



Analisis Yuridis Perlindungan Data Pribadi Sebagai Hak Privasi dalam Transaksi E-Commerce di Indonesia

Driva Megantara¹, Riska Arianti², Amanda Istiana Mutiawati³

Email : Driva@univbanten.ac.id, Riska@univbanten.ac.id, Amanda@univbanten.ac.id

¹ Fakultas Hukum Universitas Banten

Jl. Kiara No.7 Walantaka Serang-Banten, 42183, ² Fakultas Hukum Universitas Banten

Jl. Kiara No.7 Walantaka Serang-Banten, 42183

Publish: 6 Maret 2025

ABSTRACT:

Digital transformation has fundamentally reshaped business transactions, particularly through e-commerce platforms. While this transformation offers significant opportunities for efficiency and market expansion, it simultaneously presents serious challenges concerning the protection of consumers' personal data. Personal data processed in electronic transactions—such as identity, address, and financial information—are often misused due to weak regulations, low compliance among electronic system providers, and limited public awareness. This study aims to analyze the protection of personal data as a privacy right within e-commerce transactions in Indonesia, with a focus on the relevance of Law No. 27 of 2022 on Personal Data Protection, Law No. 11 of 2008 on Electronic Information and Transactions (as amended), and other sectoral regulations. This research adopts normative legal methods with statutory, conceptual, and comparative approaches. Data were collected through literature reviews of statutes, legal doctrines, and both national and international regulations. The findings reveal that although Indonesia has established legal instruments explicitly regulating privacy rights and personal data protection, their implementation faces multiple challenges, ranging from weak law enforcement and overlapping regulations to the limited capacity of supervisory institutions. Personal data protection is not yet fully recognized as an inherent fundamental human right, leaving consumers vulnerable to data misuse.

The study concludes that personal data protection in e-commerce must be regarded as an inseparable part of constitutional privacy rights. Therefore, regulatory harmonization, improved digital literacy, and the strengthening of an independent supervisory authority are urgently needed to ensure that the principles of accountability, transparency, and security are effectively implemented in e-commerce practices. In doing so, personal data protection can serve as a foundational pillar for creating a safe, fair, and sustainable electronic transaction ecosystem in Indonesia.

Keywords: Personal data protection, privacy rights, electronic transactions, e-commerce, Indonesian law.

ABSTRAK

Transformasi digital telah membawa perubahan fundamental dalam pola transaksi bisnis, khususnya melalui platform *e-commerce*. Perubahan ini membuka peluang besar bagi efisiensi perdagangan, tetapi sekaligus menimbulkan tantangan serius terkait perlindungan data pribadi konsumen. Data pribadi yang diproses dalam transaksi elektronik, seperti identitas, alamat, hingga informasi finansial, sering kali disalahgunakan karena lemahnya regulasi, rendahnya kepatuhan penyelenggara sistem elektronik, serta minimnya kesadaran masyarakat. Penelitian ini bertujuan untuk menganalisis perlindungan data pribadi sebagai hak privasi konsumen dalam transaksi *e-commerce* di Indonesia, dengan menekankan relevansi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, serta regulasi sektoral terkait. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan, konseptual, dan komparatif. Data diperoleh melalui studi kepustakaan terhadap literatur, doktrin, dan regulasi baik nasional maupun internasional. Hasil penelitian menunjukkan bahwa meskipun Indonesia telah memiliki instrumen hukum yang secara eksplisit mengatur hak atas privasi dan perlindungan data pribadi, implementasinya masih menghadapi berbagai hambatan, mulai dari lemahnya penegakan hukum, tumpang tindih regulasi, hingga terbatasnya kapasitas lembaga pengawas. Perlindungan data pribadi belum sepenuhnya dipahami sebagai bagian dari hak asasi manusia yang fundamental, sehingga

konsumen tetap berada pada posisi yang rentan terhadap penyalahgunaan data. Penelitian ini menyimpulkan bahwa perlindungan data pribadi dalam transaksi *e-commerce* harus dipandang sebagai hak privasi yang melekat pada setiap individu dan dijamin secara konstitusional. Oleh karena itu, diperlukan harmonisasi regulasi, peningkatan literasi digital masyarakat, serta penguatan lembaga pengawas independen agar prinsip *accountability*, *transparency*, dan *security* benar-benar terimplementasi dalam praktik *e-commerce*. Dengan demikian, ke depan perlindungan data pribadi dapat menjadi fondasi utama bagi terwujudnya ekosistem transaksi elektronik yang aman, adil, dan berkelanjutan di Indonesia.

Kata kunci: Perlindungan data pribadi, hak privasi, transaksi elektronik, e-commerce, hukum Indonesia.

1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi dalam dua dekade terakhir telah membawa perubahan yang signifikan dalam hampir seluruh aspek kehidupan manusia. Perubahan tersebut terlihat secara nyata dalam sektor ekonomi, khususnya melalui hadirnya perdagangan elektronik atau *electronic commerce* (e-commerce). E-commerce tidak hanya mengubah pola transaksi konvensional menjadi digital, tetapi juga melahirkan ekosistem ekonomi baru yang lebih terbuka, efisien, dan dinamis.

Data yang dirilis oleh Google, Temasek, dan Bain & Company (2022) menunjukkan bahwa nilai ekonomi digital di kawasan Asia Tenggara mencapai lebih dari USD 200 miliar pada tahun 2022, dan Indonesia menyumbang porsi terbesar, yaitu sekitar 40% dari total nilai tersebut. Fakta ini menegaskan bahwa Indonesia merupakan pasar digital terbesar di kawasan, sekaligus menempatkan negara ini sebagai episentrum perkembangan e-commerce di Asia Tenggara (Google, Temasek, & Bain, 2022).

Pesatnya perkembangan e-commerce juga menimbulkan tantangan baru dalam aspek hukum, khususnya perlindungan terhadap data pribadi konsumen. Transaksi dalam e-commerce

menuntut konsumen untuk menyerahkan berbagai informasi personal, mulai dari nama, alamat, nomor telepon, hingga data finansial seperti nomor rekening dan kartu kredit. Informasi tersebut bersifat sangat sensitif karena dapat dimanfaatkan secara ilegal untuk berbagai kejahatan siber, termasuk penipuan, pencurian identitas, hingga *phishing*. Data pribadi konsumen yang seharusnya hanya digunakan untuk kepentingan transaksi, sering kali disalahgunakan oleh pihak ketiga tanpa sepengetahuan maupun persetujuan pemilik data (Nasution, 2018).

Perlindungan data pribadi sebagai hak privasi memiliki kedudukan yang fundamental dalam kerangka hak asasi manusia. Konstitusi Indonesia, melalui Pasal 28G ayat (1) UUD 1945, secara tegas menjamin bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada di bawah kekuasaannya.

Hak ini secara konseptual mencakup perlindungan terhadap data pribadi, yang dalam konteks digital menjadi sangat krusial. Lebih jauh lagi, Pasal 28J ayat (1) UUD 1945 menekankan bahwa dalam menjalankan hak dan kebebasannya, setiap orang wajib tunduk pada pembatasan yang ditetapkan dengan undang-undang, sehingga perlindungan data pribadi dalam transaksi e-commerce harus diatur secara tegas dalam norma hukum positif (Asshiddiqie, 2006).

Kasus-kasus kebocoran data pribadi yang terjadi di Indonesia semakin mempertegas urgensi perlindungan hukum. Misalnya, pada tahun 2020 publik dihebohkan oleh dugaan kebocoran data 91 juta pengguna Tokopedia yang diperjualbelikan di forum gelap. Kasus serupa juga menimpa Bukalapak, di mana sekitar 13 juta data pengguna dilaporkan bocor dan diakses secara ilegal. Bahkan, pada tahun 2021, data 279 juta penduduk Indonesia yang berasal dari BPJS Kesehatan dilaporkan bocor dan diperjualbelikan di forum daring internasional.

Kasus-kasus tersebut menunjukkan bahwa data pribadi masyarakat Indonesia sangat rentan, dan regulasi yang ada belum sepenuhnya mampu memberikan perlindungan yang memadai (Kompas, 2021).

Regulasi terkait perlindungan data pribadi di Indonesia sebenarnya telah mengalami perkembangan. Sebelum lahirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), ketentuan mengenai perlindungan data pribadi tersebar di berbagai peraturan sektoral, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya (UU ITE), Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE), dan Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Namun, regulasi tersebut dinilai parsial, tidak komprehensif, dan belum mampu menjawab kompleksitas permasalahan yang muncul dalam ekosistem e-commerce.

Lahirnya UU PDP diharapkan dapat menjadi *landmark regulation* yang mampu mengisi kekosongan hukum sekaligus memberikan standar perlindungan yang jelas, menyeluruh, dan setara dengan praktik internasional (Simanjuntak, 2022).

Di tingkat global, perlindungan data pribadi dalam transaksi elektronik telah lama menjadi perhatian serius. Uni Eropa, misalnya, telah mengadopsi General Data Protection Regulation (GDPR) sejak 2018 yang memberikan standar perlindungan data paling komprehensif di dunia. Regulasi ini tidak hanya berlaku bagi entitas di dalam Uni Eropa, tetapi juga bagi entitas di luar Uni Eropa yang memproses data warga Eropa.

Dengan demikian, GDPR menjadi instrumen hukum transnasional yang secara langsung memengaruhi praktik e-commerce global (Voigt & Von dem Bussche, 2017). Indonesia, sebagai bagian dari komunitas global, tidak dapat mengabaikan standar internasional ini, terutama mengingat sifat lintas batas dari transaksi e-commerce.

Selain aspek regulasi, perlindungan data pribadi dalam e-commerce juga menyangkut isu kepercayaan konsumen (*consumer trust*). Dalam konteks perdagangan elektronik, kepercayaan merupakan faktor determinan yang memengaruhi keputusan pembelian. Konsumen yang merasa aman terhadap perlindungan data pribadinya akan lebih cenderung untuk bertransaksi secara daring. Sebaliknya, tingginya risiko kebocoran data akan menurunkan tingkat kepercayaan konsumen dan berpotensi menghambat pertumbuhan e-commerce. Oleh karena itu, perlindungan data pribadi tidak hanya berimplikasi pada aspek hak asasi manusia dan hukum, tetapi juga memiliki dimensi ekonomi yang sangat signifikan (Pavlou, 2003).

Dengan melihat kompleksitas

persoalan tersebut, maka analisis yuridis terhadap perlindungan data pribadi sebagai hak privasi dalam transaksi e-commerce di Indonesia menjadi penting untuk dilakukan. Analisis ini tidak hanya bertujuan untuk memetakan kerangka hukum positif yang berlaku, tetapi juga mengevaluasi efektivitasnya dalam memberikan perlindungan nyata bagi konsumen. Lebih jauh lagi, penelitian ini juga dimaksudkan untuk memberikan kontribusi akademis dalam pengembangan hukum perlindungan data di Indonesia, sehingga mampu menjawab tantangan era digital sekaligus melindungi hak-hak fundamental warga negara.

2. Tinjauan Teoritis

2.1. Konsep Hak Privasi dalam Hukum

Hak privasi merupakan salah satu hak fundamental yang lahir dari pengakuan terhadap martabat manusia. Secara historis, istilah *privacy* pertama kali dipopulerkan oleh Warren dan Brandeis dalam artikel klasik mereka "The Right to Privacy" yang diterbitkan di Harvard Law Review pada tahun 1890. Mereka mendefinisikan privasi sebagai "the right to be let alone," yaitu hak seseorang untuk dibiarkan sendiri dan bebas dari intervensi pihak lain. Sejak saat itu, hak privasi berkembang sebagai bagian integral dari hak asasi manusia yang mendapatkan pengakuan di berbagai instrumen hukum internasional maupun nasional (Warren & Brandeis, 1890).

Dalam konteks hukum Indonesia, hak privasi secara implisit diakui dalam Pasal 28G ayat (1) UUD 1945 yang menyebutkan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda. Meskipun tidak secara eksplisit menggunakan istilah "privasi," norma konstitusi ini telah dipahami mencakup

perlindungan atas informasi personal individu. Mahkamah Konstitusi dalam beberapa putusannya juga menegaskan bahwa hak atas privasi merupakan bagian dari hak asasi manusia yang tidak dapat dikurangi dalam keadaan apa pun (*non-derogable rights*). Dengan demikian, perlindungan data pribadi sebagai perwujudan konkret dari hak privasi memiliki dasar yang kokoh dalam hukum konstitusi Indonesia (Asshiddiqie, 2006).

Di tingkat internasional, hak privasi diatur secara eksplisit dalam Pasal 12 *Universal Declaration of Human Rights* (UDHR) 1948 dan Pasal 17 *International Covenant on Civil and Political Rights* (ICCPR) 1966. Kedua instrumen ini menegaskan bahwa tidak seorang pun boleh diganggu urusan pribadinya, keluarganya, rumahnya, maupun surat-menyuratnya, serta setiap orang berhak atas perlindungan hukum terhadap gangguan atau serangan semacam itu. Indonesia sebagai negara pihak ICCPR memiliki kewajiban hukum untuk menghormati, melindungi, dan memenuhi hak privasi warganya, termasuk dalam konteks perlindungan data pribadi di era digital (Nowak, 2005).

2.2. Data Pribadi Sebagai Objek Pelindungan Hukum

Data pribadi dapat diartikan sebagai setiap informasi yang dapat digunakan untuk mengidentifikasi seseorang, baik secara langsung maupun tidak langsung. Menurut Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, data pribadi dibagi menjadi dua kategori, yaitu data pribadi yang bersifat umum (misalnya nama, jenis kelamin, kewarganegaraan) dan data pribadi yang bersifat spesifik (misalnya data kesehatan, biometrik, genetika, orientasi seksual, pandangan politik, catatan keuangan, hingga data anak). Kategorisasi ini penting karena menentukan tingkat perlindungan hukum yang diberikan terhadap masing-masing jenis data.

Dalam teori hukum, data pribadi dapat dipandang sebagai perpanjangan dari diri seseorang (*extension of personality*). Oleh karena

itu, pelanggaran terhadap perlindungan data pribadi tidak hanya menimbulkan kerugian material, tetapi juga melanggar hak moral individu. Hal ini sejalan dengan konsep *informational self-determination* yang berkembang di Jerman, yaitu hak individu untuk menentukan sendiri kapan, bagaimana, dan sejauh mana data pribadinya digunakan atau dipublikasikan (Westin, 1967).

Prinsip ini menegaskan bahwa pengendalian data pribadi seharusnya berada di tangan subjek data, bukan pada pihak ketiga. Namun, dalam praktik e-commerce, sering kali subjek data kehilangan kendali atas informasi pribadinya karena adanya praktik *data harvesting*, *profiling*, hingga *targeted advertising* yang dilakukan tanpa persetujuan eksplisit. Fenomena ini menimbulkan kekhawatiran serius mengenai pelanggaran hak privasi konsumen (Tene & Polonetsky, 2012).

2.3. Transaksi E-Commerce dan Risiko Kebocoran Data

E-commerce sebagai bentuk transaksi modern memiliki karakteristik yang berbeda dengan perdagangan konvensional. Transaksi dilakukan secara daring dengan melibatkan sistem elektronik sebagai sarana utama. Dalam transaksi semacam ini, data pribadi konsumen merupakan komoditas yang bernilai tinggi. Platform e-commerce mengumpulkan data konsumen tidak hanya untuk kepentingan transaksi, tetapi juga untuk keperluan analisis perilaku konsumen, periklanan, hingga monetisasi data.

Masalah muncul ketika data tersebut tidak dikelola secara aman. Risiko kebocoran data menjadi semakin tinggi karena adanya serangan siber, lemahnya sistem keamanan, maupun kelalaian pengelola sistem. Laporan dari

DataReportal (2022) menyebutkan bahwa Indonesia mengalami lebih dari 11 juta percobaan serangan siber pada tahun 2021, sebagian besar ditujukan kepada platform e-commerce dan layanan finansial. Tingginya angka serangan ini menunjukkan bahwa data pribadi konsumen berada dalam kondisi rawan, sehingga diperlukan instrumen hukum yang tegas dan efektif untuk memberikan perlindungan.

Selain faktor eksternal berupa serangan siber, terdapat pula faktor internal berupa penyalahgunaan data oleh penyelenggara sistem elektronik. Misalnya, beberapa platform e-commerce diduga menjual data konsumen kepada pihak ketiga untuk kepentingan periklanan tanpa persetujuan yang sah. Praktik semacam ini bertentangan dengan prinsip perlindungan data pribadi yang mensyaratkan adanya persetujuan eksplisit (*consent*) dari pemilik data. Tanpa adanya regulasi yang kuat dan mekanisme pengawasan yang efektif, hak privasi konsumen dalam e-commerce akan senantiasa berada dalam posisi rentan (Nasution, 2018).

2.4. Teori Pelindungan Konsumen dan Hubungan dengan Data Pribadi

Pelindungan konsumen merupakan kerangka hukum yang relevan untuk membahas isu data pribadi dalam transaksi e-commerce. Menurut Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, konsumen memiliki hak atas kenyamanan, keamanan, dan keselamatan dalam mengonsumsi barang dan/atau jasa. Dalam konteks e-commerce, perlindungan data pribadi dapat dimasukkan dalam kategori hak atas keamanan dan keselamatan, mengingat kebocoran data dapat menimbulkan kerugian material maupun immaterial.

Dari perspektif teori hukum, perlindungan konsumen dapat dipahami sebagai upaya negara untuk mengoreksi ketidakseimbangan posisi tawar antara pelaku usaha dan konsumen. Pelaku usaha, dalam hal ini platform e-commerce, memiliki akses dan kontrol yang lebih besar terhadap data

konsumen. Tanpa regulasi yang memadai, konsumen akan selalu berada dalam posisi lemah. Oleh karena itu, perlindungan data pribadi sebagai bagian dari perlindungan konsumen menjadi sangat penting untuk menjaga keseimbangan tersebut (Az. Nasution, 2002).

Lebih jauh lagi, hubungan antara perlindungan konsumen dan perlindungan data pribadi juga dapat dilihat dari aspek kepercayaan (*trust*). Konsumen yang merasa aman dengan perlindungan datanya akan lebih percaya untuk melakukan transaksi daring. Sebaliknya, ketidakamanan data akan menurunkan kepercayaan konsumen dan pada akhirnya merugikan pertumbuhan industri e-commerce itu sendiri. Dengan demikian, perlindungan data pribadi bukan hanya isu hukum, tetapi juga memiliki implikasi langsung terhadap keberlanjutan bisnis e-commerce (Pavlou, 2003).

2.5. Perbandingan Hukum Internasional: GDPR Sebagai Model

General Data Protection Regulation (GDPR) yang berlaku di Uni Eropa sejak 2018 sering disebut sebagai regulasi perlindungan data pribadi paling komprehensif di dunia. GDPR mengatur secara rinci mengenai prinsip-prinsip pengolahan data, hak-hak subjek data, kewajiban pengendali dan pemroses data, serta mekanisme sanksi bagi pelanggaran. Salah satu prinsip utama GDPR adalah *lawfulness, fairness, and transparency*, yang menekankan bahwa setiap pemrosesan data harus dilakukan secara sah, adil, dan transparan kepada subjek data (Voigt & Von dem Bussche, 2017).

Indonesia, melalui UU PDP 2022, banyak mengadopsi prinsip serupa, meskipun dengan adaptasi yang sesuai dengan konteks nasional. Misalnya, kewajiban notifikasi kepada subjek data dalam hal terjadi kebocoran, serta pengakuan atas hak-hak subjek data seperti hak akses, hak perbaikan, dan hak

penghapusan. Namun, tantangan utama di Indonesia terletak pada aspek implementasi, mengingat masih terbatasnya kapasitas kelembagaan dan kesadaran masyarakat terhadap pentingnya perlindungan data pribadi.

Oleh karena itu, kajian perbandingan hukum dengan GDPR penting untuk memberikan perspektif kritis terhadap kelemahan dan kekuatan regulasi Indonesia (Simanjuntak, 2022).

2.6. Kerangka Teoritis

Berdasarkan uraian di atas, penelitian ini menggunakan beberapa kerangka teoritis utama. Pertama, teori hak privasi yang menekankan perlindungan individu dari intervensi yang tidak sah terhadap informasi pribadinya. Kedua, teori perlindungan konsumen yang menjelaskan pentingnya intervensi negara untuk melindungi konsumen dalam transaksi asimetris, termasuk dalam konteks e-commerce. Ketiga, teori regulasi modern yang menekankan perlunya regulasi adaptif terhadap perkembangan teknologi, di mana UU PDP dan instrumen hukum terkait harus mampu mengikuti dinamika e-commerce yang berkembang pesat.

Dengan menggunakan kerangka teoritis tersebut, penelitian ini diharapkan dapat memberikan analisis yuridis yang komprehensif mengenai perlindungan data pribadi sebagai hak privasi dalam transaksi e-commerce di Indonesia, serta menawarkan rekomendasi normatif maupun praktis bagi penguatan perlindungan hukum di masa depan.

3. Metode Penelitian

3.1. Pendekatan Penelitian

Penelitian ini merupakan penelitian hukum normatif (yuridis normatif) dengan pendekatan kualitatif. Penelitian hukum normatif dipilih karena objek utama penelitian adalah norma hukum yang berlaku, baik yang tertulis dalam peraturan perundang-undangan maupun dalam prinsip-prinsip hukum yang

hidup dalam masyarakat.

Fokus penelitian ini adalah pada perlindungan data pribadi sebagai hak privasi dalam transaksi e-commerce di Indonesia, sehingga analisis akan diarahkan pada bagaimana hukum positif Indonesia merespons perkembangan e-commerce serta implikasinya terhadap pemenuhan hak asasi manusia, khususnya hak privasi (Soekanto & Mamudji, 2003).

Selain itu, penelitian ini juga menggunakan pendekatan konseptual (*conceptual approach*) dan perbandingan hukum (*comparative approach*). Pendekatan konseptual digunakan untuk membedakan konsep hak privasi, data pribadi, dan perlindungan konsumen dalam kerangka hukum nasional maupun internasional. Sedangkan pendekatan perbandingan digunakan untuk mengkaji praktik perlindungan data pribadi di yurisdiksi lain, seperti Uni Eropa dengan GDPR, Amerika Serikat dengan model *sectoral approach*, dan Jepang dengan *Act on the Protection of Personal Information* (APPI). Pendekatan ini memungkinkan analisis yang lebih komprehensif dengan melihat praktik terbaik (*best practices*) di tingkat global sebagai rujukan bagi pengembangan hukum di Indonesia (Marzuki, 2005).

Dalam penelitian hukum, pendekatan yang digunakan menentukan arah dan keluasan analisis. Penelitian ini menggunakan beberapa pendekatan, yaitu:

1. **Pendekatan Perundang-undangan (Statute Approach)**

Penelitian ini menelaah berbagai peraturan perundang-undangan yang relevan, mulai dari UUD 1945, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, PP Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, hingga Undang-Undang Nomor 8

Tahun 1999 tentang Perlindungan Konsumen. Pendekatan ini penting untuk mengetahui sejauh mana hukum positif di Indonesia mengatur perlindungan data pribadi dalam e-commerce.

2. **Pendekatan Konseptual (Conceptual Approach)**

Digunakan untuk memahami konsep hak privasi, hak atas data pribadi, dan prinsip perlindungan konsumen dalam literatur hukum. Konsep-konsep ini kemudian dikaitkan dengan praktik e-commerce untuk memberikan kerangka teoretis yang lebih utuh.

3. **Pendekatan Kasus (Case Approach)**

Beberapa kasus kebocoran data di Indonesia, seperti kasus Tokopedia, Bukalapak, dan BPJS Kesehatan, digunakan sebagai bahan analisis. Pendekatan ini memberikan gambaran empiris mengenai kelemahan sistem hukum yang ada, sekaligus menunjukkan urgensi perlindungan data pribadi yang lebih kuat.

4. **Pendekatan Perbandingan (Comparative Approach)**

Digunakan untuk mengkaji regulasi perlindungan data pribadi di negara lain, khususnya Uni Eropa, Amerika Serikat, dan Jepang. Tujuannya adalah untuk memberikan perspektif komparatif yang dapat memperkaya analisis normatif dan menawarkan rekomendasi bagi pembaruan hukum di Indonesia.

3.2. Sumber Data

Penelitian ini menggunakan data sekunder sebagai sumber utama, yang terdiri dari:

1. **Bahan Hukum Primer**, yaitu peraturan perundang-undangan yang mengatur tentang perlindungan data pribadi, privasi, dan transaksi elektronik di Indonesia. Termasuk di dalamnya UUD 1945, UU PDP 2022, UU ITE, PP PSTE, dan UU Perlindungan Konsumen.

2. **Bahan Hukum Sekunder**, berupa literatur hukum, artikel jurnal, buku teks, laporan penelitian, serta artikel ilmiah internasional yang membahas tentang privasi, perlindungan data pribadi, dan regulasi e-commerce.
3. **Bahan Hukum Tersier**, yaitu kamus hukum, ensiklopedia, laporan media, dan sumber daring resmi yang mendukung analisis penelitian.

3.3. Teknik Pengumpulan Data

Data sekunder diperoleh melalui studi kepustakaan (*library research*). Proses ini dilakukan dengan menelusuri berbagai sumber akademik, baik cetak maupun daring. Pencarian literatur internasional dilakukan melalui database jurnal bereputasi seperti JSTOR, HeinOnline, Scopus, dan SpringerLink, sedangkan literatur nasional diperoleh dari jurnal hukum Indonesia yang terakreditasi. Selain itu, laporan resmi dari lembaga pemerintah seperti Kementerian Komunikasi dan Informatika, Otoritas Jasa Keuangan, serta Badan Siber dan Sandi Negara juga digunakan sebagai referensi.

3.4. Teknik Analisis Data

Data yang diperoleh dianalisis dengan metode analisis kualitatif. Analisis dilakukan melalui tiga tahap:

1. **Reduksi Data** – memilah data yang relevan dengan fokus penelitian, yaitu perlindungan data pribadi dalam e-commerce.
2. **Penyajian Data** – menyusun data dalam kerangka narasi hukum yang sistematis, menghubungkan teori, norma, dan kasus.
3. **Penarikan Kesimpulan** – menyimpulkan hasil analisis dengan memperhatikan keterkaitan antara norma hukum, teori hak privasi, dan praktik perlindungan data di Indonesia maupun negara lain.

Dalam konteks penelitian hukum, analisis kualitatif berarti tidak sekadar mendeskripsikan peraturan, tetapi juga mengevaluasi efektivitas dan konsistensinya, serta menilai apakah hukum yang berlaku sesuai dengan prinsip-prinsip keadilan dan perlindungan hak asasi manusia (Marzuki, 2005).

3.5. Keabsahan Data

Untuk menjaga validitas dan reliabilitas penelitian, dilakukan langkah-langkah berikut:

- **Triangulasi sumber**, yaitu membandingkan data dari regulasi, buku, jurnal, dan laporan lembaga resmi.
- **Konsistensi analisis**, yaitu melakukan cross-check antarpeneliti atau pembimbing untuk memastikan interpretasi yang obyektif.
- **Audit trail**, yaitu mendokumentasikan proses seleksi literatur, kriteria inklusi-eksklusi, serta catatan analisis agar dapat direplikasi oleh peneliti lain.

4. Hasil dan Pembahasan

4.1 Hak Privasi dan Perlindungan Data Pribadi sebagai Hak Konstitusional

Hak privasi merupakan bagian dari hak asasi manusia yang dijamin dalam konstitusi Indonesia. Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda. Ketentuan ini memberikan dasar normatif bahwa data pribadi sebagai bagian dari identitas seseorang melekat pada ranah hak privasi yang wajib dilindungi negara (Asshiddiqie, 2006).

Perkembangan teknologi informasi membuat konsep hak privasi semakin kompleks. Jika pada awalnya hak privasi dipahami sebatas perlindungan fisik dan kehidupan pribadi dari intervensi, kini berkembang menjadi perlindungan informasi pribadi dari akses ilegal, pengumpulan, dan

penyalahgunaan. Dalam konteks e-commerce, data pribadi konsumen seperti nama, alamat, nomor telepon, rekening bank, hingga jejak digital (digital footprint) seringkali menjadi objek yang rentan dieksploitasi. Oleh sebab itu, jaminan perlindungan hukum terhadap hak privasi dalam transaksi elektronik merupakan wujud konkret perlindungan konstitusional.

4.2 Perlindungan Data Pribadi dalam Undang-Undang di Indonesia

Kerangka hukum di Indonesia terkait perlindungan data pribadi baru mendapatkan penguatan setelah lahirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Sebelumnya, pengaturan masih tersebar dalam berbagai regulasi sektoral, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya, serta Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

UU PDP mengatur prinsip-prinsip dasar perlindungan data pribadi, antara lain prinsip persetujuan, keterbukaan, tujuan spesifik, akurasi, keamanan, dan tanggung jawab. Dengan demikian, penyelenggara sistem elektronik (PSE) termasuk pelaku e-commerce wajib mengelola data konsumen secara sah dan bertanggung jawab. Namun, dalam praktiknya, masih banyak penyelenggara e-commerce yang melakukan pengumpulan dan pemrosesan data tanpa persetujuan eksplisit dari konsumen, atau dengan klausul baku yang merugikan (Nasution, 2022).

4.3 Praktik Kebocoran Data dalam E-Commerce dan Dampaknya terhadap Konsumen

Fenomena kebocoran data di Indonesia semakin sering terjadi, termasuk dalam sektor e-commerce. Beberapa kasus

besar, seperti dugaan kebocoran data konsumen Tokopedia pada 2020 yang melibatkan sekitar 91 juta akun pengguna, menunjukkan lemahnya pengawasan dan penegakan hukum. Dampak kebocoran data tersebut sangat luas, mulai dari penyalahgunaan identitas, penipuan daring (*phishing*), hingga kerugian finansial bagi konsumen.

Kondisi ini memperlihatkan adanya kesenjangan antara norma hukum yang sudah tersedia dengan implementasi di lapangan. UU PDP memang telah hadir sebagai payung hukum, namun efektivitasnya sangat bergantung pada regulasi turunan, pengawasan otoritas perlindungan data pribadi, serta kesadaran hukum pelaku usaha e-commerce.

4.4 Analisis Yuridis: E-Commerce, Hak Privasi, dan Tanggung Jawab Pelaku Usaha

Secara yuridis, terdapat prinsip **strict liability** yang seharusnya diterapkan pada pelaku usaha e-commerce dalam hal perlindungan data pribadi. Artinya, setiap kebocoran data yang terjadi akibat kelalaian penyelenggara sistem elektronik harus menjadi tanggung jawab penuh, tanpa perlu pembuktian kesalahan dari pihak konsumen. Namun, hingga kini penerapan prinsip tersebut belum secara eksplisit diakomodasi dalam UU PDP maupun UU ITE.

Selain itu, konsep **informed consent** atau persetujuan sadar masih menjadi persoalan. Banyak platform e-commerce yang menerapkan perjanjian baku dengan klausul yang panjang dan sulit dipahami konsumen. Padahal, Pasal 18 Undang-Undang Perlindungan Konsumen melarang klausul baku yang meniadakan tanggung jawab pelaku usaha. Oleh karena itu, klausul baku dalam transaksi elektronik yang merugikan konsumen harus dianggap batal demi hukum.

4.5 Perbandingan dengan Rezim Hukum Internasional

Jika dibandingkan dengan rezim

hukum internasional, seperti General Data Protection Regulation (GDPR) di Uni Eropa, perlindungan data pribadi di Indonesia masih tergolong baru dan membutuhkan penguatan. GDPR, misalnya, mengatur hak-hak subjek data secara detail, seperti **right to be forgotten**, **data portability**, dan hak untuk menolak pemrosesan data tertentu. Sementara itu, UU PDP Indonesia masih terbatas pada prinsip umum tanpa mekanisme teknis yang komprehensif.

Pembelajaran dari GDPR menunjukkan bahwa perlindungan data pribadi yang efektif membutuhkan:

1. **Independen Data Protection Authority (DPA)** sebagai otoritas pengawas.
2. **Sanksi administratif dan pidana yang tegas** bagi pelanggar.
3. **Kewajiban notifikasi kebocoran data** kepada subjek data dalam jangka waktu tertentu.

Dengan adopsi praktik-praktik baik tersebut, Indonesia dapat memperkuat perlindungan data pribadi dalam transaksi e-commerce sehingga sejalan dengan standar global.

4.6 Urgensi Pembentukan Otoritas Independen Perlindungan Data Pribadi di Indonesia

Salah satu kelemahan mendasar UU PDP adalah absennya otoritas independen yang khusus mengawasi pelaksanaan perlindungan data pribadi. Saat ini kewenangan masih berada di bawah Kementerian Komunikasi dan Informatika. Kondisi ini menimbulkan potensi konflik kepentingan, mengingat pemerintah juga bertindak sebagai penyelenggara sistem elektronik.

Pembentukan lembaga independen perlindungan data pribadi menjadi sangat penting untuk menjamin objektivitas, akuntabilitas, dan perlindungan hak konsumen. Lembaga ini seharusnya memiliki kewenangan penuh untuk melakukan pengawasan, pemeriksaan, menjatuhkan sanksi administratif, hingga

membawa perkara ke ranah peradilan.

4.7 Implikasi Perlindungan Data Pribadi bagi Kepercayaan Konsumen dalam E-Commerce

Perlindungan data pribadi tidak hanya penting dari sisi hukum, tetapi juga berdampak signifikan pada aspek bisnis. Kepercayaan konsumen merupakan faktor utama keberhasilan e-commerce. Tanpa jaminan keamanan data, konsumen cenderung enggan melakukan transaksi. Oleh sebab itu, keberhasilan regulasi perlindungan data pribadi akan berbanding lurus dengan peningkatan partisipasi masyarakat dalam ekonomi digital.

Dalam perspektif teori hukum responsif, perlindungan data pribadi harus dipandang sebagai instrumen untuk membangun kepercayaan publik, bukan sekadar aturan represif. Dengan demikian, keberadaan UU PDP harus benar-benar diimplementasikan dalam praktik, bukan hanya berhenti pada tataran normatif.

5. Penutup

5.1. Kesimpulan

Berdasarkan uraian hasil penelitian dan pembahasan, dapat disimpulkan beberapa hal berikut:

1. **Hak privasi dan data pribadi merupakan hak konstitusional yang wajib dilindungi negara.** Perlindungan ini memiliki dasar normatif dalam Pasal 28G ayat (1) UUD 1945 serta berbagai instrumen hukum nasional dan internasional. Dalam konteks e-commerce, hak tersebut menjadi semakin penting karena aktivitas digital sangat bergantung pada pemrosesan data pribadi konsumen.
2. **Kerangka hukum perlindungan data pribadi di Indonesia masih dalam tahap awal penguatan.** Kehadiran Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi merupakan langkah maju yang

signifikan, namun masih terdapat sejumlah kelemahan, terutama terkait dengan mekanisme implementasi, pengawasan, dan sanksi.

3. **Kasus kebocoran data dalam sektor e-commerce menunjukkan lemahnya penegakan hukum dan kesadaran pelaku usaha.** Banyak platform e-commerce belum sepenuhnya menerapkan prinsip perlindungan data pribadi secara ketat, sehingga konsumen rentan terhadap penyalahgunaan identitas, penipuan, hingga kerugian finansial.
4. **Secara yuridis, tanggung jawab pelaku usaha e-commerce seharusnya menganut prinsip strict liability.** Artinya, setiap kebocoran data pribadi akibat kelalaian penyelenggara sistem elektronik harus menjadi tanggung jawab penuh pelaku usaha, tanpa perlu pembuktian kesalahan oleh konsumen. Namun, prinsip ini belum sepenuhnya diakomodasi dalam regulasi yang berlaku.
5. **Jika dibandingkan dengan General Data Protection Regulation (GDPR) di Uni Eropa, regulasi Indonesia masih tertinggal.** Beberapa aspek penting seperti hak untuk dilupakan (*right to be forgotten*), *data portability*, dan kewajiban notifikasi kebocoran data masih perlu diperkuat agar sejalan dengan standar internasional.
6. **Urgensi pembentukan otoritas independen perlindungan data pribadi.** Tanpa adanya lembaga independen, implementasi UU PDP berpotensi tidak efektif karena masih berada di bawah kementerian yang sekaligus berperan sebagai penyelenggara sistem elektronik.
7. **Perlindungan data pribadi berdampak langsung pada**

kepercayaan konsumen. Keberhasilan e-commerce di Indonesia sangat bergantung pada jaminan keamanan data. Oleh karena itu, kepatuhan pelaku usaha terhadap UU PDP bukan hanya kewajiban hukum, tetapi juga strategi bisnis yang krusial dalam membangun kepercayaan dan loyalitas konsumen.

5.2 Rekomendasi

Berdasarkan hasil penelitian, penulis memberikan rekomendasi sebagai berikut:

1. **Perluasan pengaturan dalam UU PDP.** Regulasi turunan perlu segera dibentuk untuk mengatur mekanisme teknis perlindungan data pribadi, termasuk prosedur pengaduan, audit kepatuhan, serta standar keamanan siber bagi pelaku usaha e-commerce.
2. **Pembentukan Otoritas**
3. **Independen Perlindungan Data Pribadi.** Lembaga ini seharusnya memiliki kewenangan penuh untuk melakukan pengawasan, pemeriksaan, serta menjatuhkan sanksi terhadap pelanggaran, dengan kedudukan yang independen dari pemerintah maupun pelaku usaha.
4. **Penguatan prinsip *informed consent* dalam transaksi elektronik.** Setiap pemrosesan data pribadi harus didasarkan pada persetujuan eksplisit yang diberikan secara sadar oleh konsumen. Klausul baku yang merugikan harus dihapus sesuai dengan prinsip perlindungan konsumen.
5. **Penerapan prinsip *strict liability*.** Pelaku usaha e-commerce harus bertanggung jawab penuh terhadap setiap kebocoran data pribadi konsumen. Penerapan prinsip ini akan memperkuat posisi konsumen dan menekan pelaku usaha untuk lebih berhati-hati.
6. **Peningkatan kesadaran hukum dan literasi digital konsumen.** Pemerintah

bersama lembaga terkait perlu melakukan kampanye edukasi publik agar konsumen memahami hak-haknya serta cara melindungi data pribadi dalam aktivitas digital.

7. **Belajar dari praktik internasional.** Indonesia perlu mengadopsi praktik terbaik dari GDPR maupun regulasi serupa di negara lain, khususnya terkait hak-hak subjek data dan kewajiban notifikasi kebocoran data.
8. **Kolaborasi lintas sektor.** Perlindungan data pribadi dalam e-commerce tidak dapat diselesaikan hanya oleh pemerintah, tetapi memerlukan kerja sama antara regulator, pelaku usaha, konsumen, dan masyarakat sipil.

Daftar Pustaka

- Asosiasi Penyelenggara Jasa Internet Indonesia. (2022). *Laporan survei penetrasi & perilaku pengguna internet Indonesia 2022*. APJII.
- Asshiddiqie, J. (2006). *Hukum tata negara dan hak asasi manusia*. Jakarta: Konstitusi Press.
- Budiarta, I. N. P. (2020). *Perlindungan hukum terhadap data pribadi dalam transaksi elektronik*. Denpasar: Udayana University Press.
- Ghozali, I., & Latan, H. (2015). *Partial Least Squares: Konsep, teknik, dan aplikasi menggunakan program SmartPLS 3.0 untuk penelitian empiris*. Semarang: Badan Penerbit Universitas Diponegoro.
- International Telecommunication Union. (2021). *Global cybersecurity index 2021*. ITU Publications.
- Katsh, E., & Rabinovich-Einy, O. (2017). *Digital justice: Technology and the internet of disputes*. Oxford: Oxford University Press.
- Kompas. (2021, 12 November). *Kasus kebocoran data pribadi terus meningkat di Indonesia*. Kompas.id. <https://www.kompas.id>
- Makarim, E. (2010). *Pengantar hukum telematika*. Jakarta: RajaGrafindo Persada.
- Nasution, A. Z. (2019). *Hak privasi dalam transaksi elektronik*. Bandung: Alumni.
- Rahardjo, S. (2000). *Ilmu hukum*. Bandung: Citra Aditya Bakti.
- Republik Indonesia. (2008). Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58.
- Republik Indonesia. (2016). Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189.
- Republik Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196.
- Samuelson, P., & Scotchmer, S. (2002). The law and economics of intellectual property in the digital age. *Journal of Economic Perspectives*, 19(2), 157–179.
- Soekanto, S., & Mamudji, S. (2003). *Penelitian hukum normatif: Suatu tinjauan singkat*. Jakarta: RajaGrafindo Persada.
- Sutedi, A. (2011). *Hukum perlindungan konsumen*. Jakarta: Sinar Grafika.
- Tempo. (2020, 20 Juni). *Kebocoran data Tokopedia: 91 juta akun dijual di forum hacker*. Tempo.co. <https://www.tempo.co>
- World Bank. (2020). *Data protection and privacy in developing countries: Policies and practices*. Washington, DC: World Bank Publications