Indonesian Journal of Law

Vol. 2, No.10, September 2025
Hal 204-211

E-ISSN: 3032-3622
P-ISSN: 3032-3614

Site: https://jurnal.intekom.id/index.php/inlaw

Perlindungan Data Pribadi Konsumen atas Kebocoran Data Pada *E-Commerce*

Graciella Dominique Phie[1], Gunardi Lie[2]
[1,2] Fakultas Ilmu Hukum, Universitas Tarumanagara, Jakarta, Indonesia

Article Info

Article history:

Received September 20, 2025
Revised September 20, 2025
Accepted September 29, 2025

Kata Kunci:

Perlindungan data pribadi konsumen,
Kebocoran data pribadi,
Keamanan data pada *e-commerce*

Keywords:

Consumer personal data protection,
Personal data breaches,
Data security in e-commerce

ABSTRAK

Perkembangan teknologi informasi kian hari semakin berkembang pesat. Dengan adanya perkembangan ini, membuat kemudahan bagi para masyarakat dalam melakukan transaksi, karena munculnya platform *e-commerce*. Namun, dibalik kemudahan tersebut terdapat sisi negatif yaitu celah terjadinya kebocoran data berupa nama, alamat, ataupun rekening bank konsumen. Kebocoran data dapat menimbulkan risiko bagi para konsumennya seperti kemungkinan terjadinya peretasan rekening bank ataupun penyalahgunaan identitas. Tidak hanya menimbulkan risiko bagi konsumen, namun juga dapat menimbulkan risiko bagi pihak *e-commerce* seperti menurunnya rasa kepercayaan konsumen kepada platform *e-commerce*. Melalui penelitian secara normatif, penulis melakukan analisis terhadap undang-undang terkait peran hukum dalam melakukan perlindungan bagi konsumen. Dengan adanya perlindungan hukum terhadap data pribadi konsumen, maka konsumen dapat melakukan pelaporan kepada pihak yang berwajib apabila mengalami kebocoran data. Penulis juga meneliti terkait strategi perlindungan dari pihak *e-commerce* dalam meningkatkan perlindungan data pribadi penjual maupun pembeli, strategi perlindungan dari pemerintah dengan melakukan pengawasan dan perlindungan data pribadi masyarakat, pemberian fasilitas berupa edukasi dan sertifikasi kepada masyarakat, dan melakukan kerja sama secara internasional untuk memperkuat strategi perlindungan data pribadi. Strategi perlindungan dari masyarakat juga diperlukan dengan meningkatkan pemahaman terkait perlindungan data pribadi. Strategi perlindungan tersebut juga perlu diketat agar memperkecil celah terjadinya kebocoran data.

ABSTRACT

The development of information technology is rapidly advancing every day. With this progress, it has become easier for people to conduct transactions duet o the emergence of e-commerce platforms. However, behind this convenience, there is a negative side, namely risk of data breaches involving consumers' names, addresses, or bank account information. Data breaches can pose risks to consumers, such as the possibility of bank account hacking or identity misuse. These risks not only affect consumers but also e-commerce platforms, as they may experience a decline in consumer trust. Through normative research, the author analyzes laws related to the role of legislation in protecting consumers. With legal protection for consumers' personal data, consumers can reportt to the authorities if a data breach occurs. The author also examines protection strategies froem e-commerce platforms to enhance the protection of personal data for both sellers and buyers; government strategies involving supervision and protection of citizens' personal data, providing facilities such as education and certification to the public, and engaging in international cooperation to strengthen

E-ISSN : 3032-3622
P-ISSN : 3032-3614

personal data protection strategies. Additionally, protection strategies from society are necessary by increasing awareness about personal data protection. These protection strategies need to be tightened to minimize the risk of data breaches.

Corresponding Author:

Graciella Dominique Phie
Fakultas Ilmu Hukum, Universitas Tarumanagara
Jakarta, Indonesia
Email: graciella.205240048@stu.untar.ac.id

1. PENDAHULUAN

Kian hari perkembangan teknologi informasi berkembang semakin pesat. Kehidupan sehari-hari masyarakat sudah selalu didampingi dengan teknologi, baik dalam komunikasi, informasi, edukasi, dan bahkan dalam kegiatan jual beli. Kegiatan perdagangan pada masa sekarang tidak hanya dapat dilakukan dengan berinteraksi secara langsung, tetapi dapat juga dilakukan dengan berinteraksi secara tidak langsung yaitu melakukan jual beli secara elektronik atau yang dikenal dengan *e-commerce*. *E-commerce* merupakan kegiatan transaksi jual beli secara elektronik yang dilakukan melalui jaringan internet dan muncul pada tahun 1962 di mana J.C.R Licklider memperkenalkan konsep dasar jaringan komputer[1] lalu masuk di Indonesia pada tahun 1990-an. Pengguna *e-commerce* di Indonesia terus mengalami pertumbuhan pengguna karena adanya keuntungan yang diberikan oleh *e-commerce* kepada konsumen, seperti kemudahan dalam pencarian barang maupun pembelian. Tidak hanya memberikan keuntungan kepada konsumen, *e-commerce* juga memberikan keuntungan kepada pelaku usaha seperti kemudahan dalam melakukan penjualan tanpa adanya kesalahan dan tepat waktu serta keuntungan bagi perusahaan *e-commerce* seperti meningkatnya pendapatan dan loyalitas konsumen[2]. Pada tahun 2024, laporan yang dirilis oleh Statista menunjukkan penggunaan *e-commerce* di Indonesia mencapai 65.65 juta orang[3]. Dari data statistik tersebut dapat diketahui bahwa, peminat penggunaan *e-commerce* semakin meningkat karena dapat memberikan kemudahan dan keuntungan bagi para konsumen dalam melakukan kegiatan perdagangan tanpa harus berinteraksi secara langsung maupun bagi para wiraswasta di platform *e-commerce* dan bagi perusahaan.

Kemudahan yang ditawarkan oleh *e-commerce* kepada konsumen tentunya perlu disertai dengan perlindungan data pribadi. Tiap *e-commerce* membutuhkan data pribadi para konsumen seperti nama lengkap, nomor telepon, alamat *email*, alamat rumah, dan rekening bank dengan tujuan verifikasi data dan kemudahan pengiriman barang ke alamat konsumen[4]. Menurut Pasal 1 Ayat (1) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, data pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik. Hal ini sudah menjadi kewajiban bagi para pelaku bisnis di *e-commerce* untuk mengelola data pribadi konsumennya dengan baik yang disertai dengan perlindungan dan tidak menyalahgunakan data pribadi konsumennya diluar kebutuhan *e-commerce*.

Namun di era digital saat ini, kasus kebocoran data semakin marak terjadi. Di *e-commerce* sendiri banyak terjadinya peristiwa kebocoran data, seperti kejadian kebocoran data yang terjadi pada platform Bukalapak pada tahun 2019 di mana terdapat 13 juta akun konsumen yang ditembus secara tidak sah oleh hacker asal Pakistan, untungnya data penting dan informasi pribadi berhasil didapatkan. Maju pada bulan Juli tahun 2020, terjadi peristiwa kebocoran data berupa pembelian 91 juta akun konsumen Tokopedia yang

ditemukan oleh Lembaga Riset Siber Indonesia Communication and Information System Security Research Center (CISSReC). Dan ada pula peristiwa kebocoran data supermarket online RedMart milik Lazada, di mana pada bulan Oktober sebanyak 1,1 juta data konsumen platform tersebut ditembus secara tidak sah dan bahkan informasi para konsumen yang bocor tersebut diperdagangkan[5]. Terjadinya kebocoran data pengguna *e-commerce* ini dapat memberikan dampak bagi para penggunanya, yaitu

i. Adanya risiko menjadi korban penipuan atau *phising;*
ii. Menerima banyak spam;
iii. Identitas yang disalahgunakan; dan
iv. Memungkinkan terjadinya pembobolan rekening bank para pengguna[6].

Bahkan kebocoran data ini tidak hanya berdampak bagi para penggunanya saja, namun juga berdampak bagi perusahaan, di mana perusahaan akan mengalami

i. Penurunan loyalitas pelanggan dan bahkan tercorengnya nama baik Perusahaan;
ii. Dikenai sanksi dan denda; dan
iii. Perusahaan harus mengeluarkan biaya besar untuk memulihkan system data *e-commerce.*

Implementasi penegakan hukum yang mengacu pada perlindungan data pribadi di Indonesia juga masih tergolong lemah, kejadian ini disebabkan karena[7]

i. Biaya implementasi yang tinggi, sebab perusahaan perlu mengembangkan infrastruktur keamanan siber, memperbarui sistem Perusahaan, ataupun membimbing para karyawan agar dapat mematuhi standar terbaru;
ii. Rendahnya literasi digital para konsumen terkait pentingnya perlindungan data pribadi, baik itu perlindungan data pribadi milik seorang diri maupun data pribadi milik anak, penyandang disabilitas, dan lansia;
iii. Ketidakjelasan mekanisme perlindungan data pribadi dari lembaga pengawas;
iv. Penegakan hukum yang kurang konsisten dan adil; dan
v. Kendala dalam menangani kasus kebocoran data yang berhubungan dengan pihak internasional.

Berbeda dengan regulasi negara Uni Eropa dalam melakukan perlindungan data pribadi masyarakatnya, regulasi Uni Eropa dikenal dengan *General Data Protection Regulation* (GDPR) yang disahkan pada tahun 2016 dan mulai berlaku pada tanggal 25 Mei 2018. Di mana peraturan ini memberlakukan ketentuan perihal pertanggungjawaban perusahaan terhadap data pribadi konsumen, memberlakukan standar enkripsi, permohonan persetujuan dari konsumen, dan memberlakukan jangka waktu tersimpannya sebuah data dalam perusahaan. GDPR juga menetapkan sebuah mekanisme di mana semua anggota Uni Eropa memiliki kewajiban dalam membentuk instansi yang memiliki tugas dalam melakukan perlindungan data[8]. Sedangkan di Indonesia sendiri masih memiliki kekurangan dalam pemberlakuan peraturan jangka waktu data konsumen tersimpan dalam perusahaan.

Dari uraian diatas dapat dilihat bahwa perlindungan data pribadi konsumen di *e-commerce* sangat penting agar tidak memberikan dampak negatif baik bagi konsumen, pelaku usaha, maupun negara. Oleh karena itu, penelitian ini akan membahas secara spesifik rumusan masalah dibawah ini:

i. Bagaimana perlindungan hukum yang dapat diberikan kepada konsumen yang mengalami kebocoran data di *e-commerce?*
ii. Strategi apa yang perlu diterapkan untuk meningkatkan perlindungan data pribadi konsumen dari kebocoran data?

2. METODE

Penelitian ini menggunakan penelitian hukum normatif. Penelitian hukum normatif Adalah penelitian yang meletakkan hukum sebagai bangunan sisten norma untuk menjawab permasalahan hukum yang dihadapi[9]. Teknik pengumpulan data dari penelitian ini yaitu studi kepustakaan, di mana penulis berfokus

mengambil segala sumber informasi melalui jurnal, buku, dan artikel. Jenis sumber data yang diterapkan dalam penelitian ini ada dua yaitu sumber hukum primer seperti peraturan perundang-undang dan sumber hukum sekunder seperti literatur dan hasil penelitian untuk memahami konsep hukum secara teoritis dan konseptual tanpa terjun langsung ke lapangan. Analisis data dilakukan secara deskriptif-analitis dengan cara menginterpretasikan norma hukum dan mengkaji perlindungan hukum dalam mengamankan data pribadi konsumen yang mengalami kebocoran di *e-commerce*. Penelitian ini juga mempertimbangkan aspek sosial dan teknis terkait perlindungan data guna memberikan rekomendasi berupa peningkatan strategi perlindungan data pribadi yang komprehensif dan aplikatif bagi pihak *e-commerce*, negara, dan juga masyarakat.

3. HASIL DAN PEMBAHASAN

3.1. Perlindungan Hukum Yang Dapat Diberikan Kepada Konsumen Yang Mengalami Kebocoran Data Pribadi di *E-Commerce*

Tiap konsumen pastinya telah melakukan perlindungan data pribadi mereka di platform *e-commerce*. Baik itu dengan cara menggunakan kata sandi yang kuat, membatasi pemberian informasi data pribadi, selalu memperbarui perangkat lunak aplikasi *e-commerce*, atau bahkan dengan melakukan verifikasi dua langkah. Fitur verifikasi dua langkah adalah perlindungan ekstra yang berfungsi melindungi akun penggunanya dari penipuan atau tindakan lain yang tidak sah[10]. Namun, walaupun konsumen telah melakukan berbagai cara untuk melindungi data pribadi mereka, data pribadi konsumen tetap terdapat peluang terjadinya kebocoran apabila konsumen tidak waspada dengan *phising*. *Phising* merupakan kejahatan daring yang dilakukan dengan cara memanipulasi data atau menipu individu agar memberikan informasi pribadinya[11], maka dari itu para konsumen perlu waspada apabila menerima pesan melalui *e-mail* ataupun lewat media lainnya yang mengatasnamakan *e-commerce* dan meminta para konsumen melakukan *login* karena bisa saja tindakan tersebut merupakan *phising*.

Meskipun fitur verifikasi dua langkah menjadi salah satu pilihan dalam perlindungan data pribadi, namun ada beberapa faktor yang dapat membuat kebocoran data dapat terjadi. Penyebab kebocoran data terjadi selain karena *phising* yaitu karena lemahnya sistem keamanan, kelalaian manusia berupa salah kirim email, kesalahan konfigurasi, atau pengelolaan data yang ceroboh, ancaman dari orang sekitar yang telah memiliki akses data pribadi, perangkat hilang atau dicuri, dan kurangnya kepatuhan terhadap regulasi yang ada[12]. Dari faktor tersebut dapat diketahui bahwa perlindungan teknis saja tidak cukup untuk melindungi data pribadi konsumen. Oleh sebab itu diperlukan perlindungan hukum yang menjadi mekanisme tambahan dalam perlindungan data pribadi konsumen.

Hukum memberikan perlindungan kepada konsumen yang mengalami kebocoran data melalui beberapa peraturan yang telah disahkan oleh pemerintah. Salah satu dasar hukum yang membahas terkait perlindungan data pribadi yaitu, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Undang-undang ini mengatur mengenai kewajiban pelaku usaha, termasuk pelaku usaha di platform *e-commerce,* dalam menjaga data pribadi konsumennya. Jika para wiraswasta lalai dalam melindungi data pribadi konsumennya, maka akan diberikan sanksi berupa sanksi administratif sesuai yang tertulis pada Pasal 57 Ayat (2) UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi yang berbunyi "Sanksi administratif sebagaimana yang dimaksud pada ayat (1) berupa:

i. Peringatan tertulis;
ii. Penghentian sementara kegiatan pemrosesan Data Pribadi;
iii. Penghapusan atau pemusnahan Data Pribadi; dan/atau
iv. Denda administratif."

Hukum juga melindungi konsumen dari kebocoran data melalui penjatuhan pidana sesuai dengan ketentuan yang ada pada pasal 67 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, dengan ketentuan sebagai berikut

i. Setiap orang yang dengan sengaja memperoleh atau mengumpulkan data pribadi yang bukan miliknya untuk keuntungan sendiri atau orang lain dan menimbulkan kerugian pada subjek data pribadi tersebut dipidana penjara selama lima tahun dan/atau pidana denda paling banyak lima miliar rupiah.
ii. Setiap orang yang dengan sengaja mengungkapkan data pribadi yang bukan miliknya dipidana penjara paling lama empat tahun dan/atau denda paling banyak empat miliar rupiah.
iii. Setiap orang dengan sengaja menggunakan data pribadi yang bukan miliknya dipidana penjara paling lama lima tahun dan/atau pidana denda paling banyak lima miliar rupiah.

Adapun dalam Pasal 68 Undang-undang Nomor 27 Tahun 2022 tentang perlindungan data pribadi disebutkan bahwa orang yang dengan sengaja melakukan atau membuat pemalsuan data pribadi untuk keuntungan diri sendiri atau orang lain sehingga menimbulkan kerugian bagi orang lain akan dipidana penjara paling lama enam tahun dan/atau denda paling banyak enam miliar rupiah.

Dalam Pasal 26 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik, disebutkan hak seseorang atas data pribadinya, yaitu

i. Berhak atas kerahasiaan Data Pribadinya;
ii. Berhak mengajukan pengaduan untuk menyelesaikan sengketa Data Pribadinya kepada Menteri;
iii. Berhak mendapatkan akses untuk mengubah atau memperbarui Data Pribadinya tanpa mengganggu sistem pengelolaan Data Pribadi, kecuali ditentukan lain oleh peraturan perundang-undang;
iv. Berhak mendapatkan akses atas historis Data Pribadinya yang sudah diserahkan kepada Penyelenggara Sistem Elektronik sesuai dengan ketentuan peraturan perundang-undangan; dan
v. Berhak meminta pemusnahan Data Pribadi miliknya dalam sistem elektronik yang dikelola oleh Penyelenggara Sistem Elektronik, kecuali ditentukan lain oleh peraturan perundang-undangan.

Sehingga, apabila konsumen mengalami kebocoran data, para konsumen berhak melakukan laporan kepada pihak *e-commerce* melalui *call center* ataupun *customer service*. Pelaporan kepada pihak *e-commerce* menjadi langkah awal saat terjadi kebocoran data agar pihak *e-commerce* dapat melakukan pengamanan dan investigasi dari insiden tersebut[13]. Namun, apabila respon dari pihak *e-commerce* tidak memuaskan, konsumen dapat melakukan laporan kepada pihak kepolisian agar kejahatan siber dapat diusut dan dijatuhi hukuman berupa sanksi sesuai dengan peraturan hukum yang berlaku. Konsumen juga dapat melaporkan kepada Otoritas Jasa Keuangan (OJK) dan Asosiasi Fintech Pendanaan Bersama Indonesia (AFPI) yang berfungsi mengawasi dan menindak pelaku usaha yang melanggar ketentuan perlindungan konsumen. Dengan adanya berbagai jalur pelaporan dan penangan kebocoran data pribadi konsumen, diharapkan konsumen dapat merasa lebih aman dan terlindungi dalam melakukan kesepakatan jual beli di *e-commerce*.

3.2 Strategi Peningkatan Perlindungan Data Pribadi Konsumen Dari Kebocoran Data

Perlindungan data pribadi konsumen dari kebocoran data tidak hanya bersumber dari perlindungan hukum saja, namun strategi peningkatan perlindungan data pribadi konsumen di platform *e-commerce* juga sangat diperlukan dan menjadi pendukung dalam perlindungan data pribadi. Penting bagi pihak *e-commerce* untuk meningkatkan dan memiliki kebijakan privasi yang transparan dan jelas agar para konsumen dapat mengetahui persoalan data pribadi mereka dikumpulkan, dimanfaatkan, dan diamankan. Seperti yang tertulis dalam Pasal 27 UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi bahwa "Pengendali Data Pribadi wajib melakukan pemrosesan Data Pribadi secara terbatas dan spesifik, sah secara hukum, dan transparan". Pemerintah juga perlu meningkatkan strategi mereka dalam melakukan pengawasan data pribadi serta dapat memberikan nasihat kepada masyarakat terkait pentingnya perlindungan data pribadi.

E-commerce bisa menjadi sasaran empuk para peretas untuk mendapatkan data pribadi konsumen, sebab di dalam *e-commerce* terdiri dari nama, alamat, NIK, dan rekening bank. Maka dari itu, pihak *e-commerce* perlu meningkatkan perlindungan data pribadi konsumennya dengan cara[14],

vi. Menggunakan sertifikasi Secure Socket Layer (SSL). SSL merupakan standar keamanan yang memastikan semua data yang ditransfer anatara server dan browser tetap terenkripsi. SSL ini sangat penting untuk memastikan semua data konsumen tetap aman selama transaksi di *e-commerce*;
vii. Mengaktifkan Otentikasi Multi-Faktor (MFA). Otentikasi multi-faktor merupakan cara efektif untuk menambah lapisan keamanan, karena dengan MFA pengguna harus melalui lebih dari satu verifikasi sebelum mengakses akun;
viii. Melakukan pembaharuan dan perubahan sistem platform *e-commerce* secara rutin. Platform *e-commerce* harus selalu dilakukan pembaharuan untuk mencegah peluang terjadinya peretasan;
ix. Menggunakan firewalldan sistem pemantauan firewall aplikasi web (WAF) untuk mempertahankan dan melindungi *e-commerce* dari serangan berbahaya seperti DDoS dan injeksi SQL;
x. Menggunakan proteksi untuk melindungi dari serangan DDoS;
xi. Melakukan backup data secara rutin dan disimpan di tempat yang aman dan ideal;
xii. Melakukan enkripsi data pelanggan;
xiii. Melakukan pelatihan keamanan siber kepada karyawan secara rutin;
xiv. Melakukan audit keamanan secara berkala untuk mengidentifikasi potensi kerentanan dalam sistem *e-commerce*; dan
xv. Mematuhi standar Payment Card Industry Data Security Standard (PCI DSS) untuk melindungi data dan mencegah pencurian informasi pemegang kartu kredit.

Tidak hanya itu, perusahaan *e-commerce* juga sangat perlu untuk memiliki sertifikasi ISO 27001. Sertifikasi ISO 27001 adalah sertifikasi standar internasional yang menetapkan persyaratan guna sistem manajemen keamanan informasi (ISMS)[15]. Sertifikasi ISO 27001 dapat menjadi pedoman para *e-commerce* dalam menjamin perlindungan keamanan data para penggunanya, baik itu data para penjual maupun pembeli[16]. Karena dengan dimilikinya sertifikasi ISO 27001 oleh perusahaan *e-commerce*, dapat dipastikan bahwa informasi para konsumen terlindungi dari kebocoran dan akses yang tidak sah, dapat meningkatkan kembali kepercayaan konsumen kepada perusahaan *e-commerce*, dan memastikan perusahaan *e-commerce* mematuhi regulasi yang ada serta terhindar dari denda dan sanksi hukum[17].

Pemerintah juga berperan penting dalam meningkatkan perlindungan data pribadi para konsumen. Pemerintah dapat meningkatkan strategi perlindungan data pribadi tidak hanya dalam pengawasan namun dapat dilakukan dengan cara menegakkan hukum melalui pemberian sanksi terhadap *e-commerce* yang melanggar aturan perlindungan data pribadi, menyediakan sertifikasi dan akreditasi guna membantu memastikan *e-commerce* memenuhi standar untuk menjaga dan melindungi data pribadi konsumennya, serta pemerintah dapat melakukan kolaborasi secara internasional untuk meningkatkan kesadaran serta perlindungan data pribadi dan dapat mengadopsi teknik negara lain dalam melindungi data pribadi konsumennya[18]. Pemerintah juga dapat melakukan edukasi kepada masyarakat berupa pelatihan secara berkelanjutan agar meningkatkan literasi digital serta kesadaran akan pentingnya pemahaman perlindungan data pribadi. Perlunya pemberian pemahaman kepada masyarakat berupa edukasi agar perlindungan data pribadi dapat berjalan dengan baik karena adanya sikap bahu-membahu dalam melakukan perlindungan data pribadi antara pemerintah, *e-commerce*, dan masyarakat, dengan begitu celah terjadinya peretasan data pribadi akan semakin kecil, berkurangnya risiko kerugian dalam keuangan, serta memastikan baik negara, Perusahaan *e-commerce*, maupun masyarakat mematuhi peraturan perundang-undangan yang berlaku.

4. KESIMPULAN

Perlindungan konsumen sangat dibutuhkan di Indonesia dikarenakan hingga saat ini masih marak terjadi peretasan data pribadi konsumen di *e-commerce* yang berujung konsumen mengalami penipuan. Dengan adanya peraturan undang-undang yang mengatur tentang perlindungan data pribadi, diharapkan data pribadi para konsumen dapat dilindungi, diawasi, serta segera dilakukan tindak lanjut apabila konsumen melakukan pelaporan kepada pihak yang berwajib. Peran pihak *e-commerce* dan pemerintah

sangat penting dalam meningkatkan strategi perlindungan data pribadi konsumen agar memperkecil celah terjadinya kebocoran data pribadi, sebab kebocoran data pribadi ini tidak hanya berdampak pada konsumen yang mengalami kebocoran data tetapi juga dapat berdampak pada pihak *e-commerce* dan juga negara. Masyarakat sendiri pun perlu turut berperan dalam melindungi data pribadi mereka dengan cara meningkatkan pemahaman terkait kebocoran data pribadi agar selalu berhati-hati dalam melaksanakan transaksi di *e-commerce* ataupun melakukan pendaftaran dalam platform *e-commerce*.

REFERENSI

[1] Muallif, "E-commerce: Pengertian, Sejarah, Macam, Kekurangan dan Kelebihan, serta Pandangan Islam." Universitas Islam An Nur Lampung, Nov. 27, 2022. [Online]. Available: https://an-nur.ac.id/e-commerce-pengertian-sejarah-macam-kekurangan-dan-kelebihan-serta-pandangan-islam/

[2] M. Mariana, "Apa itu E-commerce?" Universitas Pasundan, Feb. 17, 2012. [Online]. Available: https://www.unpas.ac.id/apa-itu-e-commerce/

[3] K. U. J. Putri, "Pengguna e-commerce Indonesia diprediksi naik 11,2 persen pada 2025," *Tech in Asia*, Jan. 23, 2025. [Online]. Available: https://id.techinasia.com/pengguna-e-commerce-indonesia-naik-2025#:~:text=23%20Jan%202025-,Pengguna%20e%2Dcommerce%20Indonesia%20diprediksi%20naik%2011%2C2%20persen%20pada,berupaya%20lepas%20ketergantungan%20dari%20marketplace

[4] N. R. Latifa, "Mengapa Bisnis E-Commerce Harus Memperhatikan Kepatuhan UU PDP?" Sibermate, Jan. 20, 2025. [Online]. Available: https://sibermate.com/hrmi/mengapa-bisnis-e-commerce-harus-memperhatikan-kepatuhan-uu-pdp

[5] I. Malia, "Sebelum BPJS Kesehatan, Ini 3 Kasus Kebocoran Data Konsumen E-Commerce," *IDN Times*, Mei 2021. [Online]. Available: https://www.idntimes.com/business/economy/selain-bpjs-kesehatan-ini-3-kasus-kebocoran-data-konsumen-e-commerce-00-9751v-45nb0z

[6] V. Septiriani, T. Sofyan, and W. N. Rosari, "Tanggung Jawab Pelaku Usaha Terhadap Kebocoran Informasi Data Pribadi Konsumen Dalam Pelaksanaan Perdagangan Elektronik (E-Commerce)," *J. Ilm. Kutel*, vol. 23, no. 1, pp. 127–136, Apr. 2024, doi: https;//doi.org/10.33369/jik.v23il.36388.

[7] M. R. Syailendra, "Perlindungan Data Pribadi: Implementasi UU No. 27 Tahun 2022 dan Tantangan Penegakannya." Universitas Tarumanagara Fakultas Hukum. [Online]. Available: https://fh.untar.ac.id/2025/09/11/perlindungan-data-pribadi-implementasi-uu-no-27-tahun-2022-dan-tantangan-penegakannya/

[8] S. A. Ramadhani, "Komparasi Pengaturan Perlindungan Data Pribadi Di Indonesia dan Uni Eropa," *J. Huk. Lex Gen.*, vol. 3, no. 1, pp. 73–84, Jan. 2021.

[9] M. F. ND, *Dualisme Penelitian Hukum Normatif & Empiris*. Yogyakarta: Pustaka Pelajar, 2017.

[10] Anonim, "[Keamanan Akun] Apa itu Verifikasi 2 (dua) Langkah?" Pusat Bantuan Shopee. [Online]. Available: https://help.shopee.co.id/portal/4/article/110995-[Keamanan-Akun]-Apa-itu-verifikasi-2-(dua)-langkah

[11] Ismail, A. Widiarti, D. Muhadiansyah, and E. Koesumah, *Bahaya Phising*. TEMPO Publisihing, 2024.

[12] Anonim, "Penyebab Kebocoran Data Pribadi dan Solusi Pencegahannya," *XL Satu*, Jan. 21, 2025. [Online]. Available: https://satu.xl.co.id/berita-dan-artikel/penyebab-kebocoran-data-pribadi

[13] Anonim, "Cara Melaporkan Pencurian Data Pribadi." Asosiasi Fintech Pendanaan Bersama Indonesia (AFPI). [Online]. Available: https://afpi.or.id/articles/detail/cara-melaporkan-pencurian-data-pribadi

[14] Diannovita, "Strategi Cyber Security untuk E-Commerce: Mengamankan Toko Online Anda," *Tim Tanggap Insiden Siber (TTIS) Teknorat*, Agustus 2024. [Online]. Available: https://csirt.teknokrat.ac.id/strategi-cyber-security-untuk-e-commerce-mengamankan-toko-online-anda/

[15] Anonim, "Sertifikasi ISO 27001." Integrated Assessment Service. [Online]. Available: https://ias-indonesia.org/sertifikasi-iso-27001/

[16] M. Mamduh, "Strategi E-Commerce Lindungi Data Pribadi Pengguna," *medcom.id*, Desember 2024. [Online]. Available: https://www.medcom.id/teknologi/news-teknologi/yKXLqX0K-strategi-e-commerce-lindungi-data-pribadi-pengguna

[17] N. D. Arini, "Keamanan E-commerce dengan ISO 27001: Standar Wajib untuk Perlindungan Data." Pusat Sertifikasi BNSP, Sept. 24, 2025.
[18] R. Milafebina, I. P. Lesmana, and M. R. Syailendra, "Perlindungan Data Pribadi terhadap Kebocoran Data Pelanggan E-Commerce di Indonesia," *J. Tana Maya*, vol. 4, no. 1, 2023, doi: https://doi.org/10.33648/jtm.v4i1.331.