Indonesian Journal of Law and Justice Volume: 2, Number 3, 2025, Page: 1-11

Tinjauan Hukum terhadap Perlindungan Data Pribadi di Era Digital: Kasus Kebocoran Data Pengguna Layanan *E-Commerce*

I Wayan Cenik Ardika*

Universitas Warmadewa, Denpasar, Bali, Indonesia

Abstrak: Era digital telah membawa perubahan besar dalam pola konsumsi dan interaksi ekonomi, dengan platform *e-commerce* menjadi salah satu aspek penting dalam transformasi ini. Namun, perkembangan ini juga menghadirkan tantangan signifikan terkait perlindungan data pribadi konsumen. Artikel ini mengkaji isu kebocoran data pribadi dalam ekosistem *e-commerce* di Indonesia, dengan fokus pada kasus kebocoran data pengguna Tokopedia pada tahun 2020. Studi ini menggunakan pendekatan yuridis normatif untuk menganalisis regulasi yang berlaku, termasuk Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), serta peraturan lainnya yang relevan. Hasil penelitian menunjukkan bahwa meskipun UU PDP memberikan dasar hukum yang lebih jelas untuk perlindungan data pribadi, tantangan tetap ada dalam implementasinya. Kasus Tokopedia menjadi contoh nyata kelemahan dalam sistem keamanan data dan akuntabilitas perusahaan. Selain itu, analisis ini mengungkapkan adanya celah dalam regulasi yang memungkinkan pelanggaran privasi tetap terjadi, serta kurangnya kesadaran konsumen terkait hak-hak mereka. Studi ini merekomendasikan penguatan regulasi, peningkatan kapasitas institusi, literasi digital, dan adopsi praktik terbaik internasional seperti *General Data Protection Regulation* (GDPR) Uni Eropa untuk menciptakan ekosistem digital yang lebih aman dan terpercaya.

Kata kunci: *E-commerce*, Perlindungan Data Pribadi, Kebocoran Data, Tokopedia, Regulasi, Era Digital

DOI: https://doi.org/10.47134/ijlj.v2i3.3601
*Correspondence: I Wayan Cenik Ardika
Email: cenikardika04@gmail.com

Received: 18-01-2025
Accepted: 25-01-2025
Published: 01-03-2025

Abstract: *The digital era has brought about major changes in consumption patterns and economic interactions, with e-commerce platforms being one of the important aspects in this transformation. However, this development also presents significant challenges related to the protection of consumers' personal data. This article examines the issue of personal data leakage in the e-commerce ecosystem in Indonesia, focusing on the case of the Tokopedia user data leak in 2020. This study uses a normative legal approach to analyze applicable regulations, including Law Number 27 of 2022 concerning Personal Data Protection (UU PDP), as well as other relevant regulations. The results of the study show that although the PDP Law provides a clearer legal basis for personal data protection, challenges remain in its implementation. The Tokopedia case is a clear example of weaknesses in the data security system and corporate accountability. In addition, this analysis reveals gaps in regulations that allow privacy violations to continue to occur, as well as a lack of consumer awareness of their rights. This study recommends strengthening regulations, increasing institutional capacity, digital literacy, and adopting international best practices such as the European Union's General Data Protection Regulation (GDPR) to create a safer and more trustworthy digital ecosystem.*

Keywords: *E-commerce, Personal Data Protection, Data Leaks, Tokopedia, Regulation, Digital Era*

Pendahuluan

Era digital telah membawa perubahan signifikan dalam preferensi dan perilaku belanja, yang memicu peralihan besar-besaran ke platform *e-commerce*. Keunggulan seperti kemudahan akses, ketersediaan produk yang beragam, dan harga yang kompetitif menjadi daya tarik utama platform ini. Era digital telah membawa perubahan mendalam dalam berbagai aspek kehidupan manusia, terutama dalam pola konsumsi dan interaksi ekonomi melalui platform *e-commerce*. Kemajuan pesat dalam teknologi informasi dan komunikasi telah memberikan berbagai kemudahan bagi masyarakat, terutama dalam mengakses produk dan layanan secara daring. Transformasi digital ini memungkinkan transaksi menjadi lebih cepat, efisien, dan mudah dilakukan kapan saja dan di mana saja. Namun, di balik manfaat yang ditawarkan, terdapat tantangan yang tidak kalah pentingnya untuk diperhatikan. Beberapa tantangan utama mencakup perlindungan hak konsumen, privasi, keamanan data, standar kualitas produk, dan mekanisme penyelesaian sengketa. Perlindungan hak konsumen menjadi sangat krusial mengingat banyaknya kasus penipuan atau ketidaksesuaian produk dengan deskripsi yang ditawarkan. Selain itu, keamanan data dan privasi juga menjadi isu sentral, karena semakin banyak data pribadi yang disimpan dan diproses oleh platform digital. Jika tidak dikelola dengan baik, data ini berpotensi disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab (Prayuti, 2024).

Salah satu ancaman terbesar yang muncul dalam ekosistem digital adalah kebocoran data pribadi. Data pribadi kini dianggap sebagai salah satu aset paling berharga, baik bagi individu maupun bagi perusahaan, karena memiliki nilai ekonomis yang tinggi. Namun, nilai tersebut menjadikannya target empuk bagi pelaku kejahatan siber. Kebocoran data yang semakin sering terjadi tidak hanya membahayakan privasi individu, tetapi juga menimbulkan dampak buruk yang luas, termasuk kerugian finansial, kerusakan reputasi, dan tekanan psikologis bagi para korban. Selain itu, pelanggaran keamanan data juga dapat mengancam kepercayaan masyarakat terhadap layanan digital, yang pada akhirnya dapat menghambat perkembangan ekonomi digital secara keseluruhan. Oleh karena itu, diperlukan upaya bersama antara pemerintah, penyedia layanan digital, dan masyarakat untuk meningkatkan kesadaran akan pentingnya keamanan data dan menerapkan langkah-langkah perlindungan yang efektif.

Pencurian data pribadi telah menjadi bentuk kejahatan yang berkembang seiring dengan kemajuan teknologi digital, di mana berbagai aktivitas kini dapat dilakukan melalui media digital. Meskipun perlindungan data memiliki banyak manfaat dan keuntungan, kebutuhan akan perangkat lunak pelindung data yang lebih ketat dan akurat menjadi semakin penting. Hal ini disebabkan oleh dampak negatif yang ditimbulkan oleh perkembangan *e-commerce*, yang dirasakan merugikan banyak masyarakat. Beberapa dampak tersebut mencakup tindakan kecurangan yang menyebabkan kerugian finansial

langsung, peretasan rekening bank, pencurian data pribadi, serta penggunaan akses oleh pihak yang tidak dikenal, sehingga menimbulkan keresahan di kalangan masyarakat (Nuranisa & Lukitasari, 2024). Dalam konteks hukum pidana, tindak pidana pencurian data pribadi dapat ditemukan dalam Pasal 482 dan Pasal 483 KUHP baru. Namun, aturan ini belum secara spesifik mengatur pencurian data pribadi secara online, sehingga perlindungan terhadap data pribadi konsumen *e-commerce* masih belum memadai. Peningkatan risiko tindak pidana pencurian data dan pelanggaran privasi pengguna *e-commerce* mencerminkan pergeseran fokus kejahatan ke ranah digital. Fenomena ini menjadi semakin kompleks dan meresahkan karena semakin banyaknya informasi sensitif yang disimpan dan dipertukarkan dalam ekosistem transaksi online.

Sebagai platform *e-commerce* terkemuka di Indonesia, Tokopedia menjadi fokus penelitian dalam memahami kasus kebocoran data pribadi dari perspektif hukum pidana. Penelitian ini penting untuk memahami dampak kejahatan siber terhadap perlindungan data pribadi dan privasi pengguna *e-commerce*, serta untuk mengidentifikasi kelemahan dalam implementasi regulasi yang ada. Kasus kebocoran data yang terjadi pada platform Tokopedia pada tahun 2020 yang mengompromikan sekitar 91 juta akun pengguna menjadi salah satu contoh nyata risiko yang dihadapi oleh konsumen dalam ekosistem *e-commerce* (Mahfudin, 2024). Insiden ini mengungkapkan lemahnya sistem keamanan yang diterapkan oleh perusahaan, serta kurangnya akuntabilitas dalam pengelolaan data pribadi. Pelanggaran seperti ini menunjukkan pentingnya perlindungan hukum yang kuat untuk mencegah insiden serupa di masa depan. Dalam konteks hukum, insiden kebocoran data semacam ini mengarah pada pertanyaan mendasar tentang tanggung jawab perusahaan, mekanisme ganti rugi bagi konsumen, serta efektivitas regulasi yang ada. Secara global, upaya untuk meningkatkan perlindungan data pribadi telah dilakukan melalui berbagai kerangka kerja hukum. *General Data Protection Regulation* (GDPR) di Uni Eropa menjadi contoh standar global yang mengatur tata kelola data pribadi dengan ketat, termasuk hak konsumen untuk mengakses, memperbaiki, dan menghapus data mereka (Chisomo Tolani & Prof. Jyoti Pareek, 2024). Di Indonesia, pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi mencerminkan kesadaran pemerintah akan urgensi perlindungan data dalam menghadapi ancaman dunia digital. Undang-undang ini menjadi langkah penting dalam menciptakan kerangka hukum yang komprehensif. Namun, implementasi dan pengawasan terhadap undang-undang tersebut masih menghadapi berbagai tantangan, termasuk keterbatasan kapasitas institusi dan kesenjangan antara regulasi dan perkembangan teknologi (Nuranisa & Lukitasari, 2024).

Hak konsumen dalam konteks perlindungan data pribadi menjadi salah satu isu penting yang harus mendapatkan perhatian serius. Konsumen memiliki hak fundamental untuk mengetahui bagaimana data mereka digunakan, serta untuk meminta perbaikan atau

penghapusan data yang dianggap tidak relevan atau digunakan secara tidak sah (Chisomo Tolani & Prof. Jyoti Pareek, 2024). Dalam kasus kebocoran data, konsumen sering kali menghadapi situasi sulit untuk menuntut keadilan, baik karena keterbatasan akses terhadap mekanisme hukum maupun karena perusahaan yang bersangkutan tidak secara proaktif memberikan solusi yang memadai. Oleh karena itu, keberadaan kerangka hukum yang memberikan jalur yang jelas bagi konsumen untuk mendapatkan ganti rugi dan memastikan akuntabilitas perusahaan menjadi kebutuhan mendesak. Di sisi lain, laju perkembangan teknologi sering kali melampaui kemampuan regulasi untuk beradaptasi. Hal ini menciptakan celah hukum yang dapat dimanfaatkan oleh pihak-pihak tidak bertanggung jawab, termasuk perusahaan yang tidak menerapkan standar keamanan yang memadai. Oleh karena itu, perlu adanya pendekatan yang holistik dalam mengatasi tantangan ini, termasuk penguatan regulasi, pengawasan yang lebih ketat, dan peningkatan literasi digital di kalangan konsumen.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis secara mendalam tantangan hukum terkait perlindungan data pribadi di era digital, khususnya dalam konteks *e-commerce*. Penelitian ini akan meninjau tanggung jawab perusahaan, efektivitas regulasi yang berlaku, serta hak konsumen dalam menghadapi kasus-kasus kebocoran data. Selain itu, kajian ini juga akan menawarkan rekomendasi kebijakan yang relevan guna memperkuat perlindungan data pribadi di Indonesia, dengan harapan dapat mewujudkan ekosistem digital yang lebih aman dan terpercaya bagi seluruh pihak.

Metode

Penelitian ini menggunakan pendekatan yuridis normatif untuk menganalisis kerangka hukum yang mengatur perlindungan data pribadi di Indonesia. Metode ini berfokus pada kajian terhadap sumber-sumber data sekunder, seperti undang-undang, peraturan pemerintah, serta literatur terkait yang relevan. Penelitian ini juga memanfaatkan analisis dokumen hukum, termasuk Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, sebagai dasar untuk menilai efektivitas regulasi saat ini dalam melindungi data pribadi konsumen (Tiffani & Faisal, 2024). Sebagai bagian dari pendekatan yuridis normatif, studi ini juga mencakup analisis kasus kebocoran data yang terjadi pada platform Tokopedia pada tahun 2020.

Studi kasus ini digunakan untuk menggambarkan implikasi praktis dari pelanggaran data pribadi, termasuk dampak yang dirasakan oleh konsumen serta tanggapan hukum yang tersedia. Analisis ini bertujuan untuk mengevaluasi sejauh mana kerangka hukum yang ada mampu memberikan perlindungan efektif bagi konsumen, serta mengidentifikasi kelemahan yang perlu diperbaiki. Data yang dikumpulkan dalam penelitian ini meliputi

teks-teks hukum, artikel jurnal, laporan, dan studi sebelumnya yang membahas isu-isu terkait perlindungan data pribadi. Penelitian ini juga mengacu pada standar internasional, seperti *General Data Protection Regulation* (GDPR), untuk memberikan perbandingan dan wawasan tambahan terkait praktik terbaik dalam perlindungan data pribadi.

Hasil dan Pembahasan

A. Praktik *E-Commerce* dan Tantangan Perlindungan Konsumen di Indonesia

Perkembangan *e-commerce* di Indonesia berlangsung dengan cepat, didorong oleh peningkatan jumlah pengguna internet dan semakin luasnya adopsi teknologi. Transformasi dalam praktik *e-commerce* meliputi meningkatnya penggunaan perangkat seluler, beragamnya jenis layanan yang ditawarkan, penerapan strategi pemasaran yang disesuaikan dengan kebutuhan lokal, serta kemajuan infrastruktur logistik (Rohmana, 2023). Perkembangan ini mencerminkan adaptasi *e-commerce* terhadap kebutuhan pasar yang terus berubah, dengan peningkatan pengalaman konsumen dan inklusi digital di seluruh negara (Hartatik et al., 2023). Perkembangan *e-commerce* di Indonesia mempengaruhi hak dan kesejahteraan konsumen melalui peningkatan kesadaran hukum, regulasi perlindungan konsumen, dan fokus pada kualitas layanan serta produk. Privasi data dan keamanan menjadi sorotan utama, dengan perlindungan dari kejahatan siber yang semakin diperkuat (Bagaskara et al., 2023).

Di Indonesia, Undang-Undang Perlindungan Konsumen (UU No. 8 Tahun 1999) dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) (UU No. 19 Tahun 2016) merupakan dua kerangka hukum utama yang memiliki peran signifikan dalam melindungi konsumen dan mengatur transaksi elektronik, terutama menghadapi tantangan baru dalam era digital yang melibatkan isu privasi dan keamanan data. Undang-Undang Perlindungan Konsumen menegaskan hak konsumen untuk mendapatkan informasi yang jujur dan benar tentang barang/jasa, termasuk dalam transaksi digital, serta memberikan hak privasi dalam pengumpulan, penggunaan, dan pengolahan informasi pribadi oleh penyedia barang/jasa. Selain itu, mengakui transaksi elektronik, UU Perlindungan Konsumen mengatur hak-hak konsumen dalam konteks ini, termasuk memberikan informasi yang jelas dan komprehensif tentang transaksi elektronik, termasuk kebijakan privasi yang diterapkan oleh penyedia layanan (Devi & Simarsoit, 2020).

Sementara itu, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) menetapkan aturan terkait perlindungan data pribadi, mencakup pengumpulan, pengolahan, dan penggunaan data pribadi konsumen oleh penyedia layanan elektronik. UU ITE menekankan pentingnya agar penyedia layanan melindungi data pribadi konsumen dan menjaga kerahasiaan informasi tersebut. Selain itu, UU ITE memberikan sanksi hukum bagi pelanggaran privasi, termasuk tindakan yang melibatkan

penyalahgunaan data pribadi atau serangan terhadap keamanan data. Kedua undang-undang ini berupaya secara bersama-sama untuk meningkatkan literasi dan kesadaran konsumen mengenai hak dan kewajiban mereka dalam era digital, dengan penekanan pada ketentuan privasi yang jelas dan komprehensif.

Undang-Undang Perlindungan Konsumen (UU No. 8 Tahun 1999) di Indonesia berperan sentral dalam melindungi konsumen dan mengatasi tantangan baru dalam era digital, termasuk dalam konteks manipulasi pasar. Dalam aspek Hak Privasi dan Informasi, UU ini mengonfirmasi hak konsumen untuk memperoleh informasi yang jujur dan benar mengenai barang/jasa, termasuk dalam transaksi digital, serta mengakui hak privasi konsumen dalam pengumpulan, penggunaan, dan pengolahan informasi pribadi oleh penyedia barang/jasa. Perlindungan Konsumen dalam Transaksi Elektronik diwujudkan melalui pengakuan terhadap transaksi elektronik dan regulasi hak-hak konsumen, termasuk hak untuk mendapatkan informasi yang jelas dan komprehensif mengenai transaksi elektronik, termasuk kebijakan privasi penyedia layanan.

B. Kasus Kebocoran Data pada Aplikasi Tokopedia

PT. Tokopedia merupakan badan hukum berbentuk Perseroan Terbatas yang didirikan dan tunduk berdasarkan hukum Negara Indonesia dengan bergerak di bidang *e-commerce*. Untuk selanjutnya, PT Tokopedia disebut sebagai Tokopedia, Whysodank merupakan pihak ketiga yang tidak berwenang dan bertindak sebagai *hacker* serta tidak memiliki hubungan apapun dengan Tokopedia. Pada tanggal 20 Maret 2020, Whsyodank berhasil melakukan peretasan berupa pencurian data pribadi Pengguna Tokopedia. Pada tanggal 23 April 2020, Whysodank bergabung dalam komunitas hacker Raid Forums untuk menawarkan sekaligus menjual data pribadi Pengguna Tokopedia Bahwa pada tanggal 1 Mei 2020, Whysodank membagikan sebagian data pribadi Pengguna Tokopedia yang diperoleh saat peretasan bulan Maret 2020 sebanyak 15 juta data.

Pembagian sebagian data ini bertujuan untuk meminta bantuan *hacker* lain agar bisa membuka kunci algoritma enkripsi *password* akun Pengguna Tokopedia karena masih terkunci. Selanjutnya Whysodank berganti nama menjadi ShinnyHunters pada tanggal 2 Mei 2020 dan menjual sebanyak 91 juta data Pengguna Tokopedia yang berupa user ID, email, nama lengkap, tanggal lahir, jenis kelamin, nomor *handphone*, dan *password* yang masih terkunci di web Empire Market seharga US$5.000 atau sekitar Rp. 74.000.000.00. Pihak Tokopedia melalui Nuraini Razak, VP of Corporate Communications, pada tanggal 3 Mei 2020 telah mengakui adanya pencurian terhadap data pribadi Penggunanya. Kemudian selanjutnya, Tokopedia memastikan bahwa data seperti *password* masih tetap aman dan berhasil dilindungi hari yang sama pada tanggal 3 Mei 2020, CEO Tokopedia William Tanuwijaya mengirimkan *email blast* kepada seluruh Penggunanya. Dalam *email blast*

tersebut, Tokopedia menginformasikan dan mengakui adanya pencurian terhadap data pribadi Penggunanya oleh pihak ketiga. Selain itu, Tokopedia telah melakukan investigasi untuk memastikan keamanan data pribadi Penggunanya dan juga merekomendasikan agar Penggunanya mengubah *password* akun.

C. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP)

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan dasar hukum yang jelas mengenai tanggung jawab perusahaan dalam menjaga data konsumen. Dengan penerapan UU PDP, pemerintah berharap dapat meminimalisir insiden kebocoran data yang selama ini kerap menghantui berbagai perusahaan teknologi di Indonesia. Keamanan siber telah menjadi isu global, dan Indonesia tidak luput dari ancaman tersebut. Kasus kebocoran data di Indonesia, mulai dari sektor perbankan hingga platform digital, telah menimbulkan kekhawatiran besar di kalangan masyarakat (INDONESIA.CO.ID, 2024).

UU PDP mencakup berbagai aspek penting yang sebelumnya diabaikan dalam regulasi terkait data di Indonesia. Undang-undang ini mengatur segala sesuatu mulai dari bagaimana data dikumpulkan, disimpan, diproses, hingga dihapus. UU PDP memberikan hak kepada individu untuk meminta akses, koreksi, dan bahkan penghapusan data pribadi mereka jika dirasa perlu.

1. Pasal 1 poin 2

UU UDP menyatakan pelindungan data pribadi sebagai seluruh upaya untuk melindungi data dalam rangkaian pemrosesan data pribadi untuk menjamin hak konstitusional subjek data pribadi, serta mengatur bagaimana data tersebut akan diberikan dan digunakan oleh pihak lain.

2. Pasal 4

Jenis data pribadi

UU PDP membagi data pribadi menjadi dua jenis, yaitu data pribadi umum dan data pribadi spesifik. Data pribadi umum boleh digunakan secara umum, seperti nama, alamat, status, agama, nomor telepon dan lainnya. Untuk data pribadi spesifik adalah data yang sensitif, seperti data kesehatan, data biometrika, atau catatan kriminal.

Hak pemilik data

Salah satu hal penting dalam UU PDP adalah hak pemilik data. Setiap individu berhak mengetahui bagaimana data mereka digunakan, siapa yang menggunakannya, memperbaiki data atau menolak penggunaan data, dan dapat meminta penghapusan data jika diperlukan. Konsep ini memberikan hak penuh kepada pemilik data terhadap penggunaan informasi pribadi mereka.

Peran pengelola data

UU PDP juga mengatur kewajiban pihak yang mengelola data pribadi, seperti perusahaan atau lembaga. Mereka harus memastikan data yang telah disimpan tetap aman, bertanggungjawab atas penggunaan data, dan tidak disebarluaskan tanpa izin pemilik. Jika kebocoran data, pengelola data wajib memberi tahu informasi tersebut atau memungkinkan dapat dikenakan sanksi hukum, termasuk denda besar atau hukuman pidana.

D. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

1. Pasal 1 ayat 4 dan 5

Penyelenggara Sistem Elektronik adalah setiap Orang, penyelenggara negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik secara sendiri-sendiri maupun bersama-sama kepada Pengguna Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain.

Penyelenggara Sistem Elektronik Lingkup Publik adalah penyelenggaraan Sistem Elektronik oleh Instansi Penyelenggara Negara atau institusi yang ditunjuk oleh Instansi Penyelenggara Negara.

2. Pasal 14 ayat 5

Jika terjadi kegagalan dalam pelindungan terhadap Data Pribadi yang dikelolanya, Penyelenggara Sistem Elektronik wajib memberitahukan secara tertulis kepada pemilik Data Pribadi tersebut.

3. Pasal 100 ayat 2 tentang sanksi

Sanksi administratif sebagaimana dimaksud pada ayat (1) dapat berupa:

a. teguran tertulis;
b. denda administratif;
c. penghentian sementara;
d. pemutusan Akses;
e. dikeluarkan dari daftar.

E. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik

1. Pasal 2 ayat 1 dan 2

- Perlindungan Data Pribadi dalam Sistem Elektronik mencakup perlindungan terhadap perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan Data Pribadi.

- Dalam melaksanakan ketentuan sebagaimana dimaksud pada ayat (1) harus berdasarkan asas perlindungan Data Pribadi yang baik, yang meliputi:
  a. penghormatan terhadap Data Pribadi sebagai privasi;
  b. Data Pribadi bersifat rahasia sesuai Persetujuan dan/atau berdasarkan ketentuan peraturan perundang-undangan;
  c. berdasarkan Persetujuan;
  d. relevansi dengan tujuan perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, dan penyebarluasan;
  e. kelaikan Sistem Elektronik yang digunakan;
  f. iktikad baik untuk segera memberitahukan secara tertulis kepada Pemilik Data Pribadi atas setiap kegagalan perlindungan Data Pribadi;
  g. ketersediaan aturan internal pengelolaan perlindungan Data Pribadi;
  h. tanggung jawab atas Data Pribadi yang berada dalam penguasaan Pengguna;
  i. kemudahan akses dan koreksi terhadap Data Pribadi oleh Pemilik Data Pribadi; dan
  j. keutuhan, akurasi, dan keabsahan serta kemutakhiran Data Pribadi.

2. Pasal 36 ayat 1

- Setiap Orang yang memperoleh, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarluaskan Data Pribadi tanpa hak atau tidak sesuai dengan ketentuan dalam Peraturan Menteri ini atau peraturan perundang-undangan lainnya dikenai sanksi administratif sesuai dengan ketentuan peraturan perundang-undangan berupa:
  a. peringatan lisan;
  b. peringatan tertulis;
  c. penghentian sementara kegiatan; dan/atau
  d. pengumuman di situs dalam jaringan (*website online*).

E. Kewajiban PT Tokopedia dalam melindungi Data Pribadi dari pemrosesan data secara melawan hukum

Untuk memastikan keamanan dan perlindungan data pribadi, Tokopedia memiliki tanggung jawab untuk mengelola sistem elektronik yang dapat melindungi data pribadi dari akses ilegal, perubahan, pengungkapan, atau kerusakan. Hal ini sejalan dengan Pasal 51 ayat 1 Undang-Undang Perlindungan Data Pribadi, yang mengharuskan pengendali data pribadi untuk menjaga keamanan data dengan menerapkan langkah-langkah pengamanan sesuai perkembangan teknologi. Selain itu, Tokopedia juga wajib memberikan informasi kepada pengguna terkait tujuan pengumpulan data pribadi, jenis data yang dikumpulkan, pihak yang akan menerima data tersebut, serta cara pengguna dapat mengakses dan memperbaiki datanya, sebagaimana tercantum dalam Pasal 51 ayat 2.

Persetujuan pengguna juga diperlukan sebelum data pribadi dikumpulkan, diproses, atau digunakan, sesuai ketentuan Pasal 51 ayat 3. Tokopedia hanya diperbolehkan memanfaatkan data pribadi untuk tujuan yang telah disetujui oleh pengguna dan tidak boleh menggunakannya untuk keperluan lain tanpa persetujuan pengguna, sebagaimana diatur dalam Pasal 51 ayat 4. Selain itu, jika pengguna meminta penghapusan data pribadinya, Tokopedia wajib menghapus data tersebut dengan cara yang aman dan memastikan data tidak dapat dipulihkan, sesuai ketentuan Pasal 51 ayat 5.

Simpulan

Era digital telah mendorong pertumbuhan pesat *e-commerce* di Indonesia, namun juga membawa tantangan besar dalam aspek perlindungan data pribadi konsumen. Kasus kebocoran data Tokopedia pada tahun 2020 menjadi salah satu contoh nyata pentingnya peningkatan keamanan data dan implementasi regulasi yang lebih efektif. Meskipun Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) memberikan kerangka hukum yang lebih kuat, implementasinya masih menghadapi kendala signifikan, seperti celah dalam regulasi, kurangnya penegakan hukum, dan minimnya kesadaran konsumen akan hak-hak mereka. Hal ini menunjukkan perlunya sinergi antara pemerintah, pelaku usaha, dan masyarakat dalam membangun ekosistem digital yang aman dan terpercaya. Rekomendasi untuk masa depan meliputi penguatan regulasi melalui harmonisasi dengan standar internasional seperti GDPR, peningkatan literasi digital masyarakat, serta adopsi teknologi dan protokol keamanan terkini oleh perusahaan *e-commerce*. Dengan langkah-langkah ini, diharapkan Indonesia dapat mengatasi tantangan perlindungan data pribadi sekaligus memanfaatkan potensi penuh ekonomi digital.

Daftar Pustaka

Bagaskara, A. E., Fadhil, S. M., & Mulyadi. (2023). PERLINDUNGAN HUKUM TERHADAP KONSUMEN DALAM TRANSAKSI ECOMMERCE.

Chisomo Tolani, & Prof. Jyoti Pareek. (2024). Introduction to Data Protection Frameworks: A Review. International Journal of Advanced Research in Science, Communication and Technology, 251–255. https://doi.org/10.48175/ijarsct-18732

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

Hartatik, Rukmana, A. Y., Efitra, E., Mukhlis, I. R., Aksenta, A., Ratnaningrum, L. P. R. A., & Efdison, Z. (2023). TREN TECHNOPRENEURSHIP : Strategi & Inovasi Pengembangan Bisnis Kekinian.

INDONESIA.CO.ID. (2024). Era Baru Perlindungan Data Pribadi. https://indonesia.go.id/kategori/editorial/8725/era-baru-perlindungan-data-pribadi

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

Nuranisa, A., & Lukitasari, D. (2024). Tindak Pidana Pencurian Data Dan Privasi Pengguna Dalam Transaksi E-Commerce. Amandemen: Jurnal Ilmu Pertahanan, Politik Dan Hukum Indonesia, 1(2), 115–126. https://doi.org/10.62383/amandemen.v1i2.145

Prayuti, Y. (2024). Dinamika Perlindungan Hukum Konsumen di Era Digital: Analisis Hukum Terhadap Praktik E-Commerce dan Perlindungan Data Konsumen di Indonesia. Jurnal Interpretasi Hukum, 5(1), 903–913. https://doi.org/10.22225/juinhum.5.1.8482.903-913

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

Tiffani, S., & Faisal. (2024). Analisis Hukum Terhadap Perlindungan Data Pribadi (Studi Kasus @farida.nurhan dan @codebluuuu). Jurnal Ilmu Hukum, Humaniora Dan Politik, 4(3), 291–300. https://doi.org/10.38035/jihhp.v4i3.1915