

BUILD ONLINE SHOP
KEAMANAN DAN ETIKA INTERNET

Dosen Pengampu :

Wartariyus, S.Kom., M.T.I.



Disusun Oleh :

Kelompok 7

Siska Septiana	(2313025054)
M. Ditto Putra Pratama	(2313035056)
Seftano Dika Karel	(2313025062)
AndraWinata Rahmadana	(2353025002)
Gading Tri Febrianto	(2353025004)

PROGRAM STUDI PENDIDIKAN TEKNOLOGI INFORMASI
FAKULTAS KEGURUAN DAN ILMU PENDIDIKAN
UNIVERSITAS LAMPUNG
2025

BAB I

1.1 Latar Belakang

Perkembangan teknologi informasi telah menghadirkan kemudahan yang signifikan bagi masyarakat, salah satunya dengan munculnya e-commerce sebagai alat untuk transaksi digital yang cepat dan efisien. Namun, dibalik kemajuan ini muncul masalah serius terkait dengan keamanan dan privasi data pribadi pengguna internet. Setiap transaksi online melibatkan pengumpulan informasi penting seperti identitas, alamat, dan data keuangan yang rentan disalahgunakan jika tidak dilindungi dengan baik.

Kasus kebocoran data yang menimpa Bukalapak pada tahun 2020 dan juga beberapa platform besar seperti Facebook dan eBay menunjukkan lemahnya sistem keamanan digital serta kurangnya kesadaran masyarakat akan pentingnya perlindungan data. Masalah keamanan data tidak hanya bisa diselesaikan melalui inovasi teknologi, tetapi juga memerlukan etika serta tanggung jawab moral dari perusahaan dalam manajemen informasi pengguna.

Perusahaan harus menjamin kerahasiaan data konsumen dan menghindari penyalahgunaan untuk tujuan bisnis tanpa izin. Pemerintah juga telah mengeluarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) untuk memperkuat perlindungan hukum terhadap informasi pribadi masyarakat. Melalui penerapan etika digital dan kepatuhan pada regulasi, diharapkan tercipta ekosistem e-commerce yang aman, transparan, dan dapat membangun kepercayaan pengguna di era digital.

1.2 Rumusan Masalah

1. Bagaimana peran etika dalam pemasaran online, khususnya terkait tanggung jawab perusahaan dalam melindungi data pribadi pengguna?
2. Bagaimana perusahaan dapat membangun kepercayaan pengguna melalui penerapan keamanan data dan etika digital dalam transaksi e-commerce?
3. Bagaimana perlindungan hukum di Indonesia menjamin keamanan dan privasi data konsumen dalam transaksi elektronik?

1.3 Tujuan

1. Untuk mengetahui dan menjelaskan peran etika digital dalam kegiatan pemasaran online, terutama dalam menjaga kerahasiaan data pengguna internet.
2. Untuk menganalisis strategi perusahaan dalam membangun kepercayaan pengguna, melalui penerapan sistem keamanan data dan transparansi penggunaan informasi pribadi.
3. Untuk memahami peran regulasi seperti Undang-Undang Perlindungan Data Pribadi (UU PDP 2022) dalam menciptakan lingkungan e-commerce yang aman, beretika, dan terpercaya.

BAB II

2.1 Kesadaran Keamanan Data di Internet

Kesadaran masyarakat mengenai perlindungan data pribadi di dunia maya saat ini masih tergolong rendah, khususnya dalam hal penggunaan layanan digital dan transaksi e-commerce. Banyak pengguna yang belum menyadari bahaya penyalahgunaan data yang mereka bagikan secara online, seperti nama, alamat, nomor telepon, hingga informasi keuangan. Dalam jurnal dijelaskan bahwa kurangnya pemahaman masyarakat mengenai pentingnya privasi digital merupakan salah satu alasan meningkatnya kasus penipuan dan kebocoran data. Banyak konsumen yang kurang berhati-hati dalam memberikan izin akses data kepada platform digital tanpa membaca syarat privasi yang ada.

Rendahnya kesadaran ini juga tampak dari kurangnya kebiasaan masyarakat dalam menjaga keamanan akun digital, seperti penggunaan kata sandi yang lemah, penyimpanan data pribadi di tempat publik, dan kecenderungan untuk membagikan informasi sensitif di media sosial. Jurnal ini menekankan bahwa perlindungan data pribadi bukan hanya menjadi tanggung jawab pemerintah dan perusahaan, tetapi juga memerlukan keterlibatan aktif masyarakat untuk menjaga diri mereka sendiri di dunia maya. Meningkatkan literasi digital menjadi langkah yang penting agar pengguna lebih paham mengenai hak dan kewajiban mereka dalam mengamankan data pribadi.

Sebagai bagian dari upaya untuk meningkatkan kesadaran tersebut, pemerintah telah mengeluarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Regulasi ini tidak hanya mengatur tanggung jawab penyelenggara sistem elektronik, tetapi juga mendorong masyarakat untuk lebih berhati-hati dan bertanggung jawab dalam memberikan data pribadi mereka. Dengan meningkatnya kesadaran individu mengenai keamanan data dan dukungan hukum yang kokoh, diharapkan dapat terwujud ekosistem digital yang lebih aman, etis, dan saling percaya antara pengguna dan penyedia layanan internet.

2.2 Privasi Dan Keamanan Data Dalam E-Commerce

Dalam lanskap digital pasca-2020, privasi dan keamanan data telah menjadi fondasi krusial sekaligus tantangan utama bagi keberlanjutan e-commerce. Peningkatan eksponensial dalam volume transaksi digital telah menjadikan platform e-commerce sebagai target utama kejahatan siber (cybercrime). Sebuah tinjauan literatur sistematis mengidentifikasi bahwa ancaman cybercrime merupakan salah satu penghambat utama dalam perkembangan bisnis e-commerce, dengan kasus-kasus signifikan terjadi di Indonesia yang melibatkan kebocoran data jutaan pengguna dari platform besar (Wibowo, Rosyidi dan Af M., 2023). Ancaman ini mencakup spektrum yang luas, mulai dari data breaches (pelanggaran data), phishing, malware, hingga berbagai bentuk penipuan (fraud) (Sari, Haryanto dan Nugroho, 2024).

Isu ini memiliki dampak langsung pada komponen bisnis paling vital: kepercayaan konsumen. Studi menunjukkan adanya hubungan positif yang signifikan antara persepsi

privasi dan kepercayaan konsumen dalam transaksi online (Irwan dan Wijayanti, 2023). Ketika terjadi insiden keamanan, dampaknya bukan hanya kerugian finansial, tetapi juga "risiko reputasi" yang dapat secara permanen merusak kepercayaan pelanggan (Sari, Haryanto dan Nugroho, 2024). Lebih lanjut, penelitian menyoroti bahwa salah satu vektor serangan paling sukses adalah mengeksploitasi "kesalahan manusia" (human error) dan rendahnya kesadaran keamanan siber (security awareness) di kalangan konsumen (Rohmah, 2022).

Sebagai respons terhadap lanskap ancaman yang kompleks ini, dua tren utama telah muncul. Pertama, adanya penekanan regulasi yang kuat. Di Indonesia, urgensi ini dijawab melalui pengesahan Undang-Undang Pelindungan Data Pribadi (UU PDP). Regulasi ini mentransformasi keamanan data dari sekadar fitur teknis menjadi kewajiban hukum yang mengikat, sejalan dengan tren global seperti GDPR di Eropa (Fitri et al., 2024).

Kedua, adopsi teknologi pertahanan canggih. Untuk melawan ancaman yang semakin terotomatisasi, platform e-commerce modern mengandalkan implementasi Kecerdasan Buatan (AI) dan Machine Learning. Teknologi ini digunakan secara proaktif untuk deteksi anomali, analisis perilaku pengguna secara real-time, dan pencegahan penipuan (Fitri et al., 2024). Tinjauan sistematis internasional juga mengkonfirmasi bahwa AI, bersama dengan teknologi seperti blockchain, dipandang sebagai solusi inti untuk memperkuat keamanan data dan membangun kembali kepercayaan dalam ekosistem e-commerce (Mishra et al., 2025).

Dengan demikian, privasi dan keamanan data di era e-commerce modern merupakan sebuah arena dinamis yang mempertemukan ancaman teknis, kerentanan psikologis pengguna, kepatuhan hukum yang ketat, dan perlombaan inovasi teknologi.

2.3 Penerapan Perlindungan Data Pribadi dan Dasar Hukumnya

Perlindungan data pribadi merupakan pilar utama dalam menciptakan ekosistem digital yang aman dan terpercaya, terutama di sektor e-commerce yang sangat bergantung pada kepercayaan konsumen. Setiap transaksi elektronik melibatkan pertukaran informasi sensitif, seperti identitas pengguna, alamat, hingga data finansial. Oleh karena itu, penerapan sistem perlindungan data yang kuat bukan hanya menjadi kebutuhan teknis, tetapi juga kewajiban hukum serta tanggung jawab etis bagi setiap penyelenggara sistem elektronik (PSE).

A. Penerapan Perlindungan Data Pribadi di Indonesia

Implementasi perlindungan data pribadi di Indonesia mulai mendapat perhatian serius seiring meningkatnya kasus kebocoran data. Pemerintah merespons fenomena ini dengan mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Regulasi ini menjadi tonggak sejarah karena merupakan payung hukum pertama di Indonesia yang secara khusus mengatur pengelolaan dan perlindungan data pribadi secara komprehensif.

UU PDP mengatur bahwa setiap pihak yang mengumpulkan dan memproses data pribadi wajib:

1. Memperoleh persetujuan eksplisit (consent) dari pemilik data sebelum mengumpulkan atau menggunakan informasi pribadinya.
2. Menjamin keamanan data pribadi dengan menerapkan langkah teknis dan organisasi yang memadai, seperti enkripsi, autentikasi berlapis, dan sistem keamanan siber yang sesuai standar.
3. Memberikan hak akses dan kontrol kepada subjek data, termasuk hak untuk mengetahui tujuan penggunaan, memperbarui, menghapus, dan menarik kembali persetujuan atas data yang telah diberikan.
4. Melaporkan insiden kebocoran data pribadi kepada otoritas dan subjek data paling lambat 3x24 jam sejak kejadian diketahui, sesuai dengan Pasal 46 UU PDP.

Ketentuan tersebut memperkuat posisi masyarakat sebagai pemilik sah data pribadinya (data subject), sementara perusahaan bertindak sebagai pengendali data (data controller) yang berkewajiban menjaga keamanan dan kerahasiaan informasi tersebut.

B. Dasar Hukum Perlindungan Data di Indonesia

Selain UU PDP 2022, penerapan perlindungan data pribadi juga didukung oleh sejumlah regulasi terkait, antara lain:

- Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE), yang mengatur kewajiban penyelenggara sistem untuk menjaga kerahasiaan, keutuhan, dan ketersediaan data elektronik.
- Peraturan Menteri Komunikasi dan Informatika (Permenkominfo) Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, yang menjadi dasar awal pengaturan teknis sebelum hadirnya UU PDP.
- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) beserta perubahannya dalam UU Nomor 19 Tahun 2016, yang menegaskan larangan penyalahgunaan data pribadi tanpa izin.

Kehadiran regulasi-regulasi tersebut menunjukkan bahwa perlindungan data di Indonesia kini berada dalam kerangka hukum yang lebih kokoh dan terintegrasi, sejalan dengan standar global seperti General Data Protection Regulation (GDPR) di Uni Eropa.

C. Tantangan Implementasi dan Kepatuhan Etis

Meskipun landasan hukumnya telah kuat, penerapan perlindungan data di lapangan masih menghadapi sejumlah tantangan, seperti rendahnya literasi digital masyarakat, kurangnya

transparansi perusahaan dalam pengelolaan data, serta lemahnya mekanisme audit dan penegakan hukum. Banyak pelaku e-commerce yang masih memandang perlindungan data sebagai beban administratif, bukan investasi jangka panjang untuk membangun kepercayaan pengguna.

Oleh karena itu, selain kepatuhan terhadap regulasi, dibutuhkan komitmen etis perusahaan untuk menempatkan privasi pengguna sebagai prioritas utama. Penerapan *privacy by design*, pelatihan keamanan siber bagi karyawan, dan komunikasi transparan mengenai kebijakan privasi merupakan langkah-langkah strategis yang dapat memperkuat kepercayaan konsumen sekaligus memperkecil risiko pelanggaran hukum.

Dengan penerapan perlindungan data pribadi yang konsisten dan berbasis etika, ekosistem e-commerce Indonesia berpotensi berkembang secara berkelanjutan — tidak hanya kompetitif secara ekonomi, tetapi juga berintegritas secara moral dan hukum.

2.4 Etika Dalam Pemasaran dan Pengelolaan Data

Etika berfungsi sebagai landasan moral dan pelengkap penting bagi kepatuhan hukum (seperti UU PDP). Etika memastikan *online shop* menjalankan bisnisnya dengan jujur, adil, dan bertanggung jawab, terutama karena mayoritas pengguna (sekitar 74,59%) di Indonesia memiliki kesadaran keamanan data yang rendah.

A. Etika dalam Pemasaran Online

Etika dalam pemasaran digital berfokus pada pembangunan kepercayaan konsumen melalui transparansi:

1. Kejujuran Total: *Online shop* wajib menghindari iklan yang menyesatkan (*misleading*). Semua informasi, mulai dari deskripsi produk hingga harga akhir (termasuk pajak dan biaya kirim), harus disajikan secara transparan di awal transaksi, tanpa ada biaya tersembunyi.
2. Kredibilitas Bukti Sosial: Penggunaan testimoni atau ulasan palsu adalah tindakan tidak etis. Perusahaan harus menjamin bahwa semua bukti sosial (*social proof*) yang ditampilkan (misalnya, ulasan, rating) adalah asli.
3. Persetujuan Penggunaan Komunikasi: Segala bentuk komunikasi pemasaran (misalnya *newsletter*) harus berdasarkan persetujuan aktif (*opt-in*) dari konsumen. Perusahaan juga harus etis dalam mengatur frekuensi pesan agar tidak mengganggu (*spamming*).

B. Etika dalam Pengelolaan Data (*Data Stewardship*)

Etika memandang data konsumen sebagai sebuah amanah yang harus dijaga, bukan hanya aset bisnis yang dapat dieksploitasi:

1. Prinsip Seperlunya (Minimalisasi Data): *Online shop* hanya boleh mengumpulkan data yang benar-benar esensial dan relevan untuk menjalankan transaksi. Pengambilan data sensitif yang tidak perlu (*data minimization*) dianggap tidak etis.
2. Tanggung Jawab Penjaga Data: Mengingat rendahnya literasi siber pengguna, perusahaan memiliki tanggung jawab etis untuk menjadi 'penjaga' data (*data steward*). Artinya, perusahaan harus secara proaktif menerapkan enkripsi dan protokol keamanan, serta bertanggung jawab penuh atas setiap kebocoran data.
3. Keadilan Penggunaan Data: Data pribadi tidak boleh dimanfaatkan untuk mengeksploitasi kerentanan konsumen, misalnya praktik diskriminasi harga (*dynamic pricing*) yang tidak transparan. Data harus digunakan secara etis untuk memberikan nilai tambah yang adil bagi konsumen.

2.5 Upaya Perusahaan Membangun Kepercayaan Pengguna

Kepercayaan pengguna merupakan elemen utama dalam kesuksesan sebuah toko online. Tanpa adanya rasa percaya, pelanggan akan ragu untuk melakukan transaksi, meskipun produk yang ditawarkan berkualitas. Oleh karena itu, perusahaan harus melakukan berbagai upaya yang sistematis untuk menumbuhkan dan mempertahankan kepercayaan tersebut.

Salah satu langkah penting adalah menampilkan testimoni dan ulasan asli dari pelanggan. Ulasan positif memberikan bukti sosial (*social proof*) bahwa toko tersebut dapat dipercaya dan telah memberikan pengalaman yang baik bagi pembeli sebelumnya. Selain itu, kebijakan pengembalian barang yang jelas dan adil juga menjadi faktor penting dalam membangun rasa aman pelanggan, karena mereka merasa memiliki perlindungan jika terjadi kesalahan dalam pengiriman atau ketidaksesuaian produk.

Perusahaan juga perlu menonjolkan identitas dan legalitas bisnis secara transparan, seperti mencantumkan alamat kantor, nomor kontak, serta izin usaha. Tindakan ini menunjukkan bahwa toko online tersebut memiliki kredibilitas dan dapat dihubungi kapan saja jika pelanggan membutuhkan bantuan. Selanjutnya, menambahkan sertifikasi keamanan seperti “Secure Site by Norton”, “Trustwave”, atau “Verified by Visa” dapat memperkuat persepsi keamanan pengguna saat melakukan transaksi online.

Selain aspek teknis, reputasi digital perusahaan juga memiliki peran besar dalam membangun kepercayaan. Respon cepat terhadap keluhan, sikap profesional di media sosial, dan konsistensi dalam menjaga komunikasi yang jujur serta transparan dapat meningkatkan kepercayaan pelanggan terhadap brand. Dengan kata lain, kepercayaan tidak hanya dibangun melalui sistem yang aman, tetapi juga melalui interaksi yang etis dan berkualitas antara perusahaan dan pengguna.

Kesimpulan

Perkembangan e-commerce memberikan kemudahan dalam transaksi digital, namun juga menghadirkan risiko kebocoran dan penyalahgunaan data pribadi. Kesadaran masyarakat terhadap keamanan data masih rendah, sehingga perlu ditingkatkan melalui edukasi dan literasi digital.

Keamanan dan etika menjadi faktor penting dalam membangun kepercayaan konsumen. Perusahaan harus menjaga privasi pengguna, bersikap transparan, dan jujur dalam promosi. Etika digital memastikan data konsumen digunakan dengan bertanggung jawab, bukan untuk kepentingan bisnis semata.

Dengan penerapan UU Perlindungan Data Pribadi (UU PDP No. 27 Tahun 2022), pemerintah memperkuat perlindungan hukum terhadap pengguna internet. Jika kesadaran masyarakat, keamanan sistem, dan etika digital dijalankan bersama, maka ekosistem e-commerce yang aman, etis, dan terpercaya dapat terwujud di Indonesia.

DAFTAR PUSTAKA

Fitri, N., Zulfadli, Z., Abdullah, A. dan Fahmi, M. (2024). 'URGENCY OF LEGAL PERSONAL DATA PROTECTION IN E-COMMERCE TRANSACTIONS INVOLVING ARTIFICIAL INTELLIGENCE', *Walisongo Law Review*, 6(1), hh. 135-156.

Irwan, A.Z. dan Wijayanti, R.A.R. (2023). 'The Relationship between E-Commerce Consumer Privacy and Trust on Online Transactions', *LIAISON JOURNAL OF BEST*, 2(1), hh. 1-13.

Mishra, A., Reddy, K.S., Shukla, V. dan Sharma, R. (2025). 'Data protection and privacy in e-commerce environment: Systematic review', *GSC Advanced Research and Reviews*, 14(1), hh. 120-130.

Rohmah, N. (2022). *Upaya Membangun Kesadaran Keamanan Siber pada Konsumen E-commerce di Indonesia*. Kudagang: Jurnal, Esai, dan Gagasan.

Sari, D.P., Haryanto, T. dan Nugroho, A. (2024). 'ANALISIS KEAMANAN SISTEM INFORMASI PADA PERUSAHAAN E-COMMERCE DI INDONESIA', *Jurnal Ilmu Ekonomi, Pendidikan dan Teknik*, 1(3), hh. 68-75.

Wibowo, A., Rosyidi, M. dan Af M. (2023). 'ANCAMAN CYBERCRIME DAN PERAN CYBERSECURITY PADA E-COMMERCE: SYSTEMATIC LITERATURE REVIEW', JURSIMA (Jurnal Sistem Informasi dan Manajemen), 11(1), hh. 110-119.

Laudon, K. C., & Traver, C. G. (2022). *E-commerce 2022: Business, Technology, and Society*. Pearson Education.

Kominfo.go.id – Artikel: “Tips Aman Bertransaksi Online”.

OJK.go.id – Edukasi Konsumen: “Perlindungan Konsumen dalam Transaksi Elektronik”.

Laudon, K. C., & Traver, C. G. (2022). *E-commerce 2022: Business, Technology, and Society*. Pearson Education.

Rohmah, N. (2022). Upaya Membangun Kesadaran Keamanan Siber pada Konsumen E-commerce di Indonesia. *Kudagang: Jurnal, Esai, dan Gagasan*.