai langkah preventif, pengguna perlu meningkatkan kesadaran dalam menjaga keamanan data pribadi, seperti tidak menyebarkan informasi sensitif secara sembarangan, menerapkan kata sandi yang aman dan kuat, serta memanfaatkan sistem keamanan tambahan seperti *two-step verification*. Kesadaran ini menjadi penting mengingat banyak kasus kebocoran data juga dipicu oleh kelalaian pengguna dalam menjaga keamanan akun mereka.⁴⁰

Dengan demikian, keberadaan Undang-Undang Pelindungan Data Pribadi diharapkan mampu menjadi instrumen yang efektif dalam mewujudkan lingkungan digital yang aman dan adil bagi semua pihak. Namun, efektivitasnya sangat bergantung pada implementasi, kesadaran, dan komitmen seluruh pihak dalam menjamin perlindungan data pribadi sebagai bagian dari hak asasi manusia.

4. PENUTUP

Praktik perjanjian elektronik pada platform Tokopedia menunjukkan bahwa pelanggaran data pribadi berupa akses ilegal, kegagalan perlindungan sistem, serta kebocoran dan penyebaran

³⁹ Sukarelawati Permana and others, 'PENGATURAN PERLINDUNGAN DATA PRIBADI Sukarelawati Permana Keywords ', 8 (2022), 386–414 <<https://doi.org/10.25123/vej.v8i2.5213>>.

⁴⁰ Irmawati, Pieries, and Widiarty.

data merupakan bentuk pelanggaran yang tidak hanya disebabkan oleh pihak eksternal seperti peretas, tetapi juga berkaitan dengan kelemahan internal penyelenggara sistem elektronik dalam mengelola dan melindungi data pengguna. Kondisi tersebut menunjukkan bahwa kewajiban hukum dalam menjamin keamanan dan keandalan sistem sebagaimana diatur dalam Undang-Undang Informasi dan Transaksi Elektronik dan Undang-Undang Pelindungan Data Pribadi belum sepenuhnya diimplementasikan secara optimal.

Perlindungan hukum terhadap data pribadi konsumen dalam perjanjian elektronik pada dasarnya telah tersedia melalui mekanisme preventif dan represif, baik dalam bentuk kewajiban penyelenggara sistem elektronik untuk menjaga keamanan data maupun melalui sanksi administratif, pidana, dan hak ganti rugi bagi korban. Namun, efektivitas perlindungan data pribadi masih terkendala pembuktian kejahatan siber, sifat lintas negara, dan penegakan hukum yang belum optimal. Karena itu, keberhasilannya tidak hanya bergantung pada norma hukum, tetapi juga implementasi, kapasitas penegak hukum, serta kesadaran para pihak. Diperlukan peningkatan pengawasan dan penegakan hukum, serta perbaikan keamanan dan transparansi oleh penyelenggara seperti Tokopedia.

DAFTAR PUSTAKA

- Abidin, Z., Thoif, M., & Marwiyah, S., 'Perlindungan Hukum Konsumen Atas Ketidakjelasan Informasi Oleh Pelaku Usaha Dalam Perjanjian E-Commerce Menurut Hukum Perdata Dan Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen', *Paper Knowledge . Toward a Media History of Documents*, 7 (2025), 107–15
<<https://aksiologi.org/index.php/courtreview/article/view/2079>>
- Angkutan, Aplikasi, Umum □ Risman, Hi Mustafa, Mulyati Pawennai, and Mursyid Mursyid, 'Peretasan Terhadap Sistem Elektronik Pada Aplikasi Angkutan Umum', *Qawanin Jurnal Ilmu Hukum*, 1 (2020), 59–71
- Anindya, Ragil Putri, and Achmad Edi Subiyanto, 'Tanggung Jawab Platform Tokopedia Dalam Kasus Kebocoran Data Menurut Undang-Undang Tentang Perlindungan Data Pribadi', 4 (2025), 1105–12
- Argiansyah, Hikmal Yusu, and M. Rizki Yudha Prawira, 'Analisis Hukum Hak Atas Privasi Dan Perlindungan.Pdf', *JURNAL HUKUM PELITA*, 5 (2024), 61–75
- Arundati, Komang, Putri Rajendra, Ida Bagus, Yoga Raditya, Universitas Udayana, Dauh Puri Klod, and others, 'PELINDUNGAN HUKUM DATA PRIBADI DALAM TRANSAKSI NON FUNGIBLE TOKEN (NFT) BERDASARKAN UNDANG- UNDANG NOMOR 27 TAHUN 2022 PELINDUNGAN HUKUM DATA PRIBADI DALAM TRANSAKSI NON FUNGIBLE TOKEN (NFT) BERDASARKAN UNDANG- UNDANG NOMOR 27 TAHUN 2022', 4 (2026)
- Ayu, Sinta Sukma, Muhammad Irwan, and Padli Nasution, 'Analisis Kebocoran Data Privacy Pada E-Commerce Tokopedia', *Jurnal Ekonomi Dan Bisnis (JUEB)*, 2 (2023)
- Banjarhanor, David, 'Konsepsi Perlindungan Hukum Konsumen Anak Yang Masuk Dalam Segmentasi Pasar Digital (E-Commerce)', *Gorontalo Law Review*, 5 (2022), 27–40
<<https://jurnal.unigo.ac.id/index.php/golrev/article/view/2036/918>>
- Budhi, Aditya Sulistyo, Aditya Sulistyo Budhi, Widi Nugrahaningsih, and Ety Isworo, 'Implementasi Pasal 32 UU No. 11 Tahun 2008 Tentang Perlindungan Data Pribadi Dalam Transaksi Fintech', *Journal of New Trends in Sciences*, 3 (2025), 68–77

- Butarbutar, Russel, 'Kejahatan Siber Terhadap Individu : Jenis , Analisis , Dan Kejahatan Siber Terhadap Individu : Jenis , Analisis , Dan Perkembangannya Fakultas Hukum Universitas Bung Karno', 2 (2023) <<https://doi.org/10.21143/TELJ.vol2.no2.1043>>
- Delpiero, Maichle, Farah Azzahra Reynaldi, Istiawati Utami Ningdiah, and Nafisah Muthmainnah, 'Analisis Yuridis Kebijakan Privasi Dan Pertanggungjawaban Online Marketplace Dalam Perlindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data', 9 (2021)
- Ervian, Alieffa Nanda, and Sepriyadi Adhan S, 'Perlindungan Hukum Terhadap Nasabah Atas Kebocoran Data Pribadi Dalam Layanan Perbankan Digital Di Indonesia', 2025, 8785–93
- Hukum, Perlindungan, Positif Indonesia, Kejahatan Penyalahgunaan, and Data Pribadi, 'PERLINDUNGAN HUKUM POSITIF INDONESIA TERHADAP KEJAHATAN PENYALAHGUNAAN DATA PRIBADI', 2023, 369–92
- Indonesia, *Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik* (Indonesia: Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952, Pasal 26 ayat (1), 2016)
- Indonesia, *Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi*, 2022
- INDONESIA, MENTERI KOMUNIKASI DAN DIGITAL REPUBLIK, *PERATURAN MENTERI KOMUNIKASI DAN DIGITAL REPUBLIK INDONESIA* (Indonesia, 2025), p. 2
- Khatimah, Husnul, 'PERLINDUNGAN HUKUM TERHADAP KONSUMEN DALAM TRANSAKSI JUAL BELI ONLINE DI APLIKASI LAZADA DAN SHOPEE', *LEX LATA: Jurnal Ilmu Hukum*, 4 (2023), 384–404
- Lupi, Fadel Retzen, and Nurdin, 'Analisis Strategi Pemasaran Dan Penjualan', *Jurnal Elektronik Sistem Informasi Dan Komputer*, 2 (2016), 20–31
- Maharani, Kuan, and Nur Hidayah, 'ANALISIS FAKTOR YANG MEMENGARUHI PERILAKU IMPULSIVE BUYING PADA PENGGUNAAN E-COMMERCE', *Jurnal Akuntansi*, 5 (2025), 505–19
- Maharani, Rista, and Andria Luhur Prakoso, 'Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital Protection of Consumer Personal Data by Electronic System Providers in Digital Peningkatan Substansial Dalam Penggunaan Platform E-Commerce Di Indonesia Telah', *USM Law Review*, 7 (2024), 333–47
- Mania, Irfan Sophan Himawan, Erlangga, Sri Wahyuni, Dini Hamidin, Astri Dwi Amdriani, and others, *ETIKA PROFESI TEKNOLOGI INFORMASI & KOMUNIKASI* (TOHAR MEDIA, 2022)
- Mei-, Djhpi, Alief Tanding Pamungkas, Andi Mulyono, and Nurjana Lahangatubun, 'The Crisis of Cybercrime Law Enforcement in Indonesia : Obstacles and Solutions', 2024 <<https://doi.org/10.35905/delictum.v2i2.10613>>
- Muhammad, Maldi Omar, and Lucky Dafira Nugroho, 'Perlindungan Hukum Terhadap Pengguna Aplikasi E-Commerce Yang Terdampak Kebocoran Data Pribadi', *Jurnal Pamator : Jurnal Ilmiah Universitas Trunojoyo*, 14 (2021), 165–74
- Nur, Andi Wahyuddin, Besse Muqita Dewi Mentari Rijal, Dewi Wahyuni Mustafa, and Nelvi, 'Tanggung Jawab Pelaksana Sistem Elektronik Dalam Melindungi Informasi Pemakai Media Sosial Menurut Undang-Undang Nomor 19 Tahun 2016 Mengenai Informasi Dan Transaksi Elektronik', *LEGAL: Journal of Law*, 3 (2024), 18–29
- Pertiwi, Wahyunanda, and Oik Yusuf, 'Anggota Forum Hacker Klaim Punya Data 13 Juta Akun Bukalapak Sumber: <https://Tekno.Kompas.Com/Read/2020/05/06/09390047/Anggota-Forum-Hacker-Klaim-Punya-Data-13-Juta-Akun-Bukalapak>. Membership: <https://Kmp.Im/Plus6> Download Aplikasi: <https://Kmp.Im/App6>', *Kompas.Com*
- Pohan, Tia Deja, Muhammad Irwan, Padli Nasution, Universitas Islam, and Negeri Sumatera, 'Perlindungan Hukum Data Pribadi Konsumen Dalam', 1 (2023), 42–48
- Sadewa, Rayhan Wira, Universitas Esa Unggul, Gousta Feriza, and Universitas Esa Unggul, 'Arus Jurnal Sosial Dan Humaniora (AJSH) Analisis Yuridis Kebocoran Data Pelanggan Pada Platform Tokopedia Dan Tanggungjawab Terhadap Perlindungan Hukum Konsumen', 5 (2025)

- Santosa, Lia, 'Kominfo Tangani 94 Kasus Kebocoran Data Pribadi Dalam Tiga Tahun', *ANTARA*, 2023 <<https://www.antaranews.com/berita/3584103/kominfo-tangani-94-kasus-kebocoran-data-pribadi-dalam-tiga-tahun>>
- Soleh, Mohamad, and Zubakhrum Tjenreng, 'STRATEGI PENCEGAHAN KEBOCORAN DATA PELAYANAN PUBLIK', *Jurnal Kajian Pemerintah (JKP)*, 11 (2024), 1–10
- Studi, Tokopedia, and Normatif Dan, 'Kebocoran 91 Juta Data Pribadi Konsumen Aplikasi Tokopedia: Studi Normatif Dan Tanggungjawab', 13 (2025), 1–11
- Tambunan, Lambok, 'Urgensi Rancangan Undang-Undang (Ruu) Perlindungan Data Pribadi', *Jurnal Hukum UNISSULA*, 37 (2024), 119–33
- Technology, Business, 'Keamanan Jaringan Komputer Dalam Bisnis E-Commerce (Studi Kasus : Kebocoran Data Tokopedia 2020)', 1 (2025), 73–77
- Vivere, Journal Honeste, 'PERLINDUNGAN KONSUMEN ATAS RISIKO KEAMANAN INFORMASI DALAM TRANSAKSI E-COMMERCE', 32 (2022), 98–107

