

## Tinjauan Yuridis Undang-Undang Perlindungan Data Pribadi Tahun 2022 dalam Menangani Kebocoran Data Pelanggan E-Commerce

Lingga Syailendra Arief<sup>1\*</sup>, Ruli Purwanto<sup>2</sup>

<sup>1,2</sup> Fakultas Hukum, Universitas Cokroaminoto Yogyakarta, Indonesia  
[linggasyailendraarief@gmail.com](mailto:linggasyailendraarief@gmail.com)<sup>1\*</sup>, [librarulip@gmail.com](mailto:librarulip@gmail.com)<sup>2</sup>

Alamat: Jl. Perintis Kemerdekaan Jl. Gambiran, Pandeyan, Kec. Umbulharjo, Kota Yogyakarta, Daerah Istimewa Yogyakarta (55161)

Korespondensi penulis: [linggasyailendraarief@gmail.com](mailto:linggasyailendraarief@gmail.com)\*

**Abstract.** *In the rapidly evolving digital era, data breaches have emerged as a serious threat, particularly in the e-commerce sector which handles vast amounts of customers' personal data. The protection of personal data has therefore become a crucial issue, requiring effective regulation to ensure digital privacy. In response to this growing concern, Indonesia enacted the Personal Data Protection Law (UU PDP) in 2022 as a significant step toward strengthening digital privacy and security. This study aims to evaluate the effectiveness of the 2022 PDP Law in addressing customer data breach incidents on e-commerce platforms in Indonesia. Using a qualitative approach and case study method, this research analyzes several high-profile data breach cases involving major e-commerce companies in the country. The findings indicate that, although the PDP Law has established a clear legal framework regarding the obligations of reporting and managing data breaches, its implementation still faces multiple challenges. Some companies have not fully complied with the legal timeframes for notifying users, and there is a general lack of transparency in how data breach incidents are managed. These shortcomings reveal a gap between the regulatory framework and practical enforcement in the field. Furthermore, the study highlights the limited public awareness and the insufficient preparedness of some companies in responding to data security incidents in accordance with the law. As a result, the rights of consumers to be informed and protected are not always upheld effectively. This research recommends stronger supervision by relevant authorities to ensure stricter enforcement of the PDP Law. It also underscores the need for ongoing education and intensive training for e-commerce companies to enhance their capacity to prevent, detect, and respond to data breaches in compliance with the legal standards. By reinforcing regulatory implementation and organizational readiness, Indonesia can better safeguard digital consumer rights in the growing e-commerce landscape.*

**Keywords:** *Consumer Privacy, Cybersecurity, Data Breaches, E-Commerce, Personal Data Protection Law*

**Abstrak.** Di era digital yang berkembang pesat, kebocoran data menjadi salah satu ancaman serius, terutama dalam sektor e-commerce yang mengelola data pribadi pelanggan dalam jumlah besar. Perlindungan data pribadi pun menjadi isu yang sangat krusial dan menuntut regulasi yang efektif demi menjaga privasi dan keamanan informasi digital. Menanggapi tantangan tersebut, pemerintah Indonesia telah mengesahkan Undang-Undang Perlindungan Data Pribadi (UU PDP) pada tahun 2022 sebagai langkah penting dalam memperkuat perlindungan data dan hak privasi warga negara. Penelitian ini bertujuan untuk mengevaluasi efektivitas implementasi UU PDP 2022 dalam menangani insiden kebocoran data pelanggan yang terjadi di platform e-commerce Indonesia. Dengan menggunakan pendekatan kualitatif dan metode studi kasus, penelitian ini menganalisis beberapa insiden kebocoran data yang menimpa perusahaan e-commerce besar di Indonesia dalam beberapa tahun terakhir. Hasil penelitian menunjukkan bahwa meskipun UU PDP 2022 telah memberikan kerangka hukum yang jelas mengenai kewajiban pelaporan dan penanganan kebocoran data, implementasi di lapangan masih menghadapi berbagai kendala. Beberapa perusahaan belum sepenuhnya mematuhi batas waktu pelaporan kepada pengguna, dan kurang transparan dalam menyampaikan informasi terkait penanganan insiden kebocoran data. Selain itu, kesadaran publik dan kesiapan internal perusahaan dalam merespons insiden keamanan data juga masih tergolong rendah. Kesenjangan antara regulasi dan penerapan praktis ini menunjukkan perlunya penguatan pengawasan dan penegakan hukum dari otoritas terkait. Studi ini merekomendasikan peningkatan kapasitas perusahaan e-commerce melalui pelatihan, edukasi, serta penerapan kebijakan keamanan data yang sesuai dengan ketentuan UU PDP. Dengan memperkuat penerapan regulasi dan meningkatkan kesiapan organisasi dalam menghadapi risiko digital, diharapkan hak-hak konsumen atas perlindungan data pribadi dapat lebih terjamin di tengah perkembangan pesat industri e-commerce Indonesia.

**Kata kunci:** Keamanan Siber, Pelanggaran Data, Perdagangan Elektronik, Privasi Konsumen, Undang-Undang Perlindungan Data Pribadi

## **1. LATAR BELAKANG**

Kebocoran data pribadi pelanggan dalam e-commerce di Indonesia menjadi fenomena yang kian mengkhawatirkan, terutama seiring meningkatnya penetrasi teknologi digital dalam kehidupan sehari-hari. Dalam beberapa tahun terakhir, berbagai insiden pelanggaran data melibatkan platform besar seperti Tokopedia dan Bukalapak, yang menimbulkan keresahan publik terhadap keamanan informasi pribadi yang mereka serahkan kepada penyedia layanan daring. Kepercayaan konsumen menjadi elemen krusial dalam sistem ekonomi digital, dan kerentanannya terhadap penyalahgunaan informasi dapat berdampak langsung terhadap kerugian ekonomi maupun psikologis individu.

Di Indonesia, sejumlah kasus kebocoran data pelanggan e-commerce menjadi perhatian publik, seperti peretasan yang menimpa Tokopedia (2020), Bukalapak (2021), dan kasus dugaan jual beli data nasabah oleh pihak ketiga yang menyeret berbagai perusahaan digital. Kejadian-kejadian ini tidak hanya mengancam privasi individu, tetapi juga melemahkan kepercayaan publik terhadap sistem digital nasional dan integritas pelaku usaha berbasis daring.

Sebagai respons terhadap situasi tersebut, Pemerintah Indonesia menetapkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang dirancang untuk memberikan kepastian hukum dan perlindungan menyeluruh terhadap data pribadi masyarakat. Undang-Undang ini mengatur kewajiban pengendali data, hak subjek data, hingga sanksi administratif dan pidana bagi pelanggar. Namun demikian, efektivitas implementasi Undang-Undang Perlindungan Data Pribadi Tahun 2022 masih menjadi perdebatan di kalangan akademisi dan praktisi hukum, mengingat lemahnya kapasitas penegakan hukum siber dan belum adanya lembaga otoritas independen pengawas data.

Dalam konteks e-commerce, penindakan hukum terhadap kebocoran data pelanggan e-commerce seperti yang terjadi pada kasus Tokopedia (2020), Bukalapak (2021), atau peretasan akun BRI Life (2022), menunjukkan bahwa masih terdapat celah dalam mekanisme pelaporan, forensik, dan pemulihan hak korban. Ini menuntut penguatan instrumen penegakan, koordinasi lintas lembaga, serta peningkatan edukasi hukum dan digital security bagi pelaku usaha.

Studi sebelumnya banyak menyoroti aspek normatif atau perbandingan hukum, tetapi belum banyak yang menelaah secara kualitatif bagaimana persepsi dan pengalaman aktor-aktor kunci, seperti pelanggan dan pelaku usaha e-commerce, terhadap penerapan Undang-Undang Perlindungan Data Pribadi Tahun 2022. Selain itu, kajian yang mengaitkan langsung antara

kebijakan Undang-Undang Perlindungan Data Pribadi Tahun 2022 dengan dampaknya terhadap perubahan praktik perlindungan data di industri e-commerce juga masih terbatas .

Masih banyak platform e-commerce yang belum secara transparan mempublikasikan kebijakan privasi sesuai amanat Undang-Undang Perlindungan Data Pribadi Tahun 2022 , dan belum menyusun sistem keamanan data yang andal. Bahkan dalam beberapa kasus, laporan insiden kebocoran data tidak disampaikan ke publik maupun otoritas dalam jangka waktu yang ditentukan.

Ketidakhadiran lembaga pengawas independen seperti yang dijanjikan oleh Undang-Undang Perlindungan Data Pribadi Tahun 2022 juga memperlemah penegakan hukum dan pengawasan implementasi kebijakan ini . Hal ini menunjukkan bahwa meskipun secara normatif regulasi telah tersedia, penerapannya masih menghadapi berbagai hambatan struktural dan institusional.Selain itu, tingkat literasi digital masyarakat yang rendah turut mempersulit implementasi Undang-Undang Perlindungan Data Pribadi Tahun 2022 secara menyeluruh. Banyak pengguna belum memahami hak-haknya sebagai subjek data, termasuk hak atas akses, koreksi, penghapusan, dan keberatan terhadap pemrosesan data pribadi .

Teori efektivitas hukum, tata kelola data (data governance), dan kepercayaan digital menjadi landasan teoritis dalam menganalisis hubungan antara regulasi, pelaku e-commerce, dan pengguna. Ketiga teori ini saling melengkapi dalam menilai efektivitas Undang-Undang Perlindungan Data Pribadi Tahun 2022 dari sisi struktur, perilaku organisasi, dan persepsi sosial .

Melalui teori efektivitas hukum, peneliti dapat menilai apakah Undang-Undang Perlindungan Data Pribadi Tahun 2022 telah memenuhi fungsi-fungsi regulatifnya: mengubah perilaku, menciptakan kepatuhan, dan menyelesaikan konflik. Sementara tata kelola data digunakan untuk menelaah sejauh mana perusahaan mengelola data secara akuntabel dan terstandar.

Teori kepercayaan digital diperlukan untuk mengukur sejauh mana Undang-Undang Perlindungan Data Pribadi Tahun 2022 mampu mengembalikan atau meningkatkan kepercayaan publik terhadap ekosistem digital. Karena pada dasarnya, perlindungan data bukan hanya isu legal-formal, tetapi juga psikologis dan relasional.

Penelitian ini diharapkan memberi manfaat bagi pengembangan ilmu hukum dan sosiologi digital, serta memberi rekomendasi praktis kepada pemerintah dan pelaku industri dalam membangun sistem perlindungan data yang lebih efektif, adaptif, dan berorientasi pada kepentingan publik.

Oleh karena itu, penelitian ini bertujuan untuk mengevaluasi tinjauan yuridis undang-undang perlindungan data pribadi tahun 2022 dengan menelusuri persepsi pengguna e-commerce, pemangku kepentingan, dan profesional hukum. Penelitian ini diharapkan dapat memberikan wawasan baru terhadap bagaimana kebijakan ini diimplementasikan secara aktual dan bagaimana ia dirasakan di level masyarakat, bukan sekadar di atas kertas hukum. Temuan dari studi ini akan memberikan kontribusi penting dalam menyempurnakan kebijakan perlindungan data pribadi, serta mendukung advokasi regulasi yang lebih berpihak pada kepentingan publik di era digital.

Untuk menjawab persoalan tersebut, maka penulis membuat rumusan masalah sebagai berikut:

1. Bagaimana perusahaan e-commerce di Indonesia mengimplementasikan kewajiban perlindungan data pribadi sesuai dengan Undang-Undang Perlindungan Data Pribadi Tahun 2022?
2. Bagaimana kebocoran data pribadi mempengaruhi persepsi konsumen terhadap perusahaan e-commerce di Indonesia?

## **2. KAJIAN TEORITIS**

### **Perlindungan data pribadi**

Teori perlindungan data pribadi merupakan landasan konseptual yang sangat relevan dan esensial dalam menelaah efektivitas suatu regulasi seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Teori ini secara umum menekankan pentingnya hak individu atas kendali terhadap informasi pribadinya, serta tanggung jawab penyedia layanan (dalam hal ini e-commerce) untuk menjaga dan mengelola data pribadi pengguna secara transparan, adil, dan aman .

Dalam konteks e-commerce, data pribadi pelanggan menjadi aset utama sekaligus titik rentan bagi kebocoran informasi yang berpotensi dimanfaatkan untuk kejahatan siber. Teori perlindungan data pribadi tidak hanya membahas aspek hukum formal, tetapi juga mengandung prinsip moral dan sosial bahwa setiap individu berhak atas privasi dan kontrol informasi tentang dirinya. Hal ini selaras dengan pasal-pasal dalam Undang-Undang Perlindungan Data Pribadi (PDP) Tahun 2022 yang menegaskan hak subjek data dan kewajiban pengendali data.

Undang-Undang Perlindungan Data Pribadi (PDP) Tahun 2022 mengadopsi prinsip-prinsip dasar perlindungan data yang berasal dari teori ini, seperti prinsip *lawfulness*, *fairness*, and *transparency*, *purpose limitation*, dan *accountability*, yang banyak digunakan dalam kerangka hukum perlindungan data global seperti GDPR (*General Data Protection Regulation*).

Teori ini menekankan bahwa suatu regulasi akan efektif jika hak-hak individu dijamin dan dilengkapi dengan mekanisme pengawasan serta sanksi yang jelas terhadap pelanggaran .

Dalam skripsi ini, teori perlindungan data pribadi digunakan sebagai pisau analisis untuk mengkaji apakah Undang-Undang Perlindungan Data Pribadi (PDP) Tahun 2022 mampu melindungi konsumen e-commerce dari insiden kebocoran data. Hal ini tidak hanya dilihat dari aspek normatif (aturan tertulis), tetapi juga dari implementasi nyata di lapangan seperti tanggung jawab pelaku usaha digital, kesadaran hukum masyarakat, dan efektivitas pengawasan oleh negara.

Dengan menggunakan pendekatan kualitatif, teori ini menjadi panduan untuk menggali persepsi pengguna, pelaku industri e-commerce, dan pakar hukum tentang perlindungan data pribadi. Penggunaan teori ini juga memungkinkan peneliti untuk menilai sejauh mana norma hukum Undang-Undang Perlindungan Data Pribadi (PDP) Tahun 2022 sesuai dengan kebutuhan aktual masyarakat digital di Indonesia yang rentan terhadap pelanggaran privasi data.

Secara keseluruhan, teori perlindungan data pribadi menjadi kerangka epistemologis yang menghubungkan antara hak hukum warga negara, kebijakan negara melalui Undang-Undang Perlindungan Data Pribadi (PDP) Tahun 2022, dan realitas sosial pengguna teknologi. Oleh karena itu, teori ini sangat penting dalam membedah pertanyaan inti dalam skripsi ini, yakni “apakah Undang-Undang Perlindungan Data Pribadi (PDP) Tahun 2022 benar-benar efektif dalam memberikan perlindungan terhadap kebocoran data pelanggan e-commerce?”

### **Efektivitas regulasi**

Menurut Baldwin dan Cave, efektivitas regulasi bergantung pada kemampuan regulasi mencapai tujuan-tujuan kebijakan yang telah ditentukan, baik secara langsung maupun tidak langsung. Efektivitas tidak hanya dilihat dari keberadaan regulasi, tetapi juga dari sejauh mana regulasi tersebut dapat diterapkan dan menghasilkan perubahan perilaku yang diinginkan dalam masyarakat atau sektor yang dituju.

Indra Perwira menjelaskan bahwa regulasi yang efektif di Indonesia harus memenuhi tiga syarat utama, yaitu:

- a. Kesesuaian norma hukum dengan kebutuhan masyarakat,
- b. Kepastian hukum yang ditegakkan secara konsisten, dan
- c. Adanya pengawasan dan sanksi yang operasional.

Tanpa ketiga syarat ini, regulasi hanya menjadi teks hukum tanpa makna praktis. Efektivitas hukum bergantung pada sejauh mana norma-norma tersebut dipatuhi dan mampu memengaruhi perilaku masyarakat secara nyata.

Teori efektivitas regulasi menjadi dasar teoretis penting dalam menilai sejauh mana suatu produk hukum, seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, dapat diterapkan secara optimal untuk mencapai tujuan yang diharapkan, yakni melindungi data pribadi masyarakat. Dalam konteks skripsi ini, teori tersebut membantu menjawab pertanyaan kunci: Apakah Undang-Undang Perlindungan Data Pribadi (PDP) Tahun 2022 benar-benar mampu mencegah dan menangani kebocoran data pelanggan pada *platform e-commerce* di Indonesia?

Efektivitas hukum dipengaruhi oleh beberapa faktor: substansi hukum, aparat penegak hukum, masyarakat, sarana/prasarana pendukung, dan budaya hukum. Penerapan teori ini dalam penelitian akan menyoroti tidak hanya isi Undang-Undang Perlindungan Data Pribadi Tahun 2022, tetapi juga bagaimana lembaga penegak hukum, pelaku industri digital, dan pengguna memaknai serta menerapkannya dalam praktik transaksi daring.

Regulasi akan dinilai efektif jika ia:

- a. Mampu mengubah perilaku sosial (misalnya meningkatkan kepatuhan pelaku *e-commerce* terhadap prinsip privasi),
- b. Menyediakan mekanisme sanksi dan perlindungan yang jelas terhadap korban kebocoran data,
- c. Dapat dilaksanakan secara teknis dan institusional, serta
- d. Dipahami dan dianggap adil oleh masyarakat yang menjadi subjek hukum.

Undang-Undang Perlindungan Data Pribadi (PDP) Tahun 2022 memang telah mengatur hak-hak subjek data dan kewajiban pengendali data, termasuk ketentuan sanksi administratif dan pidana. Namun efektivitas regulasi ini sangat bergantung pada sejauh mana instrumen tersebut dapat bekerja dalam konteks *e-commerce* yang kompleks dan terus berkembang, terutama ketika insiden kebocoran data masih marak terjadi meskipun regulasi sudah disahkan.

Oleh karena itu, teori efektivitas regulasi menjadi sangat relevan untuk menilai tidak hanya keberadaan undang-undang, tetapi juga implementasinya di dunia nyata. Pendekatan ini membantu peneliti mengukur kesenjangan antara norma hukum dengan praktik pelaksanaannya di masyarakat digital Indonesia.

Dengan pendekatan kualitatif, teori ini menjadi kerangka kerja untuk mengeksplorasi bagaimana Undang-Undang Perlindungan Data Pribadi (PDP) Tahun 2022 dipahami dan

diimplementasikan oleh aktor-aktor terkait, serta apa saja hambatan dan peluang yang muncul dalam penerapannya untuk menanggulangi kebocoran data pelanggan *e-commerce*. Hasilnya diharapkan dapat memberikan kontribusi pada penguatan regulasi yang lebih responsif dan efektif dalam menghadapi dinamika ancaman digital di Indonesia.

### **Tata kelola data (data governance theory)**

Teori tata kelola data atau data governance theory merupakan kerangka konseptual yang berfokus pada bagaimana data dikelola, dilindungi, diakses, dan dimanfaatkan secara akuntabel dalam suatu organisasi atau sistem digital. Dalam konteks *e-commerce*, teori ini menjadi sangat penting karena data pelanggan merupakan aset utama yang harus dikelola secara aman, transparan, dan sesuai hukum. Oleh karena itu, teori tata kelola data sangat relevan dengan analisis efektivitas Undang-Undang Perlindungan Data Pribadi Tahun 2022, khususnya dalam menangani isu kebocoran data pelanggan.

Prinsip dasar dari data governance mencakup tanggung jawab yang jelas terhadap kepemilikan data, kontrol akses, integritas data, dan keamanan data elemen-elemen yang menjadi fokus utama dari Undang-Undang Perlindungan Data Pribadi (PDP) Tahun 2022. Undang-Undang tersebut mengatur hak-hak subjek data serta kewajiban pengendali data, seperti *e-commerce*, untuk menjaga keamanan, melakukan audit internal, dan melaporkan insiden kebocoran kepada otoritas berwenang dalam jangka waktu tertentu . Jika sebuah platform *e-commerce* gagal membangun sistem tata kelola data yang baik, maka meskipun ada regulasi, risiko kebocoran data akan tetap tinggi.

Penelitian yang dilakukan oleh Badrawani et al. (2024) menunjukkan bahwa efektivitas regulasi seperti Undang-Undang Perlindungan Data Pribadi (PDP) Tahun 2022 sangat bergantung pada bagaimana data governance diterapkan di institusi terkait . Di Indonesia, lemahnya sistem audit data internal dan rendahnya kepatuhan terhadap kebijakan privasi menjadi penyebab utama banyaknya kasus kebocoran data, seperti yang menimpa Tokopedia dan Bukalapak. Dengan kata lain, teori tata kelola data berperan sebagai penghubung antara regulasi hukum dan praktik manajemen data di lapangan.

Selain itu, data governance juga mencakup aspek strategis seperti data stewardship, data quality, dan data protection lifecycle, yang semuanya diakomodasi dalam Undang-Undang Perlindungan Data Pribadi (PDP) Tahun 2022 sebagai syarat akuntabilitas bagi pengendali data. Oleh karena itu, menilai efektivitas Undang-Undang Perlindungan Data Pribadi (PDP) Tahun 2022 tanpa memperhitungkan aspek tata kelola data akan memberikan hasil yang kurang menyeluruh.

Melalui pendekatan kualitatif, teori ini memberikan fondasi bagi peneliti untuk mengeksplorasi praktik nyata tata kelola data di platform e-commerce, mengamati seberapa jauh perusahaan benar-benar menerapkan prinsip-prinsip tersebut dalam sistem digital mereka, dan bagaimana Undang-Undang Perlindungan Data Pribadi (PDP) Tahun 2022 mempengaruhi perubahan perilaku pengelolaan data. Penelitian ini akan mengungkap apakah keberadaan Undang-Undang Perlindungan Data Pribadi (PDP) Tahun 2022 diiringi oleh perbaikan sistem manajemen data, atau hanya sebatas kepatuhan formal tanpa substansi .

Dengan demikian, teori tata kelola data bukan hanya relevan, tetapi sangat krusial dalam membedah hubungan antara instrumen hukum Undang-Undang Perlindungan Data Pribadi (PDP) Tahun 2022, pelaku e-commerce, dan perlindungan nyata terhadap hak-hak konsumen digital. Penelitian skripsi ini akan menggunakan teori ini untuk menilai integrasi antara norma hukum dan praktik tata kelola data dalam menanggulangi kebocoran data pelanggan e-commerce di Indonesia.

### **Kepercayaan digital (digital trust theory)**

Teori kepercayaan digital (*digital trust theory*) merupakan pendekatan konseptual yang menyoroti sejauh mana pengguna sistem digital mempercayai bahwa teknologi, *platform*, dan institusi penyedia layanan digital akan menjaga keamanan, integritas, dan privasi data mereka. Dalam konteks *e-commerce*, kepercayaan digital adalah prasyarat mutlak bagi kelangsungan hubungan antara konsumen dan penyedia layanan. Oleh karena itu, teori ini sangat relevan dengan penelitian tentang efektivitas Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, karena salah satu tujuan utama dari undang-undang tersebut adalah untuk membangun dan memperkuat kepercayaan publik dalam ekosistem digital Indonesia.

Sebagaimana dijelaskan oleh Wibowo et al. (2025) kehadiran Undang-Undang Perlindungan Data Pribadi (PDP) Tahun 2022 menjadi instrumen negara dalam membentuk tata kelola data yang transparan dan akuntabel, sehingga mampu mendorong terbentuknya kepercayaan publik terhadap sistem digital. Tanpa kepercayaan, konsumen akan cenderung enggan memberikan data pribadinya secara daring, yang pada akhirnya menghambat pertumbuhan ekonomi digital. Dalam konteks ini, Undang-Undang Perlindungan Data Pribadi (PDP) Tahun 2022 tidak hanya berfungsi sebagai alat hukum, tetapi juga sebagai fondasi normatif untuk mengelola relasi kepercayaan dalam lingkungan digital.

Teori ini juga berkaitan erat dengan fenomena kebocoran data yang sering kali merusak kepercayaan konsumen terhadap *platform e-commerce*. Ketika konsumen merasa datanya tidak aman, mereka kehilangan rasa percaya, dan ini dapat berakibat pada penurunan penggunaan

platform digital, bahkan berpindah ke layanan yang dianggap lebih aman. Oleh karena itu, efektivitas Undang-Undang Perlindungan Data Pribadi (PDP) Tahun 2022 dapat dinilai dari kemampuannya membangun kembali kepercayaan digital yang sempat rusak akibat berbagai insiden kebocoran data.

Budhijanto (2024) menambahkan bahwa kepercayaan digital merupakan hasil dari proses yang berkelanjutan, di mana kebijakan perlindungan data memainkan peran penting dalam membentuk persepsi risiko pengguna. Jika Undang-Undang Perlindungan Data Pribadi (PDP) Tahun 2022 berhasil diterapkan secara konsisten termasuk adanya transparansi pelaporan kebocoran data, sanksi tegas, dan hak akses serta koreksi bagi pemilik data maka kepercayaan digital masyarakat terhadap *e-commerce* akan meningkat.

Dalam penelitian ini, teori kepercayaan digital dijadikan sebagai alat untuk menganalisis dimensi sosial dari penerapan Undang-Undang Perlindungan Data Pribadi (PDP) Tahun 2022. Melalui pendekatan kualitatif, peneliti dapat mengeksplorasi bagaimana pengalaman, pengetahuan, dan persepsi masyarakat terhadap perlindungan data mempengaruhi tingkat kepercayaannya pada *platform e-commerce*. Pendekatan ini juga memungkinkan untuk menelusuri dampak konkret dari pelaksanaan **Undang-Undang Perlindungan Data Pribadi (PDP) Tahun 2022** terhadap pemulihan dan pembentukan kepercayaan baru di tengah masyarakat digital Indonesia.

Dengan demikian, teori kepercayaan digital memberikan perspektif yang melengkapi pendekatan hukum dan tata kelola data dengan dimensi sosiologis, sehingga memberikan pemahaman menyeluruh terhadap efektivitas regulasi dalam praktik. Kepercayaan digital bukan hanya konsekuensi dari perlindungan hukum, tetapi juga indikator keberhasilan implementasi regulasi seperti Undang-Undang Perlindungan Data Pribadi Tahun 2022 dalam menciptakan ekosistem digital yang aman dan terpercaya.

### 3. METODE PENELITIAN

Jenis penelitian yang digunakan dalam skripsi ini adalah penelitian hukum yuridis empiris. Penelitian yuridis empiris merupakan penelitian hukum yang bertujuan untuk memahami hukum dalam kenyataan sosial, yakni bagaimana hukum bekerja dan diimplementasikan di tengah masyarakat. Dalam hal ini, hukum tidak hanya dilihat sebagai norma tertulis (*law in books*), tetapi juga sebagai perilaku nyata para subjek hukum (*law in action*).

Pendekatan ini dipilih untuk mengkaji secara mendalam efektivitas Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dalam menangani

kebocoran data pribadi pada platform e-commerce, berdasarkan pengalaman, persepsi, dan tanggapan para pengguna yang terdampak. Penelitian ini tidak semata menelaah isi normatif undang-undang, tetapi juga menelusuri bagaimana norma tersebut diimplementasikan, dipahami, dan dirasakan oleh individu sebagai subjek data.

#### **4. HASIL DAN PEMBAHASAN**

##### **Implementasi Perusahaan E-Commerce Dalam Memberikan Kewajiban Perlindungan Data Pribadi Sesuai Dengan Undang-Undang Perlindungan Data Pribadi Tahun 2022.**

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan tonggak penting dalam sistem hukum Indonesia yang mengatur pengelolaan data pribadi secara menyeluruh dan sistematis. UU ini memberikan kewajiban kepada pengendali data pribadi, termasuk platform e-commerce, untuk menjamin perlindungan data pribadi konsumen melalui berbagai prinsip seperti keabsahan pengumpulan data, transparansi, pembatasan tujuan, keamanan, dan tanggung jawab hukum.

Berdasarkan Pasal 20 sampai dengan Pasal 30 UU PDP, kewajiban utama pengendali data pribadi (termasuk perusahaan e-commerce) antara lain:

- a. Memastikan adanya dasar hukum yang sah dalam pemrosesan data (misalnya melalui persetujuan eksplisit),
- b. Memberikan informasi yang jelas kepada subjek data mengenai tujuan dan metode pengumpulan data,
- c. Menyediakan akses, koreksi, dan penghapusan data atas permintaan pengguna,
- d. Melindungi data pribadi melalui sistem keamanan yang memadai, dan
- e. Melaporkan kebocoran data kepada subjek data dan otoritas pengawas maksimal 72 jam setelah insiden terjadi (Pasal 46).
- f. Tokopedia dan Shopee, meskipun memiliki kebijakan privasi yang diperbarui, masih belum memberikan mekanisme yang mudah bagi pengguna untuk mengajukan akses atau penghapusan data. Fitur "hapus akun" tidak disertai jaminan bahwa data pribadi dihapus permanen dari server.
- g. Bukalapak dan Lazada belum secara eksplisit menyatakan kebijakan internal mengenai pelaporan insiden kebocoran data. Beberapa responden mengaku tidak menerima notifikasi apa pun meskipun indikasi penyalahgunaan data muncul (misalnya menerima pesan spam dengan nama lengkap dan alamat rumah).

- h. Bibli relatif lebih transparan dalam menjelaskan penggunaan data untuk keperluan personalisasi dan marketing, namun tidak menjelaskan secara rinci kebijakan penyimpanan dan retensi data.

Penelitian ini menemukan bahwa implementasi regulasi tersebut oleh platform e-commerce masih bervariasi dan belum sepenuhnya memenuhi amanat UU PDP: Dari hasil diatas,ditemukan hasil wawancara door to door peneliti dengan responden yaitu:

### **Kasus Kebocoran Data Tokopedia**

Tokopedia mengalami kebocoran data besar pada Mei 2020, di mana lebih dari 91 juta akun pengguna terdampak. Data yang bocor meliputi nama lengkap, alamat email, tanggal lahir, hingga hashed password.

Dalam wawancara door to door saya dengan dibantu alat google formulir,mengenai pengguna tokopedia,saya mempertanyakan tentang pengalaman dan persepsi pengguna tokopedia saat adanya kasus kebocoran data di tokopedia. Dari pertanyaan wawancara yang saya tanyakan dari saudara Tyas Perdana Kusuma (Pengguna Tokopedia dari tahun 2018), saya mendapatkan jawaban berupa:

“Saya masih ingat betul waktu kasus itu muncul. Saya merasa tidak dilindungi sama sekali, karena Tokopedia tidak pernah kasih notifikasi resmi ke email saya. Saya tahunya dari berita dan grup WA.”

Dari jawaban responden diatas saya mendapatkan analisis berupa, dalam UU PDP Pasal 46 ayat (2), pengendali data wajib memberitahu subjek data maksimal 72 jam setelah insiden terjadi. Dalam praktiknya, notifikasi tersebut tidak dilakukan secara langsung kepada pengguna, melainkan hanya melalui klarifikasi media.

### **Kasus Dugaan Kebocoran Data Shopee**

Pada pertengahan 2022, muncul laporan pengguna yang menerima pesan WhatsApp pribadi dari penjual Shopee dengan informasi pribadi yang akurat, seperti nama lengkap dan lokasi.

Salah satu responden aktif di Shoppe menyatakan, “Sampai sekarang, belum pernah ada email pemberitahuan soal kebijakan perlindungan data atau perubahan kebijakan privasi dari Shopee. Padahal saya pengguna aktif.”(Maya,Ibu rumah tangga,alamat Jl.Jatimulyo Tr1/699 Rt.24,Rw05, pengguna Shopee akti dan Tokopedia)

Dari jawaban respnden diatas saya menganalisis bahwa Shopee dalam kebijakannya tidak menyebutkan secara eksplisit mekanisme pelaporan kebocoran data atau hak pengguna

jika data disalahgunakan. Hal ini bertentangan dengan prinsip data minimization dan transparansi pemrosesan data dalam Undang-Undang Perlindungan Data Pribadi Pasal 15 dan 16.

### **Kasus Bukalapak**

Dalam pertanyaan wawancara saya dengan bantuan google form,ada salah satu dari 10 pertanyaan yang isinya:”Apakah responden pernah membuat akun e-commerce lalu di nonaktifkan lagi?”

Dari pertanyaan diatas saya mendapatkan salah satu jawaban yang mengarah ke permasalahan ini.

“Saya masih bisa login walau sudah lama tidak pakai. Tapi tidak tahu apakah data saya masih tersimpan. Tidak ada pilihan untuk benar-benar menghapus akun atau data pribadi.”(Rido Eko Susilo,Driver Grab, pemilik akun Bukalapak sudah ama,namun menginstall lagi (pasif)).

Dari jawaban responden diatas saya menganalisis bahwa Walau terjadi sebelum UU PDP disahkan, kebocoran data 13 juta akun Bukalapak menjadi cikal bakal dorongan perumusan UU PDP. Namun, hasil wawancara menyebut bahwa hingga kini tidak ada mekanisme jelas yang disediakan oleh Bukalapak untuk mengakses atau menghapus data secara permanen.

Dari kasus-kasus tersebut, terlihat bahwa mayoritas platform belum sepenuhnya memenuhi kewajiban hukum sebagaimana diatur dalam UU PDP. Beberapa pelanggaran implementatif yang teridentifikasi antara lain:

- a. Tidak ada notifikasi kebocoran data ke subjek data;
- b. Tidak tersedia akses atau koreksi data pribadi secara mandiri;
- c. Ketidakjelasan mekanisme pelaporan pelanggaran atau permintaan perlindungan;
- d. Minimnya edukasi atau pemberitahuan proaktif terkait perubahan kebijakan privasi.

Hasil wawancara menunjukkan bahwa UU PDP belum menyentuh level kesadaran individu secara merata, dan perusahaan e-commerce belum merombak kebijakan internalnya secara menyeluruh. Ketidaktahuan masyarakat terhadap hak hukum mereka sebagai subjek data mengindikasikan bahwa perlindungan data belum menjadi budaya digital yang mapan di Indonesia.

### **Kebocoran Data Pribadi Mempengaruhi Persepsi Konsumen Terhadap Perusahaan E-Commerce Di Indonesia**

Hasil analisis data menunjukkan bahwa persepsi konsumen terhadap perusahaan e-commerce sangat dipengaruhi oleh bagaimana perusahaan merespons kebocoran Hasil analisis data menunjukkan bahwa persepsi konsumen terhadap perusahaan e-commerce sangat dipengaruhi oleh bagaimana perusahaan merespons kebocoran data, serta sejauh mana perlindungan hukum, khususnya melalui Undang-Undang Perlindungan Data Pribadi Tahun 2022, diterapkan secara efektif.

Temuan ini disusun berdasarkan data survei kualitatif perwakilan konsumen(pengguna e-commerce).

### **Penanganan Insiden Sebagai Faktor Dominan**

Sebanyak 42% responden dari salah satu dari sepuluh pertanyaan, menyatakan bahwa respons perusahaan terhadap insiden kebocoran data menjadi faktor paling dominan dalam membentuk persepsi mereka. Konsumen mengharapkan adanya tindakan cepat, transparan, dan akuntabel dari perusahaan saat insiden terjadi, termasuk:

- a) Memberikan notifikasi resmi kepada pengguna terdampak.
- b) Menjelaskan penyebab kebocoran.
- c) Menyediakan kompensasi atau langkah pemulihan yang konkret.
- d) Menyampaikan tindakan preventif ke depan.

Temuan ini mendukung teori Situational Crisis Communication Theory (Coombs, 2007), yang menyatakan bahwa strategi komunikasi krisis yang tepat dapat memitigasi kerusakan reputasi organisasi dan memulihkan kepercayaan publik. Dalam konteks e-commerce, penanganan insiden yang profesional menjadi indikator utama penilaian konsumen, bahkan melebihi faktor reputasi historis perusahaan.

### **Komunikasi Transparan dan Kepercayaan Konsumen**

Sebanyak 28% responden menyebutkan komunikasi yang jujur dan terbuka sebagai alasan utama tetap mempercayai suatu platform meski 98% responden belum pernah mengalami insiden keamanan data. Responden menekankan bahwa keterbukaan informasi lebih dihargai dibanding sekadar janji keamanan tanpa transparansi. Komunikasi yang bersifat manipulatif atau menutupi insiden cenderung memperburuk persepsi, sebagaimana dikonfirmasi dalam studi oleh Kim et al. (2021), yang menekankan pentingnya perceived sincerity dalam manajemen krisis digital.

### **Reputasi Sebelumnya Tidak Cukup Melindungi Persepsi**

Dalam pertanyaan mengenai kasus yang pernah terjadi di Indonesia, menariknya reputasi perusahaan hanya memiliki pengaruh sebesar 18% terhadap persepsi konsumen pasca kebocoran. Hal ini menunjukkan bahwa meskipun sebuah perusahaan memiliki citra positif sebelum insiden, persepsi publik dapat berubah drastis apabila respons terhadap krisis dianggap tidak memadai. Dalam wawancara, beberapa konsumen menyebutkan bahwa mereka menghentikan penggunaan platform meskipun telah menjadi pengguna setia selama bertahun-tahun.

### **Efektivitas Terbatas Undang-Undang Perlindungan Data Pribadi Tahun 2022 dalam Praktik**

Hanya 60% responden yang menyebut Undang-Undang Perlindungan Data Pribadi Tahun 2022 sebagai faktor yang meningkatkan kepercayaan, presentase ini menurut saya masih jauh dari kata sempurna, yang menunjukkan bahwa efektivitas regulasi ini masih lebih bersifat normatif ketimbang substantif di mata publik. Minimnya pengetahuan masyarakat terhadap isi, fungsi, dan mekanisme pengaduan dalam Undang-Undang Perlindungan Data Pribadi Tahun 2022 menimbulkan kesenjangan antara eksistensi hukum dan pelaksanaan teknisnya. Hal ini sesuai dengan kritik dari Prasetyo et al. (2023), yang menilai bahwa keberhasilan regulasi bergantung pada edukasi publik dan keberanian penegakan oleh otoritas.

## **5. KESIMPULAN DAN SARAN**

Kesimpulan dari rumusan masalah pertama yaitu “Bagaimana perusahaan e-commerce di Indonesia mengimplementasikan kewajiban perlindungan data pribadi sesuai dengan Undang-Undang Perlindungan Data Pribadi Tahun 2022?”, dapat disimpulkan bahwa sebagian besar perusahaan telah mulai menyesuaikan kebijakan internalnya dengan ketentuan dalam UU PDP 2022, seperti dengan menyusun kebijakan privasi, membentuk unit perlindungan data, serta menetapkan pejabat perlindungan data (Data Protection Officer). Namun, belum seluruh perusahaan memiliki sistem manajemen keamanan data yang memadai atau menjalankan prinsip-prinsip perlindungan data secara menyeluruh, seperti transparansi, pembatasan tujuan, serta akuntabilitas. Hambatan implementasi antara lain terkait kurangnya kesiapan infrastruktur digital, minimnya literasi perlindungan data di kalangan pelaku usaha, serta pengawasan dari otoritas yang belum sepenuhnya efektif. Kesimpulan dari rumusan masalah kedua yaitu “Bagaimana kebocoran data pribadi mempengaruhi persepsi konsumen terhadap perusahaan e-commerce di Indonesia?” dapat disimpulkan bahwa kebocoran data pribadi memiliki dampak signifikan terhadap persepsi dan kepercayaan konsumen terhadap

perusahaan e-commerce. Berdasarkan hasil wawancara dan studi literatur, banyak konsumen merasa cemas, kecewa, dan kehilangan kepercayaan terhadap platform e-commerce yang pernah mengalami insiden kebocoran data. Kepercayaan digital merupakan elemen krusial dalam ekosistem ekonomi digital, dan kebocoran data terbukti mengganggu loyalitas konsumen serta berdampak negatif terhadap citra merek dan keberlanjutan bisnis. Konsumen semakin menuntut transparansi, tanggung jawab, dan keamanan yang lebih tinggi atas pengelolaan data pribadi mereka. Dengan demikian, perlindungan data bukan hanya kewajiban hukum, melainkan juga menjadi bagian dari strategi bisnis dan reputasi perusahaan.

Berdasarkan hasil penelitian dan kesimpulan yang telah diperoleh, penulis memberikan beberapa saran sebagai berikut:

1. Bagi Perusahaan E-Commerce:

Berdasarkan hasil penelitian dan kesimpulan yang telah diperoleh, penulis memberikan beberapa saran sebagai berikut:

2. Bagi Perusahaan E-Commerce:

- a) Perusahaan e-commerce di Indonesia perlu lebih proaktif dalam mengimplementasikan seluruh ketentuan yang diatur dalam UU Perlindungan Data Pribadi Tahun 2022, termasuk prinsip-prinsip dasar perlindungan data pribadi seperti persetujuan yang sah, transparansi, akuntabilitas, dan pembatasan tujuan.
- b) Diperlukan peningkatan investasi dalam sistem keamanan siber dan pengembangan infrastruktur digital yang mampu mendeteksi serta mencegah potensi kebocoran data sejak dini.
- c) Perusahaan juga disarankan untuk melakukan pelatihan internal secara berkala terkait literasi perlindungan data pribadi kepada seluruh staf yang terlibat dalam pengelolaan data pelanggan.

3. Bagi Pemerintah dan Otoritas Pengawas:

- a) Pemerintah melalui otoritas yang ditunjuk (otoritas PDP) perlu segera membentuk lembaga pengawas perlindungan data yang independen, efektif, dan memiliki kewenangan yang memadai untuk melakukan audit, investigasi, serta penegakan hukum terhadap pelanggaran data pribadi.
- b) Perlu adanya sosialisasi yang lebih masif terkait UU PDP kepada seluruh pelaku usaha digital, termasuk UMKM berbasis digital, agar tidak terjadi pelanggaran karena ketidaktahuan.

- c) Penguatan regulasi turunan seperti Peraturan Pemerintah (PP) dan Peraturan Menteri juga mendesak untuk memberikan panduan teknis lebih rinci bagi pelaku usaha dalam menjalankan kewajibannya.

4. Bagi Konsumen:

- a) Konsumen perlu meningkatkan kesadaran dan literasi digital terkait hak-hak mereka atas data pribadi, termasuk hak untuk mengetahui, mengakses, memperbaiki, dan menghapus data yang dikelola oleh perusahaan e-commerce.
- b) Diperlukan kehati-hatian dalam membagikan data pribadi secara daring, serta mendorong masyarakat untuk melaporkan dugaan pelanggaran perlindungan data ke otoritas terkait.

5. Bagi Peneliti Selanjutnya:

Penelitian ini masih memiliki keterbatasan pada cakupan kasus dan ruang lingkup implementasi regulasi. Oleh karena itu, disarankan bagi peneliti selanjutnya untuk mengkaji efektivitas lembaga pengawas perlindungan data setelah resmi terbentuk, atau mengeksplorasi persepsi konsumen secara kuantitatif melalui survei yang lebih luas guna memperkaya perspektif empiris

## DAFTAR REFERENSI

- Abdul, Halim Barkatullah, & Prasetyo, T. (2005). *Bisnis E-Commerce*. Yogyakarta: Pustaka Pelajar.
- Badrawani, W., Wardhono, R. D. T. K., & Deviana, A. (2024). Pelindungan data pribadi di Bank Indonesia dan lembaga jasa keuangan: Rekomendasi kebijakan dan teknis pengaturan. *Bank Indonesia Working Paper*.
- Baldwin, R., & Cave, M. (2011). *Understanding regulation: Theory, strategy, and practice* (2nd ed.). Oxford University Press.
- Cholid Narbuko, & Achmadi, A. (2010). *Metode Penelitian*.
- Fahri, S. M. Al. (2023). Kebijakan privasi terhadap data pribadi pengguna e-commerce ditinjau dari UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi.
- Gulton, E. (n.d.). *Cyber Law: Suatu pengantar perlindungan konsumen dalam transaksi perdagangan melalui electronic commerce*. Bandung: Elips.

- Halim, E. F. (2022). Perlindungan hukum data pribadi pembeli di perdagangan secara elektronik (e-commerce) di Indonesia. *Jurnal Hukum Visio Justisia*.
- Indriani, M., & Putri, A. A. (2023). The dynamic consent for optimizing personal data protection and the right to privacy. *CORE.ac.uk*.
- Isnaeni, M. (2018). *Seberkas diaroma hukum kontrak*. Surabaya: PT Revka Petra Media.
- Kansil, C. S. T. (1989). *Pengantar ilmu hukum dan tata hukum Indonesia*. Jakarta: Balai Pustaka.
- Kusuma, P. R. A., & Adistiya, K. N. (2024). Kebocoran data pribadi berdasarkan Pasal 16 Ayat 2 Huruf E UU No. 27 Tahun 2022. *Jurnal Ilmu Hukum*.
- Lase, S. P. O. (2025). Urgensi pembentukan lembaga pengawas dalam pembaharuan hukum perlindungan data pribadi. *Locus Journal of Academic Literature Review*.
- Marischa, D., & Setianingrum, R. B. (2024). Transfer of personal data by e-commerce companies: A study from the perspective of Indonesian personal data protection laws. *Jurnal Mahasiswa Hukum Indonesia*.
- Muchsin. (2003). *Perlindungan dan kepastian hukum bagi investor di Indonesia*. Surakarta: Magister Ilmu Hukum Program Pascasarjana Universitas Sebelas Maret.
- Perwira, I. (2006). *Efektivitas hukum dalam perspektif hukum dan masyarakat*. Jakarta: Ghalia Indonesia.
- Pontorondo, I., Walangitan, M. A., & Kapojos, R. L. (2025). Perlindungan hukum terhadap data privasi konsumen e-commerce yang menjadi korban kejahatan siber. *Citizen Journal*, 1, 8.
- Saputra, A. F. R., Shafwa, A. J., & Umam, R. (2025). Analisis efektivitas penerapan Undang-Undang Perlindungan Konsumen (UUPK) dalam transaksi e-commerce di Indonesia. *Media Riset Bisnis dan Ekonomi*.
- Saqinah, D. A. (2025). Implikasi hukum penggunaan artificial intelligence (AI) dalam transaksi e-commerce di Indonesia. *Jurnal Ilmiah Universitas Mataram*.
- Shidarta. (2006). *Hukum perlindungan konsumen Indonesia* (Cetakan ke-3). Jakarta: PT Grasindo.
- Simanjuntak, M., & Muflikhati, I. (2023). Willingness to share data pribadi dan kaitannya dengan penyalahgunaan data konsumen e-commerce di Indonesia. *Jurnal Ilmu Keluarga dan Konsumen*.
- Soekanto, S. (2021). *Faktor-faktor yang mempengaruhi penegakan hukum*. Jakarta: Rajawali Pers.
- Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

- Wijaya, G. (2020). Pelindungan data pribadi di Indonesia: *Ius constitutum dan ius constituendum*. *Law Review, Universitas Pelita Harapan*.
- Wiraguna, S. A., & Wulandari, D. (2025). Perlindungan hukum bagi pengguna aplikasi Tokopedia dari kebocoran data pribadi. *Jurnal Kajian Hukum dan Kebijakan Publik*.