



Department of Digital Business

**Journal of Artificial Intelligence and Digital Business (RIGGS)**

Homepage: <https://journal.ilmudata.co.id/index.php/RIGGS>

Vol. 5 No. 2 (2026) pp: 10747-10755

P-ISSN: 2963-9298, e-ISSN: 2963-914X

---

## Perlindungan Hukum Konsumen dalam Transaksi Elektronik atas Kebocoran Data Pribadi: Studi Kasus Tokopedia 2020 dan Implikasi Undang-Undang Perlindungan Data Pribadi

Natasya Windi Aqilla, Parlaungan Gabriel Siahaan, Desvita Dwi Herawati, Kevin Rahmat Immanuel  
Universitas Negeri Medan

[natasyawnd.3253240012@mhs.unimed.ac.id](mailto:natasyawnd.3253240012@mhs.unimed.ac.id), [parlaungansiahaan@unimed.ac.id](mailto:parlaungansiahaan@unimed.ac.id), [desvita.3252540002@mhs.unimed.ac.id](mailto:desvita.3252540002@mhs.unimed.ac.id),  
[kevin.3253240002@mhs.unimed.ac.id](mailto:kevin.3253240002@mhs.unimed.ac.id)

### Abstrak

Pertumbuhan pesat perdagangan digital di Indonesia telah memberikan kemudahan bagi masyarakat dalam melakukan transaksi elektronik. Namun, perkembangan tersebut juga meningkatkan risiko pelanggaran keamanan data pribadi konsumen. Salah satu kasus yang menjadi perhatian publik adalah kebocoran data yang dialami Tokopedia pada tahun 2020, yang mengakibatkan sekitar 91 juta data pengguna diduga tersebar dan diperjualbelikan di internet. Peristiwa ini menimbulkan kekhawatiran mengenai keamanan informasi pribadi serta efektivitas perlindungan hukum bagi konsumen dalam ekosistem digital. Penelitian ini bertujuan untuk menganalisis mekanisme perlindungan hukum terhadap konsumen yang menjadi korban kebocoran data dalam transaksi elektronik dengan menjadikan kasus Tokopedia sebagai studi kasus utama. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan kasus. Analisis dilakukan berdasarkan ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE), Undang-Undang Perlindungan Konsumen (UUPK), serta Undang-Undang Perlindungan Data Pribadi (UU PDP) Nomor 27 Tahun 2022. Hasil penelitian menunjukkan bahwa kebocoran data Tokopedia mencerminkan adanya pelanggaran terhadap kewajiban penyelenggara sistem elektronik dalam menjaga keamanan data pengguna dan memberikan pemberitahuan yang memadai kepada pihak yang terdampak. Kehadiran UU PDP menjadi langkah penting dalam memperkuat perlindungan data pribadi melalui pengaturan hak subjek data, kewajiban pengendali data, serta sanksi administratif dan pidana bagi pelanggar. Dengan demikian, konsumen memiliki landasan hukum yang lebih kuat untuk memperoleh perlindungan atas data pribadinya. Penelitian ini merekomendasikan penegakan UU PDP secara konsisten, pelaksanaan audit keamanan secara berkala oleh platform digital, serta peningkatan literasi digital masyarakat guna meminimalkan risiko penyalahgunaan data pribadi di masa mendatang.

Kata kunci: Kebocoran Data, E-Commerce, Perlindungan Konsumen, UU ITE, Perlindungan Data Pribadi, Tokopedia

### 1. Latar Belakang

Perkembangan teknologi informasi dan komunikasi yang pesat telah mentransformasi lanskap perekonomian Indonesia secara fundamental. Electronic commerce (e-commerce) tumbuh menjadi ekosistem digital yang melibatkan puluhan juta transaksi setiap harinya, dengan nilai pasar yang terus meningkat secara eksponensial. Berdasarkan data Asosiasi E-Commerce Indonesia (idEA), nilai transaksi e-commerce nasional mencapai angka ratusan triliun rupiah per tahun, dengan tren pertumbuhan yang konsisten melampaui rata-rata global.

Namun, di balik kemudahan dan efisiensi yang ditawarkan, ekosistem e-commerce menyimpan risiko serius berupa ancaman terhadap keamanan data pribadi konsumen. Setiap kali seorang pengguna mendaftarkan diri dan melakukan transaksi pada platform e-commerce, ia mempercayakan berbagai informasi yang bersifat sensitif—mulai dari nama lengkap, alamat, nomor telepon, data finansial, hingga riwayat transaksi—kepada penyelenggara platform. Data-data ini bukan sekadar aset digital, melainkan merupakan representasi identitas digital seseorang yang apabila disalahgunakan dapat menimbulkan kerugian nyata, mulai dari penipuan finansial hingga pencurian identitas.

Pada bulan Mei 2020, Indonesia dikejutkan oleh insiden kebocoran data besar-besaran yang menimpa Tokopedia, salah satu unicorn teknologi dan marketplace terbesar di tanah air. Seorang peretas dengan nama pengguna

ShinyHunters mengklaim telah berhasil membobol sistem keamanan Tokopedia dan mencuri data sebanyak 91 juta akun pengguna dan 7 juta data merchant. Data tersebut kemudian diperjualbelikan di forum dark web dengan harga yang sangat murah, mengancam privasi dan keamanan jutaan warga negara Indonesia secara serentak.

Insiden ini bukan sekadar persoalan teknis keamanan siber semata. Lebih dari itu, peristiwa Tokopedia 2020 mengungkap celah krusial dalam sistem hukum perlindungan data Indonesia: tidak adanya regulasi komprehensif yang secara khusus mengatur perlindungan data pribadi, ketidakjelasan mekanisme pertanggungjawaban penyelenggara platform, serta ketiadaan kewajiban notifikasi yang tegas kepada pihak yang terdampak. Hal ini menimbulkan pertanyaan fundamental: sejauh mana hukum Indonesia mampu melindungi konsumen digital dari risiko kebocoran data?

Kebaruan (novelty) penelitian ini terletak pada tiga aspek. Pertama, penelitian ini menganalisis kasus Tokopedia 2020 secara komprehensif dengan mengintegrasikan seluruh kerangka hukum yang berlaku secara bersamaan, baik UU ITE, PP PSTE, maupun UUPK. Kedua, penelitian ini mengkaji secara khusus implikasi lahirnya UU PDP No. 27 Tahun 2022 sebagai respons legislatif atas kelemahan hukum yang terekspos oleh kasus Tokopedia. Ketiga, penelitian ini memetakan pergeseran paradigma perlindungan data di Indonesia dari pendekatan reaktif menuju pendekatan proaktif dan berbasis akuntabilitas.

Perlindungan data pribadi dalam transaksi elektronik pada dasarnya merupakan bagian dari perlindungan hak asasi manusia. Hak atas privasi telah diakui secara universal sebagai salah satu hak fundamental yang harus dijamin oleh negara. Dalam konteks digital, perlindungan terhadap data pribadi menjadi semakin penting karena hampir seluruh aktivitas masyarakat modern bergantung pada pengumpulan, penyimpanan, dan pengolahan data oleh berbagai platform digital. Data pribadi tidak lagi sekadar informasi identitas, tetapi telah berkembang menjadi komoditas yang memiliki nilai ekonomi tinggi. Oleh karena itu, kebocoran data tidak hanya menimbulkan kerugian individual, tetapi juga dapat mengganggu kepercayaan publik terhadap sistem ekonomi digital secara keseluruhan.

Dalam praktik perdagangan elektronik, hubungan hukum antara konsumen dan penyelenggara platform tidak hanya terbatas pada transaksi jual beli barang dan jasa. Ketika konsumen memberikan data pribadinya kepada platform digital, pada saat yang sama terbentuk hubungan hukum yang mengandung kewajiban bagi penyelenggara sistem elektronik untuk menjaga kerahasiaan, keamanan, dan integritas data tersebut. Kewajiban tersebut lahir karena adanya prinsip kepercayaan (trust) yang menjadi fondasi utama dalam penyelenggaraan transaksi elektronik. Tanpa adanya jaminan keamanan data, konsumen akan kehilangan kepercayaan untuk melakukan aktivitas ekonomi melalui media digital.

Kasus kebocoran data Tokopedia tahun 2020 menunjukkan bahwa keamanan data merupakan aspek yang tidak dapat dipisahkan dari perlindungan konsumen. Dalam kasus tersebut, jutaan pengguna berpotensi menghadapi berbagai risiko lanjutan seperti pencurian identitas, penipuan berbasis rekayasa sosial (social engineering), phishing, spam, hingga penyalahgunaan informasi pribadi untuk kepentingan pihak yang tidak bertanggung jawab. Ancaman tersebut dapat berlangsung dalam jangka waktu yang panjang karena data yang telah tersebar di internet sangat sulit untuk dihapus secara permanen. Dengan demikian, dampak kebocoran data tidak hanya bersifat sesaat, tetapi dapat terus membahayakan korban selama bertahun-tahun.

Sebelum lahirnya Undang-Undang Perlindungan Data Pribadi Nomor 27 Tahun 2022, pengaturan mengenai data pribadi di Indonesia masih tersebar dalam berbagai peraturan perundang-undangan yang berbeda. UU ITE dan peraturan turunannya memang mengatur kewajiban penyelenggara sistem elektronik untuk menjaga keamanan informasi, namun pengaturannya masih bersifat umum dan belum memberikan mekanisme perlindungan yang komprehensif bagi subjek data. Akibatnya, ketika terjadi kebocoran data, konsumen sering mengalami kesulitan dalam menuntut pertanggungjawaban hukum dari penyelenggara platform karena belum adanya aturan yang secara tegas mengatur hak-hak korban dan kewajiban pengendali data.

Kondisi tersebut berbeda dengan berbagai negara yang telah lebih dahulu memiliki regulasi perlindungan data yang komprehensif. Di kawasan Eropa, misalnya, General Data Protection Regulation (GDPR) menjadi standar internasional dalam perlindungan data pribadi. Regulasi tersebut memberikan hak yang luas kepada subjek data, termasuk hak untuk memperoleh informasi, hak untuk mengakses data, hak untuk memperbaiki data, hak untuk menghapus data, serta hak untuk memperoleh ganti rugi apabila terjadi pelanggaran. Kehadiran GDPR telah mendorong perusahaan teknologi untuk menerapkan standar keamanan yang lebih tinggi dan meningkatkan akuntabilitas dalam pengelolaan data pribadi pengguna.

Lahirnya Undang-Undang Perlindungan Data Pribadi di Indonesia merupakan langkah penting dalam memperkuat perlindungan hukum terhadap konsumen digital. Undang-undang ini memberikan dasar hukum yang lebih jelas mengenai prinsip-prinsip pemrosesan data pribadi, hak-hak subjek data, kewajiban pengendali data pribadi, serta mekanisme penegakan hukum terhadap pelanggaran yang terjadi. Dengan adanya UU PDP, perlindungan data pribadi tidak lagi dipandang sebagai kewajiban moral atau etika bisnis semata, melainkan menjadi kewajiban hukum yang harus dipatuhi oleh seluruh pihak yang mengelola data pribadi.

Selain memperkuat perlindungan terhadap konsumen, UU PDP juga mendorong terciptanya tata kelola data yang lebih baik dalam penyelenggaraan sistem elektronik. Setiap penyelenggara platform digital dituntut untuk menerapkan prinsip kehati-hatian dalam mengumpulkan, menyimpan, menggunakan, dan memproses data pribadi pengguna. Kewajiban tersebut mencakup penerapan sistem keamanan yang memadai, pembatasan akses terhadap data, pengelolaan risiko keamanan siber, serta pemberitahuan kepada pemilik data apabila terjadi kegagalan perlindungan data pribadi. Dengan demikian, regulasi ini mendorong lahirnya budaya kepatuhan dan akuntabilitas dalam industri digital.

Dari perspektif hukum perlindungan konsumen, kebocoran data pribadi dapat dikategorikan sebagai bentuk kerugian yang dialami konsumen akibat kegagalan pelaku usaha dalam memenuhi kewajibannya. Konsumen memiliki hak untuk memperoleh kenyamanan, keamanan, dan keselamatan dalam menggunakan barang dan jasa yang ditawarkan oleh pelaku usaha. Oleh karena itu, ketika penyelenggara platform gagal melindungi data pribadi pengguna, maka terdapat dasar hukum bagi konsumen untuk menuntut pertanggungjawaban atas kerugian yang timbul. Hal ini menunjukkan bahwa perlindungan data pribadi dan perlindungan konsumen memiliki hubungan yang sangat erat dalam konteks transaksi elektronik.

Perkembangan teknologi digital yang semakin kompleks juga menghadirkan tantangan baru dalam penegakan hukum perlindungan data pribadi. Ancaman keamanan siber tidak hanya berasal dari peretas individu, tetapi juga dari kelompok kriminal terorganisasi yang memiliki kemampuan teknis tinggi. Selain itu, sifat internet yang lintas batas negara menyebabkan penanganan kasus kebocoran data sering kali melibatkan yurisdiksi yang berbeda. Oleh karena itu, perlindungan data pribadi memerlukan kerja sama yang kuat antara pemerintah, aparat penegak hukum, penyelenggara sistem elektronik, serta komunitas internasional untuk menciptakan ekosistem digital yang aman dan terpercaya.

Di samping aspek regulasi, peningkatan kesadaran masyarakat mengenai pentingnya perlindungan data pribadi juga menjadi faktor yang tidak kalah penting. Banyak pengguna internet yang masih kurang memahami risiko penyalahgunaan data pribadi dan cenderung memberikan informasi pribadinya tanpa mempertimbangkan aspek keamanan. Kondisi ini menunjukkan bahwa perlindungan data tidak hanya bergantung pada regulasi dan teknologi, tetapi juga memerlukan peningkatan literasi digital masyarakat agar mampu berpartisipasi secara aktif dalam menjaga keamanan data mereka sendiri.

Berdasarkan uraian tersebut, dapat dipahami bahwa kasus kebocoran data Tokopedia tahun 2020 menjadi momentum penting dalam perkembangan hukum perlindungan data pribadi di Indonesia. Kasus ini tidak hanya mengungkap kelemahan sistem keamanan digital, tetapi juga memperlihatkan kebutuhan mendesak akan regulasi yang lebih kuat dan mekanisme perlindungan yang lebih efektif bagi konsumen. Kehadiran UU PDP menjadi langkah maju dalam memperkuat perlindungan hukum terhadap data pribadi, namun efektivitasnya akan sangat bergantung pada konsistensi penegakan hukum, kepatuhan penyelenggara sistem elektronik, serta kesadaran masyarakat dalam menjaga keamanan informasi pribadinya. Oleh karena itu, perlindungan data pribadi harus ditempatkan sebagai salah satu prioritas utama dalam pembangunan ekosistem ekonomi digital yang aman, berkelanjutan, dan berorientasi pada perlindungan hak-hak konsumen.

Penelitian ini bertujuan untuk: (1) menganalisis pengaturan hukum positif Indonesia terhadap keamanan data dalam transaksi elektronik sebelum dan sesudah lahirnya UU PDP; (2) mengkaji pertanggungjawaban hukum Tokopedia atas insiden kebocoran data tahun 2020; serta (3) merumuskan implikasi UU PDP terhadap penyelenggaraan e-commerce dan perlindungan konsumen digital di Indonesia.

## 2. Metode Penelitian

Penelitian ini merupakan penelitian hukum normatif (normative legal research), yaitu penelitian yang dilakukan dengan menganalisis bahan-bahan hukum yang relevan sebagai sumber data primer. Penelitian hukum normatif dipilih karena penelitian ini berfokus pada analisis norma, prinsip, dan asas hukum yang berlaku dalam konteks perlindungan data pribadi dan transaksi elektronik di Indonesia (Marzuki, 2017).

Pendekatan penelitian yang digunakan meliputi dua pendekatan secara simultan. Pertama, pendekatan perundang-undangan (statute approach) yang dilakukan dengan menelaah seluruh peraturan perundang-undangan yang relevan, mencakup Undang-Undang Nomor 11 Tahun 2008 jo. UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Kedua, pendekatan kasus (case approach) yang dilakukan dengan menelaah kronologi, fakta hukum, dan respons berbagai pihak terhadap insiden kebocoran data Tokopedia tahun 2020.

Bahan hukum yang digunakan terdiri atas tiga kategori. Bahan hukum primer berupa peraturan perundang-undangan yang mengikat secara yuridis. Bahan hukum sekunder berupa literatur ilmiah, artikel jurnal hukum terakreditasi, laporan lembaga resmi, dan doktrin hukum yang relevan dengan topik penelitian. Bahan hukum tersier berupa kamus hukum, ensiklopedia, dan sumber referensi pendukung lainnya. Analisis dilakukan secara kualitatif-deskriptif dengan menggunakan logika deduktif, yaitu menarik kesimpulan dari premis umum (norma hukum yang berlaku) ke premis khusus (kasus Tokopedia 2020).

## 3. Hasil dan Diskusi

### Kajian Teoritis: Transaksi Elektronik, Perlindungan Data, dan Tanggung Jawab Penyelenggara

Transaksi elektronik didefinisikan dalam Pasal 1 angka 2 UU ITE sebagai perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya. Sebagai bentuk modernisasi transaksi, e-commerce menghadirkan tantangan unik dalam hukum perlindungan konsumen karena menghilangkan batas geografis, mengurangi interaksi tatap muka, dan menciptakan asimetri informasi yang sangat besar antara pelaku usaha platform dengan konsumen (Makarim, 2019).

Konsep perlindungan data pribadi dalam transaksi elektronik bertumpu pada beberapa prinsip universal yang diadopsi dari General Data Protection Regulation (GDPR) Uni Eropa dan instrumen hukum internasional lainnya. Prinsip-prinsip tersebut meliputi: lawfulness, fairness, and transparency (keabsahan, kejujuran, dan transparansi pemrosesan data); purpose limitation (pembatasan tujuan pengumpulan data); data minimization (minimalisasi data yang dikumpulkan); accuracy (keakuratan data); storage limitation (pembatasan penyimpanan); integrity and confidentiality (integritas dan kerahasiaan); serta accountability (akuntabilitas pengendali data) (Voigt & Von dem Bussche, 2017).

Dalam konteks hukum Indonesia, tanggung jawab penyelenggara sistem elektronik dikonstruksikan sebagai tanggung jawab yang bersifat strict liability dalam dimensi tertentu. Pasal 15 UU ITE menegaskan bahwa setiap penyelenggara sistem elektronik wajib menyelenggarakan sistem elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya sistem elektronik sebagaimana mestinya. Kata "wajib" dalam pasal ini mengindikasikan bahwa kewajiban pengamanan sistem bersifat imperatif dan tidak dapat dikesampingkan oleh perjanjian privat antara penyelenggara dengan penggunanya (Sitompul, 2020).

Teori pertanggungjawaban dalam hukum siber Indonesia mengakomodasi setidaknya tiga basis pertanggungjawaban. Pertama, pertanggungjawaban berdasarkan perbuatan melawan hukum (Pasal 1365 KUHPerdata), yang mensyaratkan pembuktian empat unsur: adanya perbuatan, kesalahan, kerugian, dan hubungan kausalitas. Kedua, pertanggungjawaban berdasarkan pelanggaran kontrak elektronik, di mana syarat penggunaan layanan yang tidak dipenuhi dapat menjadi dasar gugatan. Ketiga, pertanggungjawaban berdasarkan ketentuan khusus dalam UU ITE dan peraturan pelaksanaannya yang memberikan kewajiban spesifik kepada penyelenggara sistem elektronik (Ramli, 2018).

### Kronologi dan Fakta Hukum Kasus Kebocoran Data Tokopedia 2020

Tokopedia merupakan perusahaan teknologi Indonesia yang didirikan pada tahun 2009 oleh William Tanuwijaya dan Leontinus Alpha Edison. Sebagai salah satu marketplace terbesar di Asia Tenggara, Tokopedia telah berhasil menghimpun puluhan juta pengguna aktif dan menjadi infrastruktur digital perdagangan Indonesia yang vital. Pada tahun 2020, valuasi Tokopedia diperkirakan mencapai miliaran dolar Amerika Serikat, menjadikannya salah satu perusahaan rintisan paling bernilai di kawasan.

Kronologi insiden dimulai pada sekitar bulan Maret 2020, ketika diduga terjadi pembobolan sistem keamanan Tokopedia oleh pihak tidak bertanggung jawab. Pada bulan Mei 2020, peretas dengan nama ShinyHunters secara publik mengklaim telah mencuri data 91 juta akun pengguna dan 7 juta data merchant Tokopedia. Data yang diklaim berhasil dicuri meliputi nama lengkap, alamat email, tanggal lahir, nomor telepon, jenis kelamin, dan hash kata sandi (password) yang dienkripsi. Data tersebut kemudian ditawarkan untuk dijual di forum dark web Empire Market dengan harga sekitar 5.000 dolar Amerika Serikat.

Merespons insiden tersebut, pihak Tokopedia mengakui adanya upaya pencurian data dan menyatakan bahwa kata sandi pengguna telah diamankan dengan metode enkripsi hashing sehingga tidak dapat digunakan secara langsung. Tokopedia juga menyatakan telah melaporkan insiden kepada pihak berwenang dan mengambil langkah-langkah keamanan tambahan. Namun, yang menjadi sorotan dalam konteks hukum adalah kenyataan bahwa Tokopedia tidak secara proaktif dan individual memberitahukan seluruh pengguna yang terdampak mengenai insiden tersebut, serta tidak secara transparan mengungkapkan skala kerugian aktual yang dialami pengguna.

Dari perspektif hukum, setidaknya terdapat tiga persoalan fundamental yang muncul dari kasus ini: pertama, apakah standar keamanan sistem yang diterapkan Tokopedia telah memenuhi kewajiban hukum yang berlaku; kedua, apakah kewajiban notifikasi kepada pengguna yang terdampak telah dipenuhi secara memadai; dan ketiga, mekanisme hukum apa yang tersedia bagi konsumen untuk memperoleh pemulihan atas kerugian yang dialami.

**Tabel 3.1 Kronologi Insiden Kebocoran Data Tokopedia 2020**

| Waktu      | Peristiwa                                                        | Fakta Hukum                                                     |
|------------|------------------------------------------------------------------|-----------------------------------------------------------------|
| Maret 2020 | Dugaan pembobolan sistem Tokopedia oleh peretas ShinyHunters     | Pelanggaran keamanan sistem elektronik (Pasal 15 UU ITE)        |
| Mei 2020   | Data 91 juta pengguna ditawarkan di forum dark web Empire Market | Penyebaran data pribadi tanpa izin (Pasal 26 UU ITE)            |
| Mei 2020   | Tokopedia mengakui insiden dan menyatakan password terenkripsi   | Kewajiban notifikasi belum dipenuhi secara komprehensif         |
| Mei 2020   | Laporan polisi dan investigasi Kominfo dilakukan                 | Proses hukum berjalan di bawah kerangka UU ITE & PP PSTE        |
| 2022       | DPR RI mengesahkan UU PDP No. 27 Tahun 2022                      | Lahirnya regulasi komprehensif sebagai respons atas celah hukum |

### Analisis Pertanggungjawaban Hukum Tokopedia Berdasarkan Regulasi yang Berlaku

Pertama, ditinjau dari perspektif Undang-Undang ITE. Pasal 26 ayat (1) UU ITE menyatakan bahwa kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan. Norma ini menegaskan bahwa persetujuan (consent) merupakan fondasi yuridis pemrosesan data pribadi, dan bahwa setiap pemanfaatan data di luar persetujuan, termasuk yang disebabkan oleh kelalaian keamanan mengandung dimensi pelanggaran hukum.

Pasal 15 ayat (1) UU ITE lebih lanjut menegaskan bahwa setiap penyelenggara sistem elektronik wajib menyelenggarakan sistem elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya sistem elektronik sebagaimana mestinya. Norma ini mengandung makna yang luas: kewajiban "andal dan aman" bukan sekadar menyediakan sistem yang berfungsi, melainkan juga memastikan bahwa sistem tersebut terlindungi dari ancaman eksternal. Kegagalan Tokopedia dalam mencegah peretasan dapat diargumentasikan sebagai kegagalan memenuhi standar keamanan yang diamanatkan oleh pasal ini (Sitompul, 2020).

Kedua, ditinjau dari Peraturan Pemerintah Nomor 71 Tahun 2019. Pasal 25 PP PSTE mewajibkan penyelenggara sistem elektronik untuk menjamin kerahasiaan data pribadi yang dikelolanya. Pasal 26 PP PSTE mewajibkan penyelenggara untuk mengimplementasikan langkah-langkah teknis yang memadai guna melindungi data dari akses, pengungkapan, pengubahan, atau penghapusan yang tidak sah. Selain itu, Pasal 28 PP PSTE mewajibkan adanya kebijakan privasi yang komprehensif dan transparan yang dikomunikasikan kepada pengguna. Kegagalan Tokopedia dalam mempertahankan keamanan data merupakan indikasi kuat bahwa standar yang diisyaratkan PP PSTE tidak terpenuhi secara optimal.

Ketiga, ditinjau dari Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. UUPK Pasal 4 memberikan hak kepada konsumen untuk mendapatkan informasi yang benar, jelas, dan jujur mengenai kondisi dan jaminan barang dan/atau jasa. Kegagalan Tokopedia untuk secara proaktif dan individual memberitahukan pengguna yang terdampak merupakan pelanggaran terhadap hak konsumen atas informasi. Pasal 7 UUPK mewajibkan pelaku usaha untuk memberikan informasi yang benar, jelas, dan jujur mengenai kondisi dan jaminan layanan, sedangkan Pasal 19 mengatur kewajiban ganti rugi atas kerugian konsumen akibat penggunaan atau pemanfaatan jasa.

**Tabel 3.2 Matriks Pelanggaran Hukum dalam Kasus Tokopedia 2020**

| Regulasi            | Pasal yang Dilanggar | Bentuk Pelanggaran                                           |
|---------------------|----------------------|--------------------------------------------------------------|
| UU ITE No. 19/2016  | Pasal 15 ayat (1)    | Kegagalan menjamin sistem elektronik yang andal dan aman     |
| UU ITE No. 19/2016  | Pasal 26 ayat (1)    | Data pribadi pengguna diekspos tanpa persetujuan             |
| PP PSTE No. 71/2019 | Pasal 25 & 26        | Kegagalan menjaga kerahasiaan dan keamanan data pribadi      |
| PP PSTE No. 71/2019 | Pasal 28             | Kebijakan privasi tidak memadai mencegah insiden kebocoran   |
| UUPK No. 8/1999     | Pasal 4 & 7          | Hak konsumen atas informasi tidak dipenuhi secara proaktif   |
| UUPK No. 8/1999     | Pasal 19             | Kewajiban ganti rugi atas kerugian konsumen tidak dieksekusi |

### **Implikasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi**

Lahirnya UU PDP merupakan respons legislatif yang paling signifikan atas deretan insiden kebocoran data yang menimpa Indonesia, termasuk kasus Tokopedia 2020. Sebelum UU PDP, Indonesia merupakan salah satu dari sedikit negara besar di dunia yang belum memiliki undang-undang perlindungan data pribadi yang komprehensif dan berdiri sendiri. Ketiadaan regulasi khusus ini menyebabkan penanganan kasus kebocoran data harus dilakukan secara parsial berdasarkan berbagai peraturan yang tersebar, sehingga penegakannya menjadi tidak efektif (Hidayati, 2022).

UU PDP memperkenalkan sejumlah ketentuan revolusioner yang mengubah paradigma perlindungan data di Indonesia. Pertama, mengenai kewajiban notifikasi insiden. Pasal 46 UU PDP mewajibkan pengendali data pribadi

untuk memberitahukan secara tertulis kepada pemilik data pribadi dan kepada Lembaga paling lambat 14 hari kerja setelah mengetahui terjadinya kegagalan perlindungan data pribadi yang berdampak signifikan. Kewajiban ini jauh lebih tegas dan terukur dibandingkan pengaturan sebelumnya yang tidak menetapkan batas waktu yang jelas. Dalam konteks kasus Tokopedia, apabila UU PDP telah berlaku, perusahaan berkewajiban memberitahukan seluruh pengguna yang terdampak dalam tenggat waktu 14 hari.

Kedua, mengenai sanksi yang substansial. UU PDP mengatur sanksi administratif berupa denda maksimal 2% dari pendapatan tahunan dalam lingkup Indonesia bagi pelanggaran terhadap ketentuan pemrosesan data pribadi. Bagi pelanggaran yang melibatkan data sensitif, sanksi dapat diperberat. Di samping sanksi administratif, UU PDP juga mengatur sanksi pidana: pidana penjara hingga 6 tahun dan/atau denda hingga Rp 6 miliar bagi yang dengan sengaja memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud menguntungkan diri sendiri atau orang lain. Sanksi yang signifikan ini memberikan efek jera yang jauh lebih kuat dibandingkan rezim hukum sebelumnya.

Ketiga, mengenai prinsip akuntabilitas. UU PDP mengadopsi prinsip akuntabilitas (accountability) di mana pengendali data pribadi tidak hanya wajib mematuhi ketentuan perlindungan data, tetapi juga harus dapat membuktikan kepatuhannya tersebut. Implikasi praktisnya, penyelenggara e-commerce seperti Tokopedia diwajibkan mendokumentasikan seluruh aktivitas pemrosesan data, menunjuk pejabat pelindung data (data protection officer) untuk organisasi yang memproses data dalam skala besar, serta melakukan penilaian dampak perlindungan data (data protection impact assessment) untuk pemrosesan yang berisiko tinggi.

**Tabel 3.3 Perbandingan Rezim Hukum Perlindungan Data Sebelum dan Sesudah UU PDP**

| Aspek                 | Sebelum UU PDP                  | Setelah UU PDP (2022)                |
|-----------------------|---------------------------------|--------------------------------------|
| Regulasi utama        | UU ITE & PP PSTE (tersebar)     | UU PDP No. 27/2022 (komprehensif)    |
| Kewajiban notifikasi  | Tidak diatur dengan jelas       | Wajib dalam 14 hari kerja (Pasal 46) |
| Sanksi administratif  | Terbatas, tidak proporsional    | Denda maks. 2% pendapatan tahunan    |
| Sanksi pidana         | Maksimal 12 tahun (UU ITE)      | Penjara maks. 6 tahun & denda Rp 6 M |
| Prinsip akuntabilitas | Tidak diadopsi secara eksplisit | Diwajibkan, termasuk dokumentasi     |
| Lembaga pengawas      | Belum ada lembaga khusus        | Lembaga Perlindungan Data Pribadi    |
| Hak subjek data       | Tersebar, tidak komprehensif    | Dijamin secara eksplisit (Bab VI)    |

### **Mekanisme Pemulihan Hukum bagi Konsumen yang Terdampak**

Sebelum lahirnya UU PDP, konsumen yang menjadi korban kebocoran data memiliki akses terbatas terhadap mekanisme pemulihan hukum. Pertama, jalur litigasi perdata berdasarkan Pasal 1365 KUHPerdata tentang perbuatan melawan hukum. Namun, jalur ini menghadapi tantangan pembuktian yang berat, mengingat konsumen harus membuktikan secara konkret kerugian yang diderita sebagai akibat langsung dari kebocoran data. Hal ini sulit dilakukan karena kerugian akibat kebocoran data sering kali bersifat laten dan tidak langsung terasa secara finansial.

Kedua, jalur pengaduan melalui Badan Penyelesaian Sengketa Konsumen (BPSK) berdasarkan UUPK. Meskipun BPSK menawarkan proses yang lebih cepat dan murah dibandingkan pengadilan, kapasitas lembaga ini dalam menangani sengketa di bidang teknologi digital masih sangat terbatas. Ketiadaan keahlian teknis yang memadai di kalangan penyelesai sengketa menjadi hambatan signifikan dalam penanganan kasus-kasus data breach (Rachmadhani, 2021).

UU PDP hadir dengan memperkuat posisi konsumen melalui beberapa mekanisme baru. Pasal 67 dan 68 UU PDP memberikan hak kepada pemilik data pribadi untuk mengajukan gugatan ganti rugi kepada pengendali atau prosesor data yang melanggar ketentuan UU PDP. Selain itu, adanya lembaga pengawas independen yang diamanatkan UU PDP diharapkan dapat menjadi garda terdepan perlindungan hak-hak subjek data, termasuk dalam menerima pengaduan, melakukan investigasi, dan menjatuhkan sanksi administratif.

#### Perbandingan dengan Praktik Perlindungan Data di Negara Lain

Untuk memberikan perspektif komparatif, relevan untuk membandingkan regulasi Indonesia dengan General Data Protection Regulation (GDPR) Uni Eropa yang dianggap sebagai standar emas perlindungan data global. GDPR mewajibkan notifikasi insiden kepada otoritas pengawas dalam waktu 72 jam dan kepada individu yang terdampak tanpa penundaan yang tidak wajar, jauh lebih ketat dibandingkan kewajiban 14 hari kerja dalam UU PDP Indonesia. GDPR juga menerapkan sanksi hingga 4% dari omzet global tahunan atau 20 juta euro, mana yang lebih tinggi, nilai sanksi yang jauh melebihi ketentuan UU PDP (Voigt & Von dem Bussche, 2017).

Di tingkat regional Asia Tenggara, Singapura melalui Personal Data Protection Act (PDPA) mewajibkan notifikasi insiden dalam 3 hari, sementara Thailand melalui Personal Data Protection Act B.E. 2562 mengadopsi standar yang sangat mirip dengan GDPR. Perbandingan ini menunjukkan bahwa meskipun UU PDP Indonesia merupakan kemajuan signifikan, masih terdapat ruang untuk pengetatan standar, khususnya dalam hal tenggat waktu notifikasi dan besaran sanksi, guna mencapai paritas dengan praktik terbaik global.

**Tabel 3.4 Perbandingan Regulasi Perlindungan Data Indonesia dengan Standar Internasional**

| Aspek                   | Indonesia (UU PDP)           | Uni Eropa (GDPR)         | Singapura (PDPA)   |
|-------------------------|------------------------------|--------------------------|--------------------|
| Notifikasi insiden      | 14 hari kerja                | 72 jam                   | 3 hari             |
| Sanksi maks.            | 2% pendapatan nasional       | 4% omzet global          | SGD 1 juta         |
| Lembaga pengawas        | Lembaga PDP (belum dibentuk) | Supervisory Authority    | PDPC               |
| Ekstrateritorialitas    | Terbatas                     | Ya, berlaku global       | Ya, berlaku global |
| Data protection officer | Wajib (skala besar)          | Wajib (kondisi tertentu) | Opsional           |

#### 4. Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan, dapat ditarik tiga kesimpulan utama. Pertama, insiden kebocoran data Tokopedia tahun 2020 merupakan peristiwa hukum yang menimbulkan pertanggungjawaban yuridis bagi Tokopedia selaku penyelenggara sistem elektronik berdasarkan UU ITE, PP PSTE, dan UUPK. Kegagalan memenuhi standar keamanan sistem yang andal dan aman sebagaimana diamanatkan Pasal 15 UU ITE, serta tidak terpenuhinya kewajiban notifikasi yang komprehensif kepada pengguna yang terdampak, merupakan dua bentuk kelalaian hukum yang dapat dimintai pertanggungjawaban. Kedua, pengaturan perlindungan data pribadi sebelum lahirnya UU PDP bersifat fragmentatif, tersebar di berbagai instrumen hukum, dan tidak memberikan perlindungan yang memadai bagi konsumen digital Indonesia. Ketiadaan kewajiban notifikasi yang tegas, sanksi yang tidak proporsional, dan absennya lembaga pengawas khusus menciptakan ekosistem hukum yang lemah dalam menghadapi ancaman kebocoran data pada platform e-commerce berskala besar. Ketiga, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi merupakan transformasi paradigmatis yang signifikan dalam hukum perlindungan data di Indonesia. UU PDP menghadirkan kewajiban notifikasi yang terukur, sanksi yang substansial, prinsip akuntabilitas yang mendorong budaya proaktif perlindungan data, serta fondasi bagi pembentukan lembaga pengawas independen. Meskipun

demikian, efektivitas UU PDP sangat bergantung pada konsistensi penegakan hukum dan kecepatan penerbitan peraturan pelaksana yang komprehensif. Berdasarkan temuan tersebut, penelitian ini merekomendasikan tiga hal. Pertama, pemerintah melalui Kementerian Komunikasi dan Digital beserta Lembaga Perlindungan Data Pribadi yang diamanatkan UU PDP perlu segera menyelesaikan proses pembentukan lembaga dan penerbitan peraturan pelaksana agar UU PDP dapat diimplementasikan secara efektif. Kedua, seluruh penyelenggara platform e-commerce diwajibkan melakukan audit keamanan siber secara berkala dan mengimplementasikan standar keamanan internasional seperti ISO/IEC 27001 sebagai baseline minimum. Ketiga, program peningkatan literasi digital dan kesadaran hak perlindungan data bagi masyarakat Indonesia perlu digalakkan secara sistematis, sehingga konsumen dapat secara aktif menggunakan mekanisme hukum yang tersedia untuk melindungi hak-hak digital mereka.

## Referensi

1. Indonesia. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Lembaran Negara RI Tahun 1999 Nomor 42.
2. Indonesia. Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Lembaran Negara RI Tahun 2016 Nomor 251.
3. Indonesia. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Lembaran Negara RI Tahun 2019 Nomor 185.
4. Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Lembaran Negara RI Tahun 2022 Nomor 196.
5. Makarim, E. (2019). Kompilasi hukum telematika (Edisi ke-3). Rajawali Pers.
6. Marzuki, P. M. (2017). Penelitian hukum (Edisi revisi). Kencana Prenada Media Group.
7. Ramli, A. M. (2018). Cyber law dan HAKI dalam sistem hukum Indonesia. Refika Aditama.
8. Sitompul, A. (2020). Hukum internet: Pengenalan mengenai masalah hukum di cyberspace (Edisi ke-2). Citra Aditya Bakti.
9. Voigt, P., & Von dem Bussche, A. (2017). The EU general data protection regulation (GDPR): A practical guide. Springer.
10. Cahyono, A. S. (2021). Perlindungan hukum terhadap data pribadi pengguna platform digital di Indonesia. Jurnal Hukum dan Teknologi Informasi, 3(1), 45–62.
11. Hidayati, N. (2022). Urgensi undang-undang perlindungan data pribadi di Indonesia pasca insiden kebocoran data besar-besaran. Jurnal Hukum Ius Quia Iustum, 29(2), 301–325.
12. Nurhidayah, R., & Farid, M. (2021). Pertanggungjawaban penyelenggara sistem elektronik atas kebocoran data pribadi pengguna. Jurnal Hukum Islam dan Perundang-Undangan, 8(1), 29–48.
13. Rachmadhani, F. (2021). Efektivitas Badan Penyelesaian Sengketa Konsumen dalam penanganan sengketa e-commerce di Indonesia. Jurnal Hukum Bisnis dan Investasi, 13(1), 55–74.
14. Sari, I. P. (2021). Tanggung jawab penyelenggara sistem elektronik atas kebocoran data pribadi konsumen dalam perspektif UU ITE. Jurnal Hukum Bisnis dan Investasi, 12(2), 78–95.
15. Kementerian Komunikasi dan Informatika Republik Indonesia. (2020). Siaran pers: Kominfo tangani laporan insiden keamanan data Tokopedia. Kominfo.
16. Personal Data Protection Commission Singapore. (2022). Guide to data breach management. PDPC. <https://www.pdpc.gov.sg>
17. Under the Breach. (2020). Tokopedia data breach: 91 million user records exposed. <https://underthebreach.com> (diakses 15 November 2024).