Indonesian Journal of Law

Vol. 2, No. 1, Januari 2025
Hal 12-22

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

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

Perlindungan Hukum Terhadap Data Diri Konsumen Dalam Transaksi Digital

Naufal Akbar[1], Handro Kurnia Sitorus[2], Muhammad Yasir Arifin Putra Nasution[3]
[1,2,3] Fakultas Syari'ah dan Hukum, Universitas Islam Negeri Sumatera Utara, Medan, Indonesia

Article Info

Article history:

Received Januari 7, 2025
Revised Januari 7, 2025
Accepted Januari 11, 2025

Kata Kunci:

Perlindungan Data,
Teransaksi Digital,
Konsumen,
Hukum,
Keamanan Data

Keywords:

Data Protection,
Digital Transactions,
Consumers,
Law,
Data Security

ABSTRAK

Penelitian ini menganalisis regulasi yang berlaku, khususnya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Perlindungan Data Pribadi (UU PDP). UU ITE menjadi landasan awal dalam mengatur transaksi elektronik dan melarang akses ilegal terhadap data pribadi, sedangkan UU PDP memperkuat aturan terkait persetujuan pengguna dan pemberian sanksi tegas bagi pelanggaran. Meski kedua regulasi tersebut telah diberlakukan, pelaksanaannya di lapangan masih menghadapi berbagai kendala, seperti lemahnya penegakan hukum, kurangnya kesadaran pelaku usaha, dan minimnya literasi digital di kalangan masyarakat. Hasil penelitian ini menegaskan bahwa perlindungan data pribadi membutuhkan sinergi antara pemerintah, penyedia layanan digital, dan konsumen. Pemerintah perlu memperkuat regulasi dan penegakan hukum, sementara pelaku usaha wajib menerapkan sistem keamanan yang memadai untuk mengurangi risiko kebocoran data. Di sisi lain, konsumen juga diharapkan lebih berhati-hati dalam memberikan data pribadi dan meningkatkan kesadaran terkait potensi risiko transaksi digital. Melalui penerapan regulasi yang efektif dan edukasi literasi digital, diharapkan ekosistem transaksi digital di Indonesia dapat berkembang secara aman dan berkelanjutan, serta mampu meningkatkan kepercayaan publik terhadap layanan digital.

ABSTRACT

This study analyzes the applicable regulations, especially the Electronic Information and Transactions Law (UU ITE) and the Personal Data Protection Law (UU PDP). The ITE Law is the initial basis for regulating electronic transactions and prohibiting illegal access to personal data, while the PDP Law strengthens the rules regarding user consent and imposing strict sanctions for violations. Although both regulations have been enacted, their implementation in the field still faces various obstacles, such as weak law enforcement, lack of awareness among business actors, and minimal digital literacy among the public. The results of this study confirm that personal data protection requires synergy between the government, digital service providers, and consumers. The government needs to strengthen regulations and law enforcement, while business actors are required to implement an adequate security system to reduce the risk of data leakage. On the other hand, consumers are also expected to be more careful in providing personal data and increase awareness regarding the potential risks of digital transactions. Through the implementation of effective regulations and digital literacy education, it is hoped that the digital transaction ecosystem in Indonesia can develop safely and sustainably, and be able to increase public trust in digital services.

Corresponding Author:

Naufal Akbar
Fakultas Syari'ah dan Hukum, Universitas Islam Negeri Sumatera Utara,
Medan, Indonesia
Email: naufal290504@gmail.com

1. PENDAHULUAN

Di zaman modern yang berkembang ini segala sesuatu menuntut untuk kemudahan dalam hal digitalisasi. Beberapa contoh perubahan-perubahan akibat dari perkembangan dalam hal teknologi informasi dan komuniasi yang mana perekonomian, budaya, pertahanan dan keamanan serta pendidikan. Dalam mengikuti perkembangan modern. Saat ini, perdagangan digital atau e-commerce telah berkembang jauh sejak kemunculannya di era 1990-an. Dengan memanfaatkan teknologi internet dan kemajuan infrastruktur digital, e-commerce telah merombak cara kita berbelanja dan berbisnis secara mendasar. Sejarah awal e-commerce sendiri dapat ditelusuri ke tahun 1960-an, ketika organisasi bisnis mulai menggunakan Electronic Data Interchange (EDI) untuk mengirimkan dokumen bisnis secara elektronik. Bentuk e-commerce yang lebih kita kenal saat ini mulai muncul pada tahun 1990-an, seiring dengan kehadiran World Wide Web (WWW). Amazon, yang didirikan oleh Jeff Bezos pada tahun 1994, merupakan salah satu pionir yang sukses memperkenalkan konsep toko buku online yang inovatif. Di akhir 1990-an dan awal 2000-an, e-commerce mulai berkembang pesat meskipun masih dalam tahap awal. Perusahaan besar dan ritel tradisional mulai melihat e-commerce sebagai kanal penjualan yang potensial. Namun, pada masa itu, banyak konsumen masih memiliki kekhawatiran akan keamanan transaksi online, sehingga metode belanja konvensional tetap menjadi pilihan utama.

Dalam beberapa dekade terakhir, perkembangan teknologi informasi dan komunikasi telah mengubah secara drastis berbagai aspek kehidupan masyarakat, termasuk cara kita melakukan transaksi. Kemajuan di bidang teknologi ini memungkinkan masyarakat untuk bertransaksi secara digital, baik melalui e-commerce, layanan perbankan online, maupun platform keuangan lainnya. Transaksi digital menawarkan kemudahan, efisiensi, dan kenyamanan dalam berbelanja atau melakukan pembayaran tanpa harus bertatap muka. Namun, seiring dengan meningkatnya transaksi digital, muncul pula kekhawatiran terkait dengan keamanan dan perlindungan data pribadi konsumen.

Data diri konsumen, seperti nama, alamat, nomor telepon, dan informasi keuangan, kini menjadi salah satu aset penting yang diincar oleh berbagai pihak. Tidak hanya pelaku bisnis yang mengandalkan data tersebut untuk keperluan pemasaran, tetapi juga pelaku kejahatan siber yang berusaha mengeksploitasi kelemahan sistem keamanan untuk mencuri data pribadi konsumen. Kasus-kasus pencurian data, penyalahgunaan informasi pribadi, serta kebocoran data yang sering terjadi menunjukkan bahwa perlindungan data pribadi konsumen di ranah digital masih menghadapi berbagai tantangan.

Dalam konteks Indonesia, upaya untuk melindungi data pribadi konsumen sudah diatur dalam beberapa peraturan perundang-undangan, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Menteri Komunikasi dan Informatika tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Namun, regulasi yang ada dinilai belum cukup untuk memberikan perlindungan menyeluruh, mengingat perkembangan teknologi yang semakin cepat dan ancaman yang semakin kompleks. Oleh karena itu, diperlukan regulasi yang lebih komprehensif serta penerapan yang efektif guna memberikan jaminan perlindungan yang lebih kuat bagi konsumen.

Perlindungan data pribadi konsumen tidak hanya menjadi tanggung jawab pemerintah, tetapi juga penyedia layanan digital yang mengelola data tersebut. Penyedia layanan digital harus bertanggung

jawab untuk menerapkan sistem keamanan yang memadai dan transparan dalam mengelola data pribadi konsumen. Di sisi lain, konsumen juga perlu lebih waspada dalam memberikan data pribadi mereka dan memahami risiko yang mungkin timbul dari penggunaan data tersebut dalam transaksi digital.
Jurnal ini akan membahas perlindungan hukum terhadap data diri konsumen dalam transaksi digital di Indonesia. Fokus utama dari jurnal ini adalah mengeksplorasi peraturan perundang-undangan yang ada, menganalisis risiko yang dihadapi konsumen dalam transaksi digital, serta mengidentifikasi tanggung jawab penyedia layanan dalam melindungi data konsumen. Melalui analisis ini, diharapkan dapat ditemukan solusi yang tepat untuk memperkuat kerangka hukum perlindungan data pribadi di era digital.

2. METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif dengan pendekatan studi kasus kebocoran data Tokopedia dan Bukalapak. Data dianalisis berdasarkan:

1. Pendekatan perundang-undangan: Menganalisis UU PDP dan UU ITE terkait pelanggaran data digital.
2. Pendekatan konseptual: Menelaah konsep hak privasi dan perlindungan konsumen dalam transaksi digital.

Pendekatan kasus empiris: Membahas kasus nyata kebocoran data yang menimpa pengguna layanan e-commerce

3. HASIL DAN PEMBAHASAN

Kemajuan teknologi informasi telah melahirkan berbagai inovasi baru di sektor jasa keuangan, yang tidak hanya mempercepat proses transaksi tetapi juga mengubah cara masyarakat berinteraksi dengan layanan keuangan. Transformasi ini telah membawa perubahan signifikan dalam pola transaksi, di mana kegiatan yang sebelumnya memerlukan pertemuan tatap muka, seperti pembayaran, transfer dana, atau pembukaan rekening, kini dapat dilakukan secara daring melalui aplikasi perbankan, e-wallet, dan platform fintech.

Kemudahan ini memungkinkan pengguna untuk melakukan transaksi kapan saja dan di mana saja, tanpa terbatas oleh waktu dan lokasi. Namun, di balik segala manfaat tersebut, perkembangan teknologi informasi juga memunculkan sejumlah risiko dan tantangan baru. Permasalahan seperti pencurian data pribadi, penipuan daring (cyber fraud), kebocoran informasi konsumen, hingga masalah keamanan siber semakin marak terjadi, yang dapat menimbulkan kerugian material dan non-material bagi masyarakat.

Oleh karena itu, perubahan ini memerlukan respons yang memadai dari aspek hukum agar hak-hak konsumen dan pelaku usaha dapat terlindungi secara optimal. Regulasi yang tepat dan efektif harus disiapkan untuk mengatasi potensi pelanggaran dan menjaga keseimbangan antara inovasi digital dan kepastian hukum. Undang-undang seperti UU Pelindungan Data Pribadi (UU PDP) dan UU Informasi dan Transaksi Elektronik (UU ITE) menjadi fondasi penting dalam menghadapi berbagai tantangan yang timbul, namun tetap memerlukan implementasi yang konsisten dan penegakan hukum yang tegas. Dengan demikian, hukum tidak hanya berfungsi sebagai alat pengendali risiko tetapi juga sebagai penggerak untuk menciptakan ekosistem transaksi digital yang aman, adil, dan terpercaya bagi seluruh masyarakat.

3.1 Perlindungan Hukum Data diri Pengguna Transaksi Digital

Di era digital saat ini, transaksi e-commerce di Indonesia mengalami pertumbuhan yang sangat pesat. Platform-platform seperti JD.id, TikTok Shop, Tokopedia, Shopee, Blibli.com, OLX, Bhinneka.com, dan lainnya, kini sudah menjadi bagian dari keseharian masyarakat Indonesia. Sistem e-commerce memungkinkan pengguna untuk membeli dan menjual berbagai produk secara daring (online), memberikan kemudahan bagi masyarakat untuk memenuhi kebutuhan sehari-hari tanpa harus

keluar rumah. Setiap pengguna yang ingin menggunakan layanan e-commerce diwajibkan melakukan registrasi. Proses ini mengharuskan pengguna untuk mengisi data pribadi seperti nama lengkap, tanggal dan tahun lahir, serta alamat. Registrasi ini penting untuk mendata pengguna dengan akurat serta menjamin keamanan transaksi. Setelah terdaftar, pengguna akan mendapatkan akun resmi dan dapat melanjutkan proses transaksi jual-beli dengan mudah. Sebagai bagian dari kemudahan yang ditawarkan, banyak platform e-commerce di Indonesia yang menyediakan dompet digital atau e-wallet. Fasilitas ini memungkinkan pengguna untuk melakukan pembayaran secara langsung tanpa harus menggunakan aplikasi perbankan terpisah. Dengan konsep serupa seperti mobile banking, e-wallet memberikan kenyamanan dan fleksibilitas dalam transaksi [1]. Hanya pemilik akun dan penyelenggara e-commerce yang memiliki akses terhadap data keuangan ini, untuk menjamin kerahasiaan informasi pengguna. Walaupun e-commerce menawarkan kemudahan, pengguna juga harus berhati-hati dengan risiko keamanan data pribadi. Setiap transaksi dan aktivitas belanja daring mengandalkan data pribadi yang sensitif seperti metode pembayaran, informasi pemasaran, serta preferensi konsumen. Perlindungan data pribadi menjadi aspek yang sangat esensial dalam menjaga kepercayaan konsumen dan keamanan ekosistem digital. Kebocoran data, misalnya, dapat mengakibatkan konsekuensi serius seperti pencurian identitas, penyalahgunaan informasi pribadi untuk penipuan daring, hingga kerugian finansial yang sulit dipulihkan. Berdasarkan laporan oleh Cybersecurity Ventures**,** kejahatan dunia maya global diperkirakan menyebabkan kerugian hingga USD 10,5 triliun per tahun pada 2025 [2]. Oleh karena itu, penting bagi pengguna untuk memastikan platform e-commerce yang digunakan memiliki kebijakan perlindungan data yang kuat dan transparan.

Perlindungan hukum dapat dibedakan berdasarkan sumbernya menjadi dua jenis, yaitu perlindungan hukum internal dan perlindungan hukum eksternal. Perlindungan hukum internal berfokus pada pengaturan yang disepakati oleh para pihak dalam kontrak. Pada saat perjanjian disusun, kedua belah pihak menyepakati klausul-klausul yang bertujuan untuk melindungi kepentingan masing-masing. Semua risiko yang mungkin muncul dalam transaksi diantisipasi melalui ketentuan-ketentuan yang dituangkan dalam kontrak tersebut. Dengan demikian, setiap pihak memperoleh perlindungan hukum berdasarkan persetujuan bersama. Perlindungan ini hanya dapat terwujud apabila posisi tawar kedua belah pihak relatif setara, sehingga mereka dapat bebas menegosiasikan klausul-klausul kontrak sesuai dengan kebutuhan dan kepentingan masing-masing.

Namun, dalam praktiknya, banyak pengguna layanan digital tidak membaca *disclaimer* atau *terms of use* yang disediakan oleh platform digital. Mereka seringkali dihadapkan pada pilihan biner, seperti "yes" atau "no", "agree" atau "disagree", di mana jika mereka ingin melanjutkan penggunaan aplikasi, mereka terpaksa memilih "agree" atau "yes". Dengan memilih opsi tersebut, pengguna dianggap telah memberikan persetujuan atas segala syarat dan ketentuan yang berlaku, termasuk otorisasi penggunaan data pribadi oleh penyedia layanan.

Contohnya, dalam platform Tokopedia, data pribadi pengguna dikumpulkan dan digunakan untuk berbagai keperluan, seperti memproses transaksi, verifikasi pembayaran, promosi, hingga pengiriman produk. Selain itu, data tersebut dapat dimanfaatkan oleh mitra pemasaran, konsultan, atau penyedia layanan lainnya untuk tujuan komersial. Tokopedia menjelaskan dalam kebijakannya bahwa mereka berupaya melindungi data pengguna dengan menerapkan berbagai prosedur keamanan, seperti penggunaan kata sandi dan kode OTP. Namun, mereka juga menegaskan bahwa data yang dikirimkan melalui internet tidak sepenuhnya aman, dan risiko keamanan tersebut menjadi tanggung jawab pengguna.

Perlindungan hukum eksternal, di sisi lain, disediakan oleh negara dalam bentuk regulasi untuk mencegah ketidakadilan dan kerugian yang mungkin menimpa pihak yang lebih lemah dalam suatu transaksi [3]. Regulasi ini diperlukan agar bisnis dapat beroperasi dalam koridor yang adil dan sesuai hukum. Undang-undang disusun untuk mengantisipasi adanya eksploitasi oleh pihak yang memiliki posisi tawar lebih tinggi, sehingga pihak yang lebih lemah tetap dapat memperoleh manfaat secara adil.

Dalam konteks transaksi digital, UU Pelindungan Data Pribadi dan regulasi terkait lainnya menjadi instrumen penting untuk memastikan keseimbangan kepentingan antar pihak dan melindungi hak konsumen dari potensi penyalahgunaan.

3.2 Perlindungan Data Diri Konsumen Dalam Hukum Indonesia

Di Negara Indonesia, perlindungan data diri/data pribadi konsumen yang sudah diatur melalui beberapa regulasi, di antaranya :

1. Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah diubah dengan UU No. 19 Tahun 2016.
2. Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

Namun, pada penerapanya masih dianggap belum cukup mencakup keseluruhannya untuk menghadapi tantangan perlindungan data di era digital yang semakin kompleks. Penetapan pengesahan undang- undang perlindungan data pibadi (UU PDP) yang sangat diharapkan memberikan kepastian hukum yang lebih jelas bagi konsumen masih dalam proses pembahasan. Dalam percakapan sehari-hari, transaksi sering kali dipahami sebagai kesepakatan jual beli antara pihak-pihak yang terlibat. Namun, dalam konteks hukum, istilah transaksi lebih mengacu pada adanya perikatan atau hubungan hukum yang terjadi antara para pihak tersebut. Dengan kata lain, membahas transaksi berarti membahas aspek materiil dari hubungan hukum yang disepakati oleh para pihak (berdasarkan Pasal 1320 dan Pasal 1338 KUH Perdata). Pembahasan ini tidak merujuk pada tindakan hukum formal kecuali dalam kasus yang melibatkan benda tidak bergerak. Untuk transaksi yang melibatkan benda tidak bergerak, hukum mengatur bahwa tindakan hukum tersebut harus dilakukan secara jelas dan langsung.

Transaksi menggunakan media elektronik atau *online contract* adalah bentuk perjanjian atau hubungan hukum yang dilakukan secara digital, menggabungkan sistem informasi berbasis komputer dengan sistem komunikasi melalui jaringan dan layanan telekomunikasi. Proses ini didukung oleh adanya jaringan komputer global yang memungkinkan pertukaran informasi elektronik [4]. Oleh karena itu, keabsahan perjanjian juga sangat bergantung pada keandalan dari sistem elektronik tersebut. Suatu perjanjian dapat dianggap sah apabila komponen-komponen dalam sistem elektronik itu dapat dipercaya dan berfungsi sesuai dengan yang diharapkan.

3.3 Resiko Pelanggaran Data dalam Transaksi Digital

Seiring perkembangan zaman , pengguna dari transaksi digital semakin meningkat. Data pribadi , seperti nama alamat, nomor telepon, data bank, dan sebagainya, menjadi asset penting yang harus dijaga dari pelaku kejahatan siber yang mencari celah cara untuk mengeksploitasi kelemahan sistem keamanan. Resiko-resiko serius yg dapat terjadi, di antaranya:

1. Kebocoran dan Penyalahgunaan Data Pribadi

Informasi pribadi pengguna, seperti nama, alamat, nomor telepon, hingga data keuangan, rentan terhadap kebocoran saat disimpan atau diproses oleh penyedia layanan. Data yang bocor dapat dimanfaatkan oleh pihak tidak bertanggung jawab untuk berbagai kejahatan, seperti pencurian identitas dan penipuan finansial.

2. Penipuan dan Phishing

Phishing adalah metode penipuan di mana pelaku mengelabui korban agar memberikan informasi sensitif melalui tautan palsu atau pesan elektronik. Dalam konteks transaksi digital, konsumen bisa tertipu oleh situs atau email yang menyerupai layanan resmi, mengakibatkan pencurian data kartu kredit atau akses akun.

3. Penggunaan Data tanpa Izin (Unauthorized Use)

Dalam banyak kasus, pengguna layanan digital tidak menyadari bahwa data pribadi mereka digunakan di luar tujuan yang disepakati. Penyedia layanan mungkin bekerja sama dengan pihak ketiga untuk kepentingan pemasaran, tanpa mendapatkan persetujuan eksplisit dari pengguna, yang melanggar prinsip perlindungan data.

4. Eksploitasi Data melalui Data Mining dan Profiling

Platform digital sering melakukan data mining untuk mendapatkan wawasan tentang perilaku pengguna. Meskipun tujuannya bisa untuk meningkatkan layanan, data mining yang tidak diatur dengan baik dapat memicu praktik diskriminatif, seperti profiling konsumen berdasarkan status keuangan atau preferensi pribadi.

5. Serangan Siber (Cyber Attacks)

Peretas (hacker) dapat menyerang sistem penyedia layanan digital melalui malware atau serangan DDoS untuk mencuri informasi sensitif. Serangan ini tidak hanya merusak reputasi perusahaan, tetapi juga menimbulkan kerugian finansial bagi konsumen.

6. Kurangnya Tanggung Jawab dari Penyedia Layanan

Beberapa platform digital menyatakan dalam syarat penggunaan bahwa mereka tidak bertanggung jawab atas kerugian akibat kebocoran data, seperti terlihat dalam terms of use Tokopedia. Hal ini membuat konsumen menanggung risiko penuh jika terjadi pelanggaran data, sementara perlindungan yang dijanjikan seringkali tidak memadai.

7. Keterbatasan Keamanan pada Teknologi Internet

Meskipun sistem penyedia layanan menerapkan berbagai langkah keamanan, seperti OTP dan enkripsi, pengiriman data melalui internet tidak pernah sepenuhnya aman. Ancaman keamanan ini meningkatkan risiko pelanggaran data, terutama jika ada kelalaian dalam pengelolaan sistem atau lemahnya perlindungan keamanan siber.

8. Kepatuhan Hukum yang Tidak Konsisten

Beberapa platform mungkin tidak beroperasi sepenuhnya sesuai dengan regulasi yang berlaku, seperti UU Pelindungan Data Pribadi di Indonesia. Hal ini dapat menyulitkan pengguna untuk menuntut hak-haknya jika terjadi pelanggaran, terutama ketika layanan digital tersebut berbasis di luar negeri.

3.4 Kronologi dan Analisis Kasus Kebocoran Data Tokopedia dan Bukalapak

1. Tokopedia

Pada Mei 2020, sebuah laporan muncul bahwa data pengguna Tokopedia telah bocor dengan jumlah 91 juta data pengguna Tokopedia di retas dan data diperjualbelikan di forum gelap (dark web) dengan harga USD 5.000. Informasi yang bocor mencakup nama, alamat email, nomor telepon, username, dan hash password [4]. Pada awalnya, peretas hanya membocorkan sebagian kecil data untuk menarik perhatian dan menawarkan sisa data dengan imbalan pembayaran. Meski hash kata sandi telah dienskripsi, ada resiko peretas dapat membobol kata sandi tersebut menggunakan teknik brute force attack.

2. Bukalapak

Pada Maret 2019, 13 juta data pengguna Bukalapak dilaporkan bocor dan dijual di internet [5]. Meski data finansial tidak termasuk dalam kebocoran ini, informasi pribadi pengguna tetap bocor, yang dapat digunakan untuk aktivitas phishing dan penipuan. Ini bukan insiden pertama yang menimpa Bukalapak, karena sebelumnya mereka juga pernah mengalami serangan siber dengan sekala yang lebih kecil.

Kebocoran data di Tokopedia dan Bukalapak menjadi pengingat serius akan lemahnya sistem keamanan digital di Indonesia. Dengan semakin tingginya transaksi digital, diperlukan sistem perlindungan data yang kuat. Diharapkan bahwa penerapan UU PDP dapat menjadi solusi untuk

mengurangi risiko serupa di masa depan dan membangun kepercayaan publik dalam ekosistem digital Indonesia.

Contoh lain Risiko Penggunaan KTP dalam Kampanye Pemilihan

1. Penyalahgunaan Identitas (Identity Theft) Salinan KTP yang diberikan oleh pemilih kepada tim kampanye rentan disalahgunakan oleh pihak yang tidak bertanggung jawab. Data KTP bisa digunakan untuk:
    - Pembukaan rekening bank atau akun digital tanpa sepengetahuan pemilik.
    - Pendaftaran layanan pinjaman online atau pinjaman ilegal (pinjol).
    - Pemalsuan identitas untuk tindak pidana seperti penipuan atau pencucian uang.
2. Kebocoran Data Pribadi di Tangan Pihak Ketiga Tim kampanye sering kali tidak memiliki protokol keamanan data yang ketat, sehingga dokumen seperti fotokopi KTP dapat tersebar dan bocor tanpa kontrol. Data ini juga dapat diperjualbelikan di dark web, memperbesar peluang tindak kriminal [6].
3. Pemaksaan Partisipasi Politik dan Manipulasi Data Pemilih Dalam beberapa kasus, pemilih yang memberikan KTP dan menerima uang atau hadiah berisiko dijadikan alat politik untuk kepentingan kelompok tertentu. Selain itu, data pribadi bisa digunakan untuk memanipulasi hasil pemilu atau kampanye melalui pembuatan daftar pemilih fiktif atau ganda.

Adapun dampak Negatif Transaksi Digital Berbasis KTP dalam Kampanye :

1. Kehilangan Kendali atas Data Pribadi Ketika data KTP diserahkan, pemilik kehilangan kendali penuh atas penggunaannya. Dalam skenario terburuk, pengguna dapat menjadi korban phishing atau kejahatan siber lainnya karena identitasnya telah bocor.
2. Kerugian Finansial dan Hukum bagi Pemilik Data Penyalahgunaan KTP untuk pendaftaran akun bank atau pinjaman online dapat menimbulkan kerugian finansial, seperti utang tak terduga yang harus dibayar oleh korban. Selain itu, korban dapat terseret ke masalah hukum atas transaksi yang tidak pernah mereka lakukan.
3. Krisis Kepercayaan terhadap Sistem Pemilu Praktik ini menciptakan persepsi negatif terhadap proses pemilu dan memicu ketidakpercayaan publik terhadap integritas politik. Masyarakat bisa merasa bahwa pemilu tidak adil dan dipengaruhi oleh politik transaksional, yang merusak tatanan demokrasi.

3.5 Tantangan dalam Implementasi UU PDP

Meskipun UU PDP merupakan langkah maju dalam memperkuat perlindungan data pribadi, implementasinya di Indonesia masih menghadapi berbagai tantangan:

1. Kesiapan Infrastruktur dan Teknologi Keamanan

Banyak pelaku usaha, khususnya UMKM, belum memiliki teknologi keamanan yang sesuai standar, seperti enkripsi dan autentikasi dua faktor. Implementasi teknologi ini membutuhkan biaya besar, sehingga menjadi kendala bagi pelaku usaha kecil dan menengah. Selain itu, beberapa organisasi masih menggunakan sistem lama yang rentan terhadap serangan siber, seperti yang terlihat pada kasus kebocoran data di Tokopedia dan Bukalapak.

2. Rendahnya Kesadaran dan Kepatuhan Pelaku Usaha

Pelaku usaha seringkali memproses data konsumen tanpa izin eksplisit, bertentangan dengan prinsip *consent* yang diatur dalam UU PDP. Fokus utama perusahaan masih sering pada kepentingan komersial, bukan pada perlindungan privasi konsumen. Contoh praktik ini bisa dilihat dalam kebijakan privasi platform e-commerce, yang sering kali mengumpulkan data pengguna untuk kepentingan pemasaran.

3. Kurangnya Literasi Digital Masyarakat

Konsumen sering tidak menyadari hak-hak mereka terkait perlindungan data. Banyak pengguna layanan digital menyetujui syarat dan ketentuan tanpa membaca isinya secara detail, membuat mereka

rentan terhadap penyalahgunaan data. Edukasi dan literasi digital yang memadai sangat diperlukan agar masyarakat dapat lebih memahami risiko transaksi digital.

4. Penegakan Hukum yang Lemah

Penegakan UU PDP membutuhkan pengawasan dan koordinasi antar lembaga. Namun, keterbatasan sumber daya di instansi pengawas, seperti Kementerian Kominfo, dan proses hukum yang lambat membuat banyak kasus kebocoran data tidak mendapatkan penanganan yang tegas. Hal ini memperburuk situasi dengan kurangnya efek jera bagi pelaku pelanggaran.

5. Koordinasi Internasional dalam Penanganan Lintas Batas Negara

Banyak platform digital yang beroperasi di Indonesia memiliki basis di luar negeri, sehingga menyulitkan penegakan UU PDP. Tidak adanya keselarasan regulasi dengan undang-undang internasional, seperti GDPR di Uni Eropa, menjadi tantangan dalam menangani kasus kebocoran data lintas negara.

6. Kekosongan Hukum dalam Beberapa Aspek

Meskipun UU PDP telah mengatur banyak aspek perlindungan data, masih ada kekosongan hukum, seperti pengaturan mengenai penyimpanan data di luar negeri dan mekanisme penyelesaian sengketa. Kekosongan ini menimbulkan ambiguitas dalam penerapan dan menyulitkan konsumen untuk menuntut hak mereka saat terjadi pelanggaran.

3.6 Upaya Pencegahan dan Rekomendasi

Perlindungan data pribadi konsumen menjadi semakin penting seiring dengan meningkatnya penggunaan internet dan media sosial. Informasi pribadi, seperti nama, alamat, nomor telepon, dan detail lainnya yang dikumpulkan oleh berbagai platform dan penyedia layanan, menjadi aset berharga bagi berbagai pihak. Meskipun data pribadi ini umumnya dikumpulkan untuk tujuan bisnis dan pemasaran yang sah, tetap ada potensi risiko yang perlu diwaspadai. Salah satu ancaman utamanya adalah kebocoran data atau pelanggaran keamanan yang dapat menyebabkan data konsumen jatuh ke pihak yang tidak bertanggung jawab, yang berpotensi memicu pencurian identitas, penipuan, dan eksploitasi lainnya. Kebocoran data dapat berdampak buruk secara finansial dan merusak reputasi individu maupun perusahaan yang terkait. Oleh karena itu, melindungi data pribadi konsumen adalah suatu kebutuhan mendesak. Regulasi perlindungan data dalam transaksi e-commerce berfungsi untuk mengatur pengumpulan, pemanfaatan, penyimpanan, dan keamanan data konsumen oleh perusahaan dan platform e-commerce. Tujuan dari regulasi ini adalah menjaga privasi, keamanan, serta hak-hak konsumen terkait penggunaan data pribadi mereka.

Secara umum, perlindungan data pribadi sebenarnya sudah diatur dalam UU ITE. Beberapa pasal dalam UU ITE, khususnya Pasal 30-33 dan Pasal 35 yang berada di BAB VII tentang Tindakan yang Dilarang, secara jelas melarang akses ilegal terhadap data pribadi milik orang lain melalui sistem elektronik dengan cara menembus sistem keamanan untuk mendapatkan informasi. UU ITE juga menyatakan bahwa penyadapan (intersepsi) termasuk dalam tindakan terlarang, kecuali dilakukan oleh pihak yang berwenang dalam konteks penegakan hukum. Setiap orang yang dirugikan akibat tindakan terlarang ini berhak mengajukan tuntutan ganti rugi, dan pelaku memiliki kewajiban hukum atas tindakannya.

Meski UU ITE memberikan perlindungan bagi data pribadi dalam transaksi elektronik, undang-undang ini tidak menjelaskan secara rinci apa yang dimaksud dengan data pribadi. Definisi data pribadi dapat ditemukan dalam regulasi turunan di bawah UU ITE, seperti Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik dan Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Selain itu, definisi data pribadi juga diatur dalam UU PDP, yang merinci jenis-jenis data pribadi. Berdasarkan Pasal 4 UU tersebut, data pribadi terbagi menjadi dua jenis, yaitu:

1. Data pribadi yang bersifat spesifik, meliputi:

a) Data dan informasi kesehatan;
b) Data biometrik;
c) Data genetika;
d) Catatan kejahatan;
e) Data anak;
f) Data keuangan pribadi;
g) Data lainnya sesuai dengan ketentuan peraturan perundang-undangan.

2. Data pribadi yang bersifat umum, meliputi:
a) Nama lengkap;
b) Jenis kelamin;
c) Kewarganegaraan;
d) Agama;
e) Status perkawinan;
f) Data Pribadi yang dikombinasikan untuk mengidentifikasi seseorang.

3.8 Implementasi UU PDP dan UU ITE

1. *Implementasi UU PDP (Undang-Undang Perlindungan Data Pribadi)*

UU PDP merupakan regulasi baru yang diharapkan dapat memberikan kepastian hukum dan meningkatkan perlindungan data pribadi di Indonesia. Beberapa aspek penting dalam implementasi UU PDP antara lain:

1. Kesiapan Infrastruktur dan Sistem Elektronik

Perusahaan dan instansi pemerintah dituntut untuk menyesuaikan sistem keamanan informasi dengan standar yang ditetapkan UU PDP. Tantangan ini tidak mudah karena diperlukan biaya besar dan tenaga ahli dalam membangun sistem keamanan yang memadai. Bahkan, beberapa perusahaan e-commerce di Indonesia masih mengalami kebocoran data meski telah mengklaim menerapkan sistem keamanan berlapis [7].

2. Kesadaran dan Kepatuhan Pelaku Usaha Banyak pelaku bisnis belum memiliki pemahaman menyeluruh tentang kewajiban mereka dalam pengelolaan data pribadi konsumen. Mereka sering menggunakan data konsumen untuk pemasaran tanpa izin, yang melanggar prinsip *consent* sebagaimana diatur dalam UU PDP [8].

3. Sanksi dan Penegakan Hukum UU PDP menetapkan sanksi administratif berupa denda dan penutupan layanan serta sanksi pidana bagi pelanggaran serius. Namun, efektivitas sanksi ini sangat bergantung pada pengawasan dan konsistensi penegakan hukum oleh Kominfo dan lembaga terkait lainnya.

2. Implementasi UU ITE dalam Konteks Perlindungan Data Konsumen

UU ITE (Undang-Undang Informasi dan Transaksi Elektronik) memberikan landasan hukum untuk mengatur transaksi elektronik dan perlindungan data pribadi. Beberapa aspek penting dalam implementasi UU ITE adalah:

1. Perlindungan terhadap Akses Tanpa Izin dan Penyadapan UU ITE melarang tindakan peretasan dan penyadapan data pribadi tanpa izin (Pasal 30-33). Namun, dalam beberapa kasus, implementasinya masih kurang optimal karena keterbatasan teknologi dan kurangnya koordinasi antar penegak hukum [9]

2. Tantangan Penanganan Kasus Siber Kasus kebocoran data di Tokopedia dan Bukalapak menunjukkan bahwa penegakan hukum terkait perlindungan data masih memiliki banyak kelemahan. Sistem keamanan digital perusahaan perlu diperkuat untuk mencegah insiden serupa di masa depan.

3. Kolaborasi Internasional Mengingat banyak platform digital beroperasi lintas negara, Indonesia perlu berkolaborasi dengan lembaga internasional dan negara lain dalam penegakan hukum siber. Ini sangat penting untuk menangani pelanggaran data yang melibatkan perusahaan multinasional.

3. Penggabungan UU PDP dan UU ITE untuk Perlindungan Data yang Lebih Baik

Kedua regulasi ini harus berjalan seiring untuk menciptakan ekosistem transaksi digital yang aman. Beberapa langkah yang dapat diambil meliputi:

1. Penguatan Lembaga Pengawas Dibutuhkan lembaga pengawas independen untuk memantau pelaksanaan UU PDP dan UU ITE serta menindak pelanggaran dengan tegas.
2. Kampanye Literasi Digital Pemerintah dan perusahaan perlu mengedukasi masyarakat agar lebih sadar tentang pentingnya perlindungan data pribadi dan risiko dalam transaksi digital.
3. Penerapan Standar Keamanan Tinggi Semua platform digital wajib menerapkan teknologi enkripsi dan autentikasi ganda untuk melindungi data konsumen dari peretasan dan penyalahgunaan.

4. KESIMPULAN

Perkembangan transaksi digital di Indonesia telah membawa banyak manfaat, seperti efisiensi dan kemudahan bagi konsumen. Namun, di sisi lain, kemajuan ini juga menimbulkan risiko terhadap keamanan data pribadi konsumen. Kasus kebocoran data di platform e-commerce seperti Tokopedia dan Bukalapak menjadi bukti nyata bahwa sistem keamanan masih belum optimal dalam melindungi informasi pribadi pengguna.

Upaya perlindungan data pribadi konsumen di Indonesia telah diatur melalui UU ITE dan UU PDP. UU ITE menyediakan dasar hukum untuk melarang akses ilegal dan peretasan data, sedangkan UU PDP memperkuat perlindungan dengan menetapkan kewajiban persetujuan konsumen dan sanksi tegas bagi pelanggaran. Namun, implementasi kedua undang-undang ini masih menghadapi tantangan, seperti kurangnya kesadaran pelaku usaha, lemahnya penegakan hukum, dan kurangnya literasi digital di kalangan masyarakat.

Untuk menciptakan ekosistem transaksi digital yang aman dan terpercaya, diperlukan kolaborasi antara pemerintah, penyedia layanan digital, dan konsumen. Pemerintah harus memperkuat regulasi dan penegakan hukum, sementara pelaku usaha wajib menerapkan teknologi keamanan yang memadai. Di sisi lain, konsumen perlu meningkatkan kewaspadaan dalam memberikan data pribadi.

Melalui sinergi berbagai pihak dan penerapan regulasi secara konsisten, risiko kebocoran data dapat diminimalkan, sehingga kepercayaan publik terhadap layanan digital dapat meningkat. Dengan begitu, ekosistem transaksi digital di Indonesia dapat berkembang secara aman dan berkelanjutan.

REFERENSI

[1] DataReportal. (2023). "Digital 2023: Indonesia". Melaporkan statistik terbaru pengguna internet dan e-commerce di Indonesia.
[2] Cybersecurity Ventures, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025."
[3] Gellert, R., & Gutwirth, S. (2013). "The Legal Construction of Privacy and Data Protection." *Computer Law & Security Review*, 29(5), 522–530.
[4] Maulana, R. (2020). “Analisis Kebocoran Data Tokopedia dan Dampaknya terhadap Perlindungan Konsumen.” *Jurnal Keamanan Siber*, 5(2), 112-126.
[5] Makarim, Edmon. *Pengantar Hukum Telematika dan Transaksi Elektronik*. Jakarta: Rajawali Pers, 2019.
[6] Raharjo, Agus. *Hukum Siber: Perlindungan Data Pribadi dan Hak Konsumen*. Yogyakarta: Deepublish, 2020.
[7] Kominfo, *Kasus Kebocoran Data Tokopedia dan Implikasinya terhadap Perlindungan Data Konsumen* (2020), hlm. 15.
[8] Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, Pasal 14

[9] Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan perubahan dengan UU No. 19 Tahun 2016.
[10] Bainbridge, David. *Introduction to Information Technology Law*. London: Pearson, 2015.