

Perlindungan Data Pribadi Konsumen Dalam Transaksi *E-Commerce* di Era Ekonomi Digital

^{1.*} M. Miftahul Ikhsan

^{2.} Nova Elsa

^{3.} Fathan Elan Yuukhaa, M.

^{4.} Kristina Andini

^{5.} Meni Apriyani

^{1,2.} Fakultas Humaniora dan Informasi, Universitas Muhammadiyah Ahmad Dahlan Palembang.

* Corresponding author, email: mmikhsan27@gmail.com

 <https://doi.org/10.56128/jkih.v6i2.1063>

ABSTRAK: Penelitian ini membahas tentang Perlindungan Data Pribadi UU Nomor 27 Tahun 2022, dalam konteks pesatnya kemajuan teknologi dan perdagangan elektronik (*e-commerce*). Era digital yang semakin kompleks menimbulkan tantangan serius terkait keamanan dan privasi data pribadi masyarakat. Artikel ini menguraikan latar belakang, kerangka hukum, serta evaluasi efektivitas UU Perlindungan Data Pribadi guna melindungi dari pelanggaran maupun penyalahgunaan data pribadi. Meskipun undang-undang telah menetapkan kebijakan seperti kewajiban penunjukan *Data Protection Officer*, persetujuan eksplisit pengguna, serta sanksi administratif dan pidana. Di wilayah Uni Eropa terdapat regulasi *General Data Protection Regulation* (GDPR) yang menunjukkan bahwa penerapan tersebut dapat menurunkan angka pelanggaran secara signifikan. Oleh karena itu, artikel ini menekankan perlunya pembaruan regulasi yang bertaraf Internasional guna menjamin pengamanan data yang lebih efektif dan menjawab tantangan perkembangan teknologi digital.

KATA KUNCI: *e-commerce*; *General Data Protection Regulation*; keamanan data; perlindungan data pribadi.

PENDAHULUAN

Transformasi digital yang terjadi dalam dua dekade terakhir telah mengubah pola aktivitas ekonomi masyarakat secara signifikan. Perkembangan internet, perangkat komunikasi digital, dan teknologi informasi telah mendorong pertumbuhan perdagangan elektronik (*e-commerce*) (Anugrah et al., 2025) sebagai salah satu sektor utama dalam ekonomi digital. Indonesia menjadi salah satu negara dengan pertumbuhan ekonomi digital terbesar di kawasan Asia Tenggara yang ditandai dengan meningkatnya jumlah pengguna internet serta tingginya intensitas transaksi melalui berbagai platform digital. Kondisi tersebut memberikan peluang yang besar bagi pelaku usaha untuk memperluas pasar dan meningkatkan efisiensi bisnis,

sekaligus memberikan kemudahan bagi masyarakat dalam memperoleh barang dan jasa tanpa dibatasi ruang dan waktu (Arief & Risma, n.d.).

Di balik berbagai manfaat tersebut, perkembangan *e-commerce* juga menimbulkan tantangan baru yang berkaitan dengan pengelolaan data pribadi konsumen. Dalam setiap transaksi digital, konsumen umumnya diminta untuk memberikan berbagai informasi yang diperlukan dalam proses registrasi, verifikasi identitas, pembayaran, maupun pengiriman barang. Seiring meningkatnya volume transaksi digital, jumlah data pribadi yang tersimpan dalam sistem elektronik juga semakin besar. Kondisi tersebut menyebabkan data pribadi menjadi salah satu aset yang memiliki nilai ekonomi tinggi sekaligus menjadi objek yang rentan terhadap penyalahgunaan, akses tanpa hak, maupun kebocoran data (Kasus & Com, 2021).

Fenomena kebocoran data yang terjadi dalam beberapa tahun terakhir menunjukkan bahwa perlindungan data pribadi masih menjadi persoalan penting dalam penyelenggaraan sistem elektronik di Indonesia. Berbagai kasus kebocoran data pada *platform* digital menunjukkan bahwa risiko penyalahgunaan data tidak hanya menimbulkan kerugian ekonomi bagi konsumen, tetapi juga berpotensi mengurangi kepercayaan masyarakat terhadap layanan digital. Situasi tersebut menjadi semakin penting setelah meningkatnya penggunaan layanan *e-commerce*, *financial technology*, dan berbagai layanan berbasis digital yang mengandalkan pengumpulan serta pemrosesan data pribadi dalam jumlah besar (Alifia Fisilmi Kaffah & Siti Malikhatun Badriyah, 2024).

Sebagai respons terhadap perkembangan tersebut, pemerintah Indonesia telah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi sebagai landasan hukum yang mengatur hak dan kewajiban para pihak dalam pemrosesan data pribadi. Kehadiran regulasi ini diharapkan mampu memberikan kepastian hukum bagi masyarakat sekaligus meningkatkan akuntabilitas penyelenggara sistem elektronik dalam mengelola data pribadi konsumen. Namun demikian, keberadaan regulasi belum tentu menjamin efektivitas perlindungan data apabila tidak diikuti oleh kepatuhan pelaku usaha, efektivitas pengawasan, kesiapan infrastruktur keamanan, dan kesadaran hukum masyarakat sebagai pengguna layanan digital.

Penelitian mengenai perlindungan data pribadi dan transaksi elektronik telah banyak dilakukan oleh peneliti sebelumnya dengan fokus kajian yang beragam. Penelitian yang dilakukan oleh Yulianingsih dan Putra (2024) mengkaji perlindungan konsumen dalam *transaksi e-commerce* melalui pendekatan yuridis normatif dan menemukan pentingnya penguatan instrumen hukum dalam menjamin hak-hak konsumen pada transaksi digital (Yulianingsih & Putra, 2024). Penelitian Kaffah dan Badriyah (2024) menyoroti aspek hukum perlindungan bisnis di era digital serta pentingnya penyesuaian regulasi terhadap perkembangan teknologi (Alifia Fisilmi Kaffah & Siti Malikhatun Badriyah, 2024). Sementara itu, (Ridha et al., 2024) menelaah perlindungan konsumen digital dari perspektif hukum perlindungan konsumen dan menemukan bahwa pengawasan terhadap pelaku usaha digital masih menjadi tantangan dalam menjamin perlindungan hak-hak konsumen.

Penelitian lainnya dilakukan oleh (Khairani Alawiyah Matondang et al., 2025) yang mengkaji perlindungan data pribadi dari perspektif etika bisnis dan menekankan pentingnya tanggung jawab perusahaan dalam menjaga kepercayaan konsumen melalui pengelolaan data yang bertanggung jawab. Selanjutnya, (Rasid, 2025) mengkaji implikasi Undang-Undang Perlindungan Data Pribadi terhadap transaksi *e-commerce* dan menunjukkan bahwa regulasi tersebut memberikan dasar hukum yang lebih kuat dalam melindungi hak-hak subjek data. Di sisi lain, Vania et al. (2024) mengkaji perlindungan data pribadi dari aspek keamanan data dan keamanan siber dengan menekankan pentingnya penerapan sistem keamanan informasi dalam mencegah terjadinya kebocoran data.

Berbagai penelitian terdahulu tersebut menunjukkan bahwa kajian mengenai perlindungan data pribadi telah berkembang dari berbagai perspektif, baik perlindungan konsumen, hukum bisnis digital, keamanan siber, maupun etika bisnis. Akan tetapi, sebagian besar penelitian masih membahas aspek-aspek tersebut secara terpisah. Penelitian yang berfokus pada perlindungan konsumen umumnya belum mengaitkan secara mendalam implementasi Undang-Undang Nomor 27 Tahun 2022 dengan praktik pengelolaan data pribadi dalam transaksi *e-commerce*. Sebaliknya, penelitian yang membahas keamanan data dan keamanan siber cenderung lebih menitikberatkan pada aspek teknis dan belum mengintegrasikan analisis mengenai tanggung jawab hukum pelaku usaha serta efektivitas penegakan hukum dalam perlindungan data pribadi.

Berdasarkan kondisi tersebut, masih terdapat kesenjangan penelitian (*research gap*) yang perlu dikaji lebih lanjut, yaitu belum adanya analisis yang mengintegrasikan implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, tanggung jawab pelaku usaha *e-commerce*, perlindungan konsumen, efektivitas penegakan hukum, serta tantangan perlindungan data pribadi dalam satu kerangka hukum bisnis digital yang komprehensif. Padahal keterkaitan antara aspek regulasi, kepatuhan pelaku usaha, perlindungan konsumen, dan keamanan data menjadi faktor penting dalam menentukan efektivitas perlindungan data pribadi di era ekonomi digital.

Berdasarkan kesenjangan tersebut, kebaruan (*novelty*) penelitian ini terletak pada pendekatan integratif yang menghubungkan aspek perlindungan data pribadi, hukum bisnis digital, perlindungan konsumen, tanggung jawab pelaku usaha, dan efektivitas implementasi Undang-Undang Nomor 27 Tahun 2022 dalam praktik transaksi *e-commerce*. Selain itu, penelitian ini juga mengkaji berbagai kasus kebocoran data sebagai dasar untuk mengevaluasi efektivitas perlindungan data pribadi yang telah diterapkan dalam ekosistem perdagangan digital di Indonesia. Pendekatan tersebut diharapkan dapat menghasilkan analisis yang lebih komprehensif dibandingkan penelitian terdahulu yang umumnya hanya berfokus pada satu aspek tertentu.

Berdasarkan uraian tersebut, penelitian ini bertujuan untuk menganalisis implementasi perlindungan data pribadi konsumen dalam transaksi *e-commerce* berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, mengkaji tanggung jawab hukum pelaku usaha dalam pengelolaan data pribadi konsumen, serta menganalisis berbagai tantangan dan prospek perlindungan data pribadi dalam mendukung perkembangan ekonomi digital di Indonesia.

Secara akademis, penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan kajian hukum bisnis digital, hukum perlindungan konsumen, dan hukum siber, khususnya yang berkaitan dengan perlindungan data pribadi dalam transaksi elektronik. Secara praktis, hasil penelitian ini diharapkan dapat menjadi bahan pertimbangan bagi pemerintah dalam penyempurnaan kebijakan perlindungan data pribadi, menjadi rujukan bagi pelaku usaha dalam meningkatkan tata kelola data yang sesuai dengan ketentuan peraturan perundang-undangan, serta menjadi sumber informasi bagi masyarakat mengenai pentingnya perlindungan data pribadi dalam aktivitas ekonomi digital.

METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan komparatif untuk mengkaji perlindungan data pribadi dalam transaksi *e-commerce* (Afrizal, 2014). Pendekatan perundang-undangan digunakan untuk menelaah Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Informasi dan Transaksi Elektronik, serta regulasi terkait transaksi elektronik dan pelindungan konsumen, sedangkan pendekatan konseptual digunakan untuk menganalisis pelindungan data pribadi, tanggung jawab pelaku usaha, dan pelindungan konsumen dalam ekonomi digital. Bahan hukum primer berupa peraturan perundang-undangan terkait, bahan hukum sekunder meliputi buku, jurnal, hasil penelitian, prosiding, laporan kasus kebocoran data, dan publikasi akademik, serta bahan hukum tersier berupa kamus dan ensiklopedia hukum (Ikhsan et al., 2024). Bahan hukum dikumpulkan melalui studi kepustakaan dan dokumentasi, kemudian dianalisis secara deskriptif-kualitatif melalui inventarisasi, klasifikasi, interpretasi, dan penalaran hukum. Analisis difokuskan pada kesesuaian implementasi dengan Undang-Undang Pelindungan Data Pribadi, tanggung jawab pelaku usaha, efektivitas pelindungan konsumen, dan kontribusinya terhadap kepercayaan digital sebagai fondasi ekonomi digital Indonesia (Nanda Dwi Rizkia, 2023).

HASIL & PEMBAHASAN

Kerangka Hukum Perlindungan Data Pribadi di Indonesia

Perlindungan Data Pribadi dalam UU Nomor 27 Tahun 2022 mendefinisikan sebagai serangkaian tindakan yang dilakukan untuk melindungi informasi individu selama proses pengelolaan data, untuk menjamin terpenuhinya hak konstutisional pemilik data. Berdasarkan pasal 4, informasi individu dipecah dibagi dua macam. Pertama, informasi bersifat spesifik, mencakup data seperti kondisi kesejahteraan, riwayat tindak pidana, informasi anak, perekonomian, dan informasi yang ditur oleh Undang-Undang. Kedua, informasi bersifat umum, meliputi nama lengkap, *gender*, kebangsaan, keyakinan yang dianut, status menikah, dan data lainnya.(Yuniarti, 2019)

Pemerintah mengesahkan UU Perlindungan Data Pribadi untuk memeberikan keamanan informasi individu sebagai hak warga negara. Peraturan ini juga dimaksudkan dalam memperkuat aspek norma dalam pengelolaan informasi individu, serta memberikan jaminan hukum apabila terjadi penyalahgunaan terhadap informasi pribadi. Sebelum aturan ini diberlakukan, ketentuan mengenai perlindungan data tetap menyebar di regulasi sektoral dan belum struktur dengan menyeluruh. Akibatnya, berbagai regulasi di tingkat sektoral belum sepenuhnya mampu memberikan perlindungan maupun kepastian hukum yang menyeluruh terhadap pengelolaan data pribadi. Sementara itu, dalam karyanya, Celina Tri Siwi Kristiyanti (2011) mengemukakan sejumlah prinsip perlindungan konsumen yang berbeda berdasarkan jenis tanggung jawabnya. Adapun beberapa prinsip aturan tersebut antara lain:

- a. Aturan pertanggung jawaban atas kesalahan.
- b. Aturan pertanggung jawaban dalam kecurigaan.

- c. Aturan tidak semua pihak harus dipertanggung jawabkan atas peristiwa informasi.
- d. Aturan pertanggung jawaban sepenuhnya.
- e. Aturan batasan pertanggung jawaban.(Kasus & Com, 2021)

Meskipun kerangka pengaturan bervariasi pada setiap negeri, secara umum ketentuan-ketentuan tersebut tetap berpedoman pada prinsip dasar yang serupa. Sebagian besar sistem perlindungan data merujuk pada asas *Organization for Economic Coperation and Development* (OECD) di tahun 1980. Asas tersebut memperkenalkan ajaran utama pada informasi, kemudian diterima secara global (OECD, 2013). Adapun Aturan-aturan berdasarkan OECD yaitu meliputi sebagai berikut:

Prinsip	Penjelasan
Prinsip Pembatasan Pengumpulan <i>Collection Limitation Principle</i>	Harus ada batasan untuk pengumpulan data pribadi dan data semacam itu harus diperoleh dengan cara yang sah dan adil dan dengan sepengetahuan atau persetujuan dari subjek data.
Prinsip Kualitas Data <i>Data Quality Principle</i>	Data pribadi harus relevan dengan tujuan penggunaannya, dan sejauh yang diperlukan untuk tujuan tersebut, harus akurat, lengkap, dan terus diperbarui.
Prinsip Spesifikasi Tujuan <i>Purpose Specification Principle</i>	Tujuan pengumpulan data pribadi harus ditentukan selambat-lambatnya pada saat pengumpulan data dan penggunaan selanjutnya terbatas pada pemenuhan tujuan tersebut atau tujuan lainnya yang tidak sesuai dan ditentukan untuk setiap perubahan tujuan.
Prinsip Pembatasan Penggunaan <i>Use Limitation Principle</i>	Data pribadi tidak boleh diungkapkan, tersedia atau digunakan untuk tujuan selain yang ditentukan kecuali: (a) dengan persetujuan subjek data; atau (b) oleh otoritas hukum.
Prinsip Perlindungan Keamanan <i>Security Safeguards Principle</i>	Data pribadi harus dilindungi oleh perlindungan keamanan yang wajar terhadap risiko seperti kehilangan atau akses tidak sah, perusakan, penggunaan, modifikasi atau pengungkapan data.
Prinsip Keterbukaan <i>Openness Principle</i>	Adanya kebijakan keterbukaan tentang perkembangan, praktik, dan <i>policy</i> berkenaan dengan data pribadi. Sarana tersebut harus tersedia untuk menetapkan keberadaan dan sifat data pribadi, dan tujuan utama penggunaannya, serta identitas dan lokasi pengontrol data (<i>data controller</i>).
Prinsip Partisipasi Individu <i>Individual Participation Principle</i>	Individu berhak: a. untuk memperoleh dari pengontrol data (<i>data controller</i>), atau konfirmasi, apakah pengontrol data memiliki data terkait atau tidak; b. untuk berkomunikasi dengan mereka, data yang berkaitan dengan mereka: (i) dalam waktu yang wajar;(ii) dengan biaya, jika ada;(iii) alasan yang cukup; dan (iv) diberikan dalam bentuk yang dapat dipahami. c. Diberikan alasan jika permintaan dibuat berdasarkan huruf (a) dan (b) di tolak, dan dapat diargumentasikan penolakan tersebut; d. Untuk melawan data terkait mereka, dan seandainya perlawanan tersebut benar, untuk menghapus data, memperbaiki, melengkapi atau mengubah.
Prinsip Akuntabilitas <i>Accountability Principle</i>	Pengontrol data (<i>data controller</i>) harus bertanggung jawab untuk mematuhi langkah-langkah yang berdampak pada prinsip-prinsip yang disebutkan di atas.

Gambar 1.1 Prinsip Perlindungan Data

UU PDP juga menetapkan prinsip-prinsip fundamental yang harus ditaati dalam segala bentuk pengolahan data. Pengumpulan data harus dilakukan dengan tujuan yang jelas, sah, serta berdasarkan persetujuan dari subjek data. Setiap penggunaan data wajib dilakukan secara transparan dan bertanggung jawab, sedangkan keamanan dan kerahasiaan data harus selalu dijaga agar terhindar dari risiko kebocoran maupun akses tidak sah. Semua proses data harus tetap berpedoman pada kewajaran, proporsionalitas, serta penghormatan terhadap hak data individu.

Hak-hak utama yang dijamin meliputi hak untuk memperoleh informasi terkait pemrosesan datanya, hak mengakses dan memperbaiki data, hak menghapus data, serta hak menarik persetujuan atas pemrosesan datanya. Selain itu, subjek data juga berhak mengajukan keberatan terhadap perlakuan data dan menuntut ganti rugi apabila mengalami kerugian akibat pelanggaran data pribadi. Selain itu, pihak yang bertanggung jawab dalam pengendalian maupun penyimpanan informasi memperoleh izin yang jelas dari pemilik data sebelum melakukan pengumpulan atau pengolahan. Mereka juga harus memastikan keamanan serta keutuhan data, dan segera memberikan laporan jika terjadi pelanggaran atau kebocoran informasi (Rasid, 2025).

Implementasi perlindungan data juga melibatkan pembentukan lembaga pengawas yang disebut Otoritas Pelindungan Data Pribadi. Lembaga ini berfungsi untuk mengawasi

pelaksanaan undang-undang, menerima pengaduan, serta menjalankan fungsi penegakan hukum administrasi. Walaupun hingga pertengahan 2025 lembaga ini masih dalam proses finalisasi, untuk sementara fungsi pengawasan dijalankan oleh kementerian terkait. Keberadaan lembaga ini diharapkan dapat menjamin efektivitas perlindungan data serta menyelesaikan celah penegakan hukum yang sebelumnya ada di Indonesia. (Yuniarti, 2019)

Aspek Hukum Bisnis dalam Pengelolaan Data *E-Commerce*

Perlindungan Data pribadi pada Sistem Elektronik (Peraturan Kominfo 20/2016) disusun melalui Peraturan Kementerian Komunikasi dan Informatika tentang transaksi elektronik bagi konsumen. Umumnya, ketentuan dalam peraturan tersebut memuat hal-hal sebagai berikut:

a. Definisi Data Pribadi

Data pribadi diartikan seolah-olah semua informasi yang bersangkutan pada individu bisa digunakan untuk mengenali identitasnya, baik secara langsung maupun melalui penggabungan dengan data lain. Jenis informasi tersebut mencakup antara nama lain, tempat tinggal, nomor ponsel, *email*, *personalitas*, catatan transaksi, serta informasi lainnya (Ardika, 2025).

b. Hak Pribadi atas Data Pribadi

Peraturan ini juga menegaskan hak-hak dasar individu atas data pribadi yang mereka miliki. Konsumen berhak memperoleh informasi, mengakses, memperbarui, memperbaiki, menghapus, membatasi pemanfaatan, hingga menyimpan data pribadinya. Selain itu, individu juga dapat menyampaikan keberatan atau pengaduan apabila data pribadinya digunakan tanpa izin atau bertentangan dengan ketentuan hukum yang berlaku..

c. Kewajiban Pengelola Data Pribadi

Pihak yang mengelola data pribadi, yakni mereka yang menghimpun, memproses, menyimpan, dan memanfaatkan data tersebut, diwajibkan menerapkan sejumlah prinsip dasar seperti keadilan, keterbukaan, menggarap tujuan, memahami, kebermanfaatan, keakuratan, keamanan, dan akuntabilitas dalam setiap kegiatan pengelolaan data pribadi konsumen.

d. Ketentuan Penyimpanan dan Pemanfaatan Data

Dalam peraturan ini juga diatur mengenai pengumpulan dan penyimpanan informasi pribadi, dimana hal ini harus dilakukan dalam kurun waktu sesuai dengan tujuan di awal. Pihak yang bertanggung jawab dalam menjaga keamanan informasi dan penyebaran data tanpa izin merupakan tugas pengelola data informasi.

e. Pemberitahuan Pelanggaran Data

Apabila terjadi pelanggaran atau kebocoran keamanan data, pengelola wajib memberitahukan hal tersebut kepada konsumen yang datanya terdampak. Pemberitahuan ini bertujuan agar pemilik data dapat segera mengantisipasi dalam melindungi data informasi dari penyalahgunaan data.

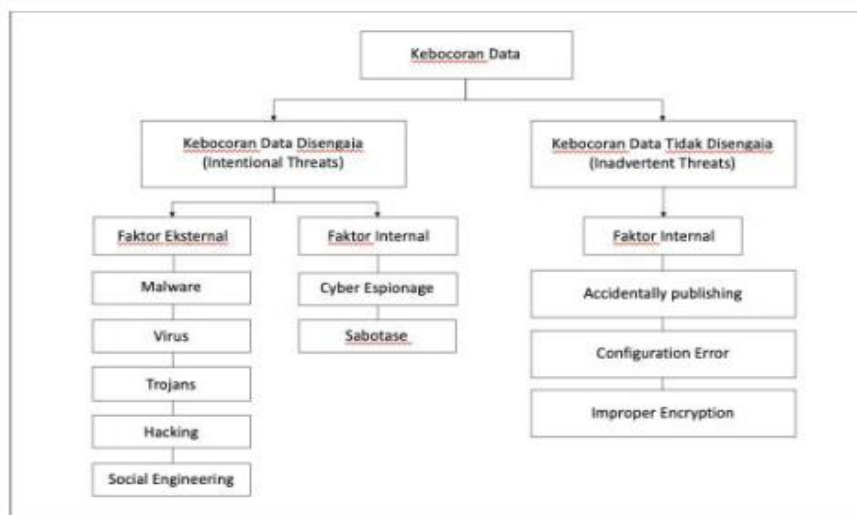
e. Pemanfaatan Data Pribadi untuk Kegiatan Pemasaran

Penggunaan data informasi hanya boleh dilakukan apabila pengelola telah memperoleh izin eksplisit dari konsumen, kecuali terdapat dasar hukum lain yang secara jenis mengizinkan pemanfaatan tanpa izin yang telah diatur pada Peraturan Kominfo 20/2016. Selain itu, pengalihan data pribadi ke pihak lain juga harus adanya persetujuan dari pemilik data (Fathaniyah et al., 2023).

f. Penghapusan Data Pribadi

Peraturan ini mewajibkan penghapusan data pribadi apabila tujuan pengumpulannya terlaksana dengan baik, sehingga tidak dibutuhkan lagi jika ada kepentingan resmi. Proses penghapusan perlu dilaksanakan dengan cara yang terjamin agar data tidak dapat diakses atau digunakan kembali oleh pihak yang tidak berwenang.

Menurut Isnaeni “perlindungan hukum dibagi menjadi 2 (dua) macam yaitu perlindungan internal dan perlindungan eksternal. Perlindungan hukum *internal* dibentuk adanya kedudukan hukum yang relatif setara. Berdasarkan hak asasi manusia, masing-masing kelompok diberikan kebebasan dalam menyatakan pendapat. Sedangkan, perlindungan hukum *eksternal* ditetapkan oleh negara melalui peraturan untuk melindungi kelompok yang lebih lemah. Esensi dari peraturan perundang-undangan haruslah seimbang dan tidak memihak. Secara proposional, perlindungan hukum yang seimbang juga harus segera diberikan pada kelompok lain. Oleh karena itu, ketika kelompok yang pada awalnya kuat bisa berubah menjadi kelompok yang lemah. Sebagai ilustrasi, jika orang yang meminjam melanggar persyaratan perjanjian dari orang yang memberikan pinjaman, maka orang yang memberikan pinjaman juga perlu perlindungan hukum. (Di & Priliasari, 2023)



Gambar 1.2 Jenis Kebocoran Data

Pemaparan informasi yang bersifat rahasia, baik yang dilakukan secara sengaja (ancaman yang disengaja) maupun tidak disengaja (ancaman yang tidak disengaja), kepada pihak yang tidak memiliki izin. Kebocoran yang bersifat ancaman yang tidak disengaja terjadi karena kelalaian atau ketidaksengajaan. Faktor penyebabnya antara kelemahan lain dalam sistem keamanan data pribadi pengguna pasar online, misalnya kesalahan konfigurasi (*configure error*), enkripsi yang tidak tepat, risiko cyber espionage dan sabotase (Kurmaliasari et al., 2025).

Sebagai perlindungan hukum, penyelenggara platform digital melindungi data dengan UU *privacy policy* (kebijakan privasi), *privacy statement*, dan *privacy notice* sebagai *self regulation*. Kebijakan privasi (yang dikenal juga sebagai *Privacy Policy*, *Privacy Statement*, atau *Privacy Notice*) adalah bentuk kesepakatan antar penyedia platform digital dengan para penggunanya. Pengguna platform digital dianggap telah mengikatkan diri dengan ketentuan-ketentuan yang ada di dalam kebijakan privasi. Meskipun pengguna platform digital hanya mengunjungi website, sudah mengikatkan diri melalui kebijakan privasi (Maharani & Prakoso, 2024).

Meskipun pada awalnya belum memiliki undang-undang tunggal secara komprehensif, Indonesia telah menetapkan sejumlah peraturan sektoral yang mengatur aspek perlindungan data pribadi secara terpisah. Beberapa di antaranya tercantum dalam UU Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik (UU ITE), peraturan tentang Telekomunikasi terdapat di pasal 40 UU Nomor 30 Tahun 1999, dan peraturan tentang Keterbukaan Informasi Publik

terdapat di Pasal 6 Undang-Undang Nomor 14 Tahun 2008. Selain itu, Perlindungan Data Pribadi dalam Sistem Elektronik (Permen PDPSE) diatur oleh Peraturan Kementerian Komunikasi dan Informatika Nomor 20 Tahun. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE) mengatur perdagangan digital (*e-commerce*). UUD Negara Republik Indonesia Tahun 1945 Pasal 28 G ayat (1) menyatakan bahwa semua warga negara mempunyai kewenangan untuk melindungi diri, kerabat harga diri, dan harta bendanya. Dengan demikian, hak informasi seseorang dapat dipandang dari hak milik yang melekat pada setiap individu sebagai subjek data pribadi. Perlindungan ini mencakup seluruh tahapan pengelolaan data, mulai dari pengumpulan, penggunaan, penyimpanan, transmisi, hingga penghapusan, serta berlaku bagi seluruh individu tanpa memandang kewarganegaraan (Simarmata et al., 2024).

Sanksi dan Penegakan Hukum

Perlindungan Data Pribadi berfungsi dalam pengumpulan, pemanfaatan, hingga pengamanan data pribadi agar setiap privasi individu tetap terjamin. Di dalam UU Perlindungan Data Pribadi terdapat aturan yang menegaskan larangan penggunaan data informasi milik orang lain tanpa izin. Larangan tersebut tertuang pada Pasal 65 serta Pasal 67 ayat (1), (2), dan (3), yaitu:

- a. Orang yang berupaya dengan sengaja menolak peraturan dalam memperoleh data informasi yang bukan haknya, dengan tujuan keuntungan pribadi maka dapat menyebabkan kerugian. Orang yang melanggar ketentuan pada pasal 65 dapat dikenakan sanksi pidana kurungan mencapai 5 (lima) tahun atau dengan ganti rugi maksimal Rp 5.000.000.000,00 (lima miliar rupiah).
- b. Orang yang sengaja menolak peraturan menyatakan bahwa data informasi yang bukan haknya pada Pasal 65 ayat (2) dikenakan sanksi pidana kurungan mencapai 4 (empat) tahun atau dengan ganti rugi maksimal Rp 4.000.000.000,00 (empat miliar rupiah).
- c. Orang yang sengaja menolak peraturan menyatakan bahwa data informasi yang bukan haknya pasal 65 ayat (3) dikenakan pidana kurungan mencapai 5 (lima) tahun dengan ganti rugi sebesar Rp 5.000.000.000,00 (lima miliar rupiah).

Terkait dengan tindakan penyebaran data pribadi, apabila tindakan tersebut dilakukan secara sengaja serta bertentangan dengan ketentuan hukum, maka pelaku dapat dikenai ketentuan sebagaimana diatur dalam peraturan yang dapat menimbulkan risiko pada pasal 36. Orang yang terungkap telah melakukan pelanggaran dapat dijatuhi hukuman sesuai dengan ketentuan yang tercantum pada Pasal 48 yaitu:

- a. Orang yang melaksanakan unsur dengan benar sesuai di dalam Pasal 32 ayat (1) dihukum dengan kurungan mencapai 8 (delapan) tahun atau ganti rugi sebesar Rp2.000.000.000,00 (dua miliar rupiah).
- b. Orang yang melaksanakan unsur dengan baik sesuai di dalam Pasal 32 ayat (2) dihukum dengan kurungan mencapai 9 (sembilan) tahun atau ganti rugi sebesar Rp3.000.000.000,00 (tiga miliar rupiah).
- c. Orang yang melaksanakan unsur dengan benar sesuai pada Pasal 32 ayat (3) dihukum dengan kurungan mencapai 10 (sepuluh) tahun atau ganti rugi sebesar Rp5.000.000.000,00 (lima miliar rupiah).

Arbitrase merupakan alternatif penyelesaian sengketa melalui mekanisme nonlitigasi yang dinilai lebih efisien dan efektif dalam memberikan solusi atas perselisihan yang terjadi (Hidayat & Komarudin, 2020). Arbitrase berkaitan dengan penyalahgunaan data informasi, UU Perlindungan Data Pribadi memberikan jaminan perlindungan bagi individu yang datanya bocor. Instansi ataupun pelaku usaha dapat meminta tanggung jawab, sesuai ketentuan di dalam

Pasal 1365 Kitab Undang-Undang Hukum Perdata (KUHPerdata) jika tindakan tersebut menolok hukum, yaitu:

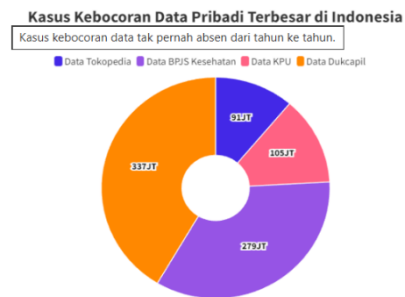
- a. Adanya suatu tindakan, baik berupa perbuatan aktif maupun kelalaian (tidak berbuat sesuatu).
- b. Tindakan yang menimbulkan risiko.
- c. Timbulnya sebab-akibat antara tindakan yang dilakukan dengan kerugian yang timbulkan.
- d. Orang yang melakukan kejahatan mengaku salah.

Metode yang paling efektif dalam penuntasan sengketa pada umumnya menggunakan arbitrase, khususnya antar pelaku usaha. Ketika para pihak telah menyepakati adanya klausul arbitrase, maka mahkama tidak berhak memeriksa sengketa tersebut. Oleh karena itu, lembaga peradilan wajib menghormati dan mengakui kewenangan arbitrase sebagai forum penyelesaian. Umumnya, arbitrase yang ditunjuk adalah individu dengan keahlian di bidang terkait, sehingga mampu memahami substansi persoalan dan berupaya memberikan solusi. Keunggulan lain dari arbitrase antara lain tingginya tingkat kerahasiaan informasi, proses persidangan tidak dipublikasikan ke ruang publik, serta efisiensi waktu yang lebih baik dibandingkan dengan proses litigasi di pengadilan (Sitta Saraya, Dkk, 2025).

Studi Kasus Kebocoran Data Pribadi Konsumen

Kasus kebocoran data pribadi konsumen telah beberapa kali terjadi, baik di sektor e-commerce maupun perbankan. Salah satu contoh yang cukup besar terjadi pada tahun 2014, ketika platform eBay mengalami insiden kebocoran data pengguna dalam skala global. Dalam sektor perbankan, kasus serupa juga sering muncul, seperti pertukaran data pribadi nasabah antar lembaga kartu kredit (*card center*) atau pemberian akses informasi nasabah kepada pihak ketiga untuk memperoleh keuntungan ekonomi melalui praktik jual beli data. Di Indonesia, beberapa pasar daring besar seperti Tokopedia, Bukalapak, dan Bhinneka juga pernah mengalami peristiwa serupa (Zaenal & Orias, 2024).

Kebocoran data yang disebabkan oleh aksi peretasan menunjukkan bahwa Tokopedia belum sepenuhnya menerapkan unsur perlindungan data pribadi, khususnya dalam mencegah penyalahgunaan informasi oleh pihak yang tidak berwenang. Kasus serupa juga pernah mengguncang dunia internasional, yakni insiden kebocoran data pengguna Facebook pada tahun 2018. Saat itu, terungkap bahwa perusahaan analisa data telah mengambil dan memanfaatkan informasi data tanpa persetujuan dari pihak bersangkutan. Informasi tersebut dimanfaatkan dalam memengaruhi opini publik. Kejadian ini memicu komentar tajam mengenai kebijakan Facebook serta menumbuhkan kerisauan global mengenai keamanan informasi pribadi pada platform media social. Di sisi lain, maraknya kebocoran data pada platform *e-commerce* di Indonesia juga menjadi ancaman serius terhadap privasi dan keamanan konsumen. Berbagai kasus tersebut memperlihatkan pentingnya komitmen perusahaan digital dalam memperkuat sistem keamanan siber dan memastikan perlindungan maksimal terhadap data pribadi penggunanya. Berikut ini merupakan sejumlah data yang menunjukkan skala dan dampak kebocoran data di Indonesia (Tia Deja Pohan & Muhammad Irwan Padli Nasution, 2023) .



Gambar 1.4 Jumlah Kebocoran Data Pribadi Yang Terjadi di Indonesia

Evaluasi terhadap penerapan UU Nomor 27 Tahun 2022 dapat mengindikasikan peraturan tersebut masih belum memberikan hasil yang optimal dalam menekan kasus pelanggaran data pribadi di Indonesia. Walaupun sudah terdapat ketentuan mengenai sanksi administratif dan pidana, tujuan untuk menimbulkan efek jera belum tercapai. Hal ini disebabkan oleh masih lemahnya penegakan hukum serta ketiadaan sistem pengawasan yang independen dan terorganisir dengan baik. Situasi ini membuat banyak lembaga, baik sektor publik maupun swasta, cenderung kurang memperhatikan atau menyepelekan risiko yang muncul akibat penyalahgunaan informasi. Sebagai perbandingan, studi mengenai penerapan GDPR di Uni Eropa menunjukkan penurunan signifikan dalam kasus pelanggaran data karena sanksi berat, seperti denda hingga €20 juta atau 4% dari pendapatan global perusahaan, serta pengawasan ketat oleh otoritas independen. Fakta ini menunjukkan bahwa regulasi yang ketat seperti yang dijalankan oleh GDPR, lebih efektif dalam melindungi informasi data pada perbandingan pendekatan oleh UU Nomor 27 Tahun 2022. Oleh karena itu, diperlukan revisi dan penguatan kebijakan di Indonesia, termasuk harmonisasi dengan standar global, guna dapat menghadapi permasalahan dalam perlindungan data di era digital yang semakin rumit (Zaenal & Orias, 2024).

Kebocoran Data Pribadi yang dialami oleh Mahasiswa

Ada beberapa hal yang terjadi terkait kebocoran data dimana objeknya mahasiswa yang sering mengalami kerugian akibat hal yang tidak diduga, adapun seperti berikut:

1. Penyalahgunaan Identitas Mahasiswa

Kebocoran data pribadi seperti nama lengkap, Nomor Induk Kependudukan (NIK), alamat tempat tinggal, nomor telepon, alamat email, hingga foto identitas dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk melakukan penyalahgunaan identitas. Dalam kasus mahasiswa, data tersebut dapat digunakan untuk mendaftarkan akun pinjaman online (pinjol), akun dompet digital, maupun layanan keuangan lainnya tanpa sepengetahuan pemilik data. Akibatnya, mahasiswa dapat menerima tagihan, ancaman penagihan, atau bahkan menghadapi permasalahan hukum atas transaksi yang tidak pernah dilakukannya. Selain menimbulkan kerugian materiil, penyalahgunaan identitas juga dapat merusak reputasi dan menimbulkan kesulitan bagi mahasiswa dalam mengakses layanan keuangan di masa depan.

2. Penipuan Melalui Telepon atau Pesan

Kebocoran data pribadi juga dapat meningkatkan risiko terjadinya penipuan melalui telepon, SMS, maupun aplikasi pesan instan. Pelaku biasanya memanfaatkan informasi yang telah diperoleh, seperti nama lengkap, nomor telepon, atau riwayat transaksi, untuk meyakinkan korban bahwa mereka merupakan pihak resmi dari kampus, bank, e-commerce, atau penyedia layanan digital lainnya. Dengan menggunakan teknik rekayasa sosial (*social engineering*), pelaku akan meminta informasi sensitif seperti kode OTP, PIN, password, atau data perbankan. Mahasiswa yang kurang memahami modus penipuan digital berpotensi menjadi korban karena

menganggap permintaan tersebut berasal dari pihak yang terpercaya. Akibatnya, pelaku dapat mengambil alih akun korban atau melakukan transaksi yang merugikan secara finansial.

3. Pembobolan Akun Digital

Mahasiswa sering kali menggunakan kombinasi alamat email dan kata sandi yang sama untuk berbagai akun digital, seperti *e-commerce*, media sosial, email akademik, hingga layanan mobile banking. Apabila data login pada salah satu platform mengalami kebocoran, pelaku dapat mencoba menggunakan kombinasi data tersebut untuk mengakses akun lainnya melalui metode yang dikenal sebagai *credential stuffing*. Jika berhasil, pelaku dapat mengambil alih berbagai akun digital milik mahasiswa, mengubah kata sandi, mengakses informasi pribadi, bahkan menggunakan akun tersebut untuk melakukan tindakan yang merugikan. Kondisi ini tidak hanya menyebabkan hilangnya akses terhadap akun penting, tetapi juga berpotensi mengganggu aktivitas akademik dan kehidupan sosial mahasiswa.

4. Kerugian Finansial

Salah satu dampak paling nyata dari kebocoran data pribadi adalah terjadinya kerugian finansial. Pelaku dapat memanfaatkan informasi pembayaran yang tersimpan dalam akun *e-commerce*, seperti data kartu debit, kartu kredit, rekening bank, maupun fasilitas *paylater* untuk melakukan transaksi tanpa izin pemilik akun. Selain itu, pelaku juga dapat menggunakan akun yang telah berhasil diretas untuk membeli barang, mentransfer saldo dompet digital, atau mengajukan pinjaman atas nama korban. Bagi mahasiswa yang umumnya memiliki keterbatasan ekonomi, kerugian finansial akibat kebocoran data dapat memberikan dampak yang sangat besar, mulai dari terganggunya kebutuhan sehari-hari hingga terhambatnya biaya pendidikan.

5. Penyebaran Informasi Pribadi

Kebocoran data pribadi juga dapat menyebabkan tersebarnya informasi pribadi mahasiswa kepada pihak-pihak yang tidak berwenang. Informasi seperti alamat tempat tinggal, nomor telepon, alamat email, riwayat pembelian, hingga kebiasaan konsumsi dapat diperjualbelikan atau dimanfaatkan untuk kepentingan komersial dan tindak kejahatan. Akibatnya, mahasiswa dapat menerima berbagai bentuk spam, iklan yang tidak diinginkan, penawaran palsu, hingga upaya penipuan yang lebih terarah karena pelaku telah mengetahui profil dan kebiasaan korban. Selain mengganggu privasi, penyebaran informasi pribadi ini juga dapat menimbulkan rasa tidak aman dan kekhawatiran dalam menggunakan layanan digital di masa mendatang.

Dari hasil observasi serta wawancara dengan objek penelitian yaitu mahasiswa universitas muhammadiyah palembang, ditemukan bahwa:



Gambar 1.5 Instagram Aisyah Rahma Di Hack oleh orang tidak dikenal

Aisyah Rahma, seorang mahasiswa aktif, mengalami kejadian yang tidak pernah ia bayangkan sebelumnya. Akun Instagram pribadinya tiba-tiba tidak dapat diakses, meskipun ia

merasa telah menjaga keamanan akun dan data pribadinya dengan baik. Aisyah mengaku tidak pernah membagikan kata sandi kepada orang lain, tidak pernah memberikan kode OTP kepada siapa pun, serta selalu berusaha berhati-hati dalam menggunakan media sosial.

Setelah mencari tahu penyebabnya, Aisyah menyadari bahwa selama ini ia sering menggunakan berbagai aplikasi e-commerce, seperti Tokopedia dan Shopee, untuk memenuhi kebutuhan sehari-hari. Ia juga menggunakan alamat email dan nomor telepon yang sama pada berbagai *platform* digital. Diduga, kebocoran atau penyalahgunaan data pribadi yang terkait dengan akun digital tersebut dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk memperoleh informasi pribadinya.

Beberapa hari sebelum akun Instagramnya diretas, Aisyah menerima sejumlah pesan dan notifikasi yang tidak biasa, termasuk SMS promosi dan upaya masuk ke akun dari perangkat yang tidak dikenalnya. Karena merasa pesan tersebut tidak penting, ia mengabaikannya. Namun, tidak lama kemudian, akun Instagram miliknya berhasil diambil alih oleh peretas. Foto profil, informasi akun, dan unggahan pribadinya diubah, sementara peretas menggunakan akun tersebut untuk menyebarkan pesan yang mengatasnamakan dirinya.

Peristiwa ini menyebabkan Aisyah mengalami kerugian tidak hanya dari segi keamanan data, tetapi juga secara psikologis. Ia merasa khawatir, kehilangan privasi, dan takut jika data pribadi lainnya juga telah disalahgunakan. Kasus yang dialami Aisyah menunjukkan bahwa meskipun seseorang merasa telah berhati-hati dalam menjaga data pribadi, penggunaan berbagai layanan digital dan e-commerce tetap memiliki risiko apabila terjadi kebocoran data atau penyalahgunaan informasi oleh pihak yang tidak bertanggung jawab. Oleh karena itu, penting bagi setiap pengguna, khususnya mahasiswa, untuk selalu meningkatkan keamanan akun digital dengan menggunakan kata sandi yang berbeda pada setiap platform, mengaktifkan autentikasi dua faktor, serta secara rutin memantau aktivitas pada akun yang dimilikinya.



Gambar 1.6 Nomor HP Rizky Spam oleh orang tidak dikenal

Rizky Putra Dewangga, seorang mahasiswa aktif, mulai merasa terganggu dengan banyaknya pesan promosi yang masuk ke nomor telepon pribadinya. Hampir setiap hari, ia menerima SMS dari berbagai pihak yang menawarkan produk dan layanan yang tidak pernah ia

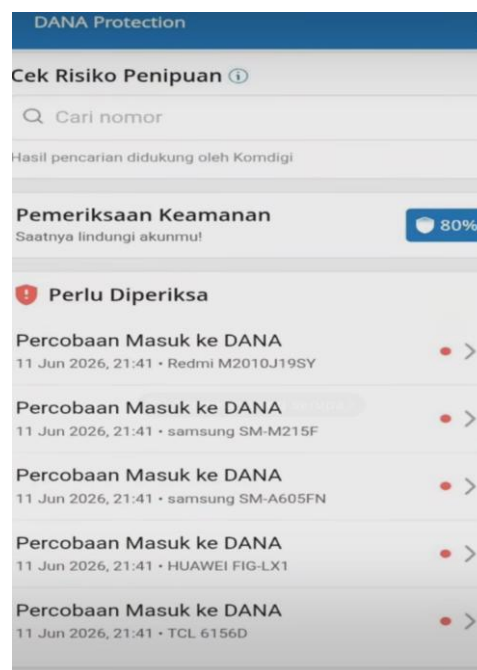
daftarkan sebelumnya. Pesan-pesan tersebut berasal dari aplikasi pinjaman online, bank digital, restoran cepat saji, hingga tempat permainan anak di pusat perbelanjaan. Jumlah pesan yang masuk semakin banyak dan berulang, sehingga mengganggu aktivitas perkuliahan dan kehidupan sehari-harinya.

Rizky merasa heran karena selama ini ia selalu berusaha menjaga keamanan data pribadinya. Ia tidak pernah membagikan nomor telepon kepada orang yang tidak dikenal, tidak pernah mengunggah informasi pribadi secara sembarangan di media sosial, serta tidak pernah memberikan kode OTP atau data sensitif lainnya kepada pihak mana pun. Menurutnya, ia telah cukup berhati-hati dalam menjaga privasi dan keamanan data pribadinya.

Rizky mengingat kembali aktivitas digital yang sering dilakukannya, Rizky menyadari bahwa ia merupakan pengguna aktif berbagai aplikasi *e-commerce*, seperti Shopee, Tokopedia, dan platform belanja online lainnya. Dalam proses pendaftaran dan transaksi, ia harus memberikan berbagai informasi pribadi, seperti nama lengkap, nomor telepon, alamat email, dan alamat tempat tinggal. Meskipun data tersebut diberikan untuk kepentingan transaksi yang sah, Rizky mulai menduga bahwa nomor teleponnya mungkin telah tersebar atau disalahgunakan oleh pihak yang tidak bertanggung jawab.

Akibat dugaan kebocoran data tersebut, nomor telepon Rizky digunakan untuk berbagai kepentingan pemasaran dan promosi. Ia menerima puluhan pesan dari aplikasi pinjaman online yang menawarkan pinjaman instan, promosi makanan dari restoran cepat saji, penawaran layanan perbankan digital, hingga iklan permainan anak di pusat perbelanjaan. Meskipun tidak menimbulkan kerugian finansial secara langsung, kondisi ini menyebabkan terganggunya privasi, menurunkan kenyamanan dalam menggunakan layanan telekomunikasi, serta meningkatkan risiko menjadi korban penipuan digital di kemudian hari.

Pengalaman yang dialami Rizky menunjukkan bahwa kebocoran atau penyalahgunaan data pribadi dapat terjadi meskipun seseorang merasa telah berhati-hati dalam menjaga informasi pribadinya. Oleh karena itu, penting bagi setiap pengguna layanan digital, khususnya mahasiswa, untuk lebih selektif dalam memberikan data pribadi, memahami kebijakan privasi aplikasi yang digunakan, serta meningkatkan kesadaran akan risiko keamanan data di era digital.



Gambar 1.7 Akun Dana Jepriansyah sedang di Hack oleh orang tidak dikenal

Jepriansyah, seorang mahasiswa aktif, mengalami kejadian yang membuatnya merasa khawatir terhadap keamanan data pribadinya. Saat membuka fitur keamanan pada aplikasi DANA, ia menemukan adanya beberapa percobaan masuk ke akun DANA miliknya dari berbagai perangkat yang tidak dikenalnya. Dalam riwayat keamanan tersebut, tercatat upaya login dari beberapa jenis perangkat berbeda dalam waktu yang hampir bersamaan. Temuan ini membuat Jepriansyah menyadari bahwa akun keuangan digitalnya telah menjadi target percobaan peretasan oleh pihak yang tidak bertanggung jawab.

Jepriansyah mengaku bahwa selama ini ia selalu berusaha menjaga keamanan data pribadinya dengan baik. Ia tidak pernah membagikan PIN, password, maupun kode OTP kepada siapa pun. Selain itu, ia juga tidak pernah mengklik tautan mencurigakan yang dikirim melalui pesan singkat, email, maupun media sosial. Ia merasa telah menerapkan berbagai langkah pencegahan untuk melindungi akun dan data pribadinya sehingga tidak menyangka bahwa akun DANA miliknya dapat menjadi sasaran percobaan peretasan.

Namun, setelah mengingat kembali aktivitas digital yang sering dilakukannya, Jepriansyah menyadari bahwa ia merupakan pengguna aktif berbagai aplikasi *e-commerce*. Ia rutin menggunakan aplikasi belanja online untuk memenuhi kebutuhan sehari-hari, mulai dari membeli perlengkapan kuliah, kebutuhan pribadi, hingga berbagai transaksi digital lainnya. Dalam proses pendaftaran dan penggunaan aplikasi *e-commerce* tersebut, ia telah memberikan berbagai informasi pribadi seperti nama lengkap, nomor telepon, alamat email, dan informasi pendukung lainnya.

Jepriansyah kemudian menduga bahwa data pribadinya kemungkinan telah tersebar atau disalahgunakan oleh pihak yang tidak bertanggung jawab. Kebocoran atau penyalahgunaan data tersebut diduga dimanfaatkan oleh pelaku untuk mencoba mengakses akun DANA miliknya. Meskipun percobaan peretasan tersebut belum berhasil karena adanya sistem keamanan tambahan pada aplikasi DANA, kejadian ini tetap menimbulkan kekhawatiran bahwa informasi pribadinya telah berada di tangan pihak lain.

Peristiwa yang dialami Jepriansyah menunjukkan bahwa risiko kebocoran data dan penyalahgunaan informasi pribadi dapat terjadi meskipun pengguna merasa telah berhati-hati dalam menjaga keamanan data. Penggunaan berbagai aplikasi digital, khususnya *e-commerce*, dapat meningkatkan risiko apabila terjadi kebocoran data atau penyalahgunaan informasi oleh pihak yang tidak bertanggung jawab. Oleh karena itu, pengguna perlu meningkatkan keamanan akun dengan menggunakan kata sandi yang kuat dan berbeda pada setiap platform, mengaktifkan autentikasi dua faktor, serta rutin memantau aktivitas keamanan pada seluruh akun digital yang dimiliki.

PENUTUP

Perlindungan data pribadi konsumen dalam transaksi *e-commerce* merupakan aspek fundamental dalam mendukung perkembangan ekonomi digital di Indonesia. Kehadiran Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah memberikan landasan hukum yang lebih komprehensif dalam menjamin hak-hak subjek data, mengatur kewajiban pelaku usaha, serta memberikan kepastian hukum terhadap pengelolaan data pribadi. Namun demikian, implementasi regulasi tersebut masih menghadapi berbagai tantangan, seperti

lemahnya penegakan hukum, belum optimalnya pengawasan, serta rendahnya kesadaran dan kepatuhan sebagian penyelenggara sistem elektronik dalam melindungi data konsumen.

Berbagai kasus kebocoran data yang terjadi pada *platform* digital, termasuk yang dialami oleh mahasiswa sebagai pengguna aktif layanan *e-commerce* dan keuangan digital, menunjukkan bahwa risiko penyalahgunaan data pribadi masih sangat tinggi. Dampak yang ditimbulkan tidak hanya berupa kerugian finansial, tetapi juga ancaman terhadap privasi, keamanan digital, dan kepercayaan masyarakat terhadap ekosistem ekonomi digital. Oleh karena itu, perlindungan data pribadi tidak dapat hanya dibebankan kepada pemerintah melalui regulasi, tetapi juga memerlukan komitmen pelaku usaha dalam menerapkan tata kelola data yang baik, penguatan sistem keamanan siber, serta peningkatan literasi dan kesadaran masyarakat dalam menjaga keamanan data pribadinya.

Pada akhirnya, keberhasilan perlindungan data pribadi di era ekonomi digital sangat bergantung pada sinergi antara regulasi yang efektif, penegakan hukum yang tegas, kepatuhan pelaku usaha, serta partisipasi aktif masyarakat. Penguatan pengawasan, harmonisasi regulasi dengan standar internasional, dan peningkatan keamanan sistem elektronik menjadi langkah strategis yang perlu dilakukan untuk mewujudkan ekosistem digital yang aman, terpercaya, dan berkelanjutan di Indonesia.

REFERENSI

- Afrizal. (2014). *Metode Penelitian Kualitatif*. Pustaka Baru Press.
- Alifia Fisilmi Kaffah & Siti Malikhatun Badriyah. (2024). Aspek Hukum Dalam Perlindungan Bisnis Era Digital Di Indonesia. *Lex Renaissance*, 9(1), 203–228. <https://doi.org/10.20885/JLR.vol9.iss1.art10>
- Anugrah, D., Andriyani, Y., Fauji, A. R., Nurohmah, A., Sumawijaya, A., Pratiwi, C. N., Kurniawati, I., Az-Zahra, K., Priatama, R. B., Susanti, R., Akbar, S. F. N., & Nugraha, E. Y. (2025). Peningkatan Perlindungan Hak Konsumen E-Commerce Bagi Masyarakat Desa Mancagar Kecamatan Garawangi Kabupaten Kuningan. *JUKEMAS: Jurnal Pengabdian Kepada Masyarakat*, 2(2), 84–91. <https://doi.org/10.60126/jukemas.v2i2.922>
- Ardika, I. W. C. (2025). Tinjauan Hukum terhadap Perlindungan Data Pribadi di Era Digital: Kasus Kebocoran Data Pengguna Layanan E-Commerce. *Indonesian Journal of Law and Justice*, 2(3), 11. <https://doi.org/10.47134/ijlj.v2i3.3601>
- Arief, A., & Risma, A. (n.d.). *Legal Protection Of Youth Consumers In E-Commerce Transactions*.
- Di, E. M. P. P., & Priliyasi, E. (2023). *Perlindungan data pribadi konsumen dalam transaksi*. 12(27), 261–279.
- Fathaniyah, L., Makbul, M., & Makhrus, M. (2023). Urgensi Perlindungan Data Pribadi pada Transaksi e-Commerce Terhadap Pembangunan Ekonomi di Indonesia. *JURNAL HUKUM EKONOMI SYARIAH*, 6(2), 77. <https://doi.org/10.30595/jhes.v0i0.17171>
- Hidayat, M. R., & Komarudin, P. (2020). Penyelesaian Sengketa Wakaf Melalui Jalur Litigasi Dan Non-Litigasi. *Al-Adl: Jurnal Hukum*, 11(2), 184. <https://doi.org/10.31602/al-adl.v11i2.1936>

- Ikhsan, M. M., Nuraeni, N., & Meiriyanti, D. (2024). Integrating Islamic Business Ethics In Labor Protection And Minimum Wage Determination In Indonesia. *Mu'amalah: Jurnal Hukum Ekonomi Syariah*, 3(1), 105. <https://doi.org/10.32332/muamalah.v3i1.8188>
- Kasus, S., & Com, E. B. (2021). *Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan Ruu Perlindungan Data Pribadi*. 5(1), 46–68.
- Khairani Alawiyah Matondang, Tia Handani, Annisa Handayani, & Fidia Wati. (2025). Etika Bisnis dalam Perlindungan Data Pribadi Konsumen di Era Bisnis Digital: Dalam Studi Literatur. *Jurnal Publikasi Sistem Informasi dan Manajemen Bisnis*, 4(3), 551–565. <https://doi.org/10.55606/jupsim.v4i3.5508>
- Kurmaliasari, A., Sari, E. P. B., Putri, H. A., Kharismawati, S. D., & Kuncoro, A. B. (2025). *Analisis Perlindungan Hukum Konsumen Dalam Transaksi Jual Beli Online Berdasarkan Perspektif Hukum Perdata Di Indonesia*. 2.
- Maharani, R., & Prakoso, A. L. (2024). Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital. *JURNAL USM LAW REVIEW*, 7(1), 333–347. <https://doi.org/10.26623/julr.v7i1.8705>
- Marjan Miharja. (2023). *Buku Ajar Metode Penelitian Hukum*. CV Cendekia Press.
- Muri, Y. (2017). *Metode Penelitian, Kuantitatif, Kualitatif, Dan Metode Gabungan*. Kencana.
- Nanda Dwi Rizkia, H. F. (2023). *Metode Penelitian Hukum (Normatif Dan Empiris)*. Penerbit Widina.
- Rasid, M. (2025). Implikasi Undang-Undang Perlindungan Data Pribadi Konsumen dalam Transaksi E-Commerce. *Jurnal Ilmu Hukum, Humaniora dan Politik*, 5(4), 3149–3158. <https://doi.org/10.38035/jihhp.v5i4.4307>
- Ridha, I., Maulana, R., Harahap, R. A., Safitri, R., Adji, R., Wirani, S., Ramadhan, S., Salim, S. A. P., Syahputra, W., & Aulia, Y. (2024). *Aspek Hukum Perlindungan Konsumen Digital*. 3(2).
- Simarmata, R., Akyuwen, R. J., & Pesulima, T. L. (2024). Perlindungan Data Pribadi Konsumen Lazada Dalam Transaksi E-Commerce. *PATTIMURA Law Study Review*, 2(1), 145–161. <https://doi.org/10.47268/palasrev.v2i1.13786>
- Sitta Saraya, Dkk. (2025). *Hukum Telematika: Regulasi, Perlindungan Data, dan Keamanan Siber*. Yayasan Tri Edukasi Ilmiah.
- Sugiyono. (2013). *Metode Penelitian Kualitatif Kuantitatif Dan R&D*. Alfabeta.
- Tia Deja Pohan & Muhammad Irwan Padli Nasution. (2023). Perlindungan Hukum Data Pribadi Konsumen Dalam Platform E Commerce. *Sammajiva: Jurnal Penelitian Bisnis dan Manajemen*, 1(3), 42–48. <https://doi.org/10.47861/sammajiva.v1i3.336>
- Yulianingsih, S., & Putra, R. K. (2024). Analisis Yuridis tentang Perlindungan Konsumen pada E-Commerce di Indonesia: Pendekatan Yuridis-Normatif. *Hakim: Jurnal Ilmu Hukum dan Sosial*, 2(4), 842–856. <https://doi.org/10.51903/hakim.v2i4.2204>
- Yuniarti, S. (2019). *Perlindungan hukum data pribadi di indonesia*. 1(1), 147–154.
- Zaenal, H. K., & Orias, M. (2024). *Urgensi Perlindungan Hukum Data Pribadi Konsumen Dalam Transaksi E-Commerce*. (4).

Editorial Office of Locus: Jurnal Konsep Ilmu Hukum (JKIH)

Medan City, North Sumatra, Indonesia.

Phone / WhatsApp Business: +62 811-620-1239

Email: support@jurnal.locusmedia.id

E-ISSN: 2809-9265 | DOI Prefix: 10.56128/jkih

Powered by Locus Media Publishing
