BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi telah mendorong transformasi aktivitas ekonomi menuju sistem digital. Salah satu bentuk nyata dari transformasi tersebut adalah berkembangnya perdagangan elektronik atau *e-commerce* yang memungkinkan transaksi dilakukan tanpa batas ruang dan waktu. Melalui platform *e-commerce*, berbagai jenis data pribadi pengguna dikumpulkan dan diproses, mulai dari nama, alamat, nomor telepon, alamat email, hingga data transaksi keuangan[1]. Dalam hal ini, data pribadi menjadi komponen penting dalam ekosistem ekonomi digital karena mendukung kelancaran transaksi dan peningkatan kualitas layanan[2]. Namun demikian, tingginya penggunaan data pribadi juga menimbulkan risiko terhadap penyalahgunaan serta kebocoran data yang dapat merugikan pengguna[3].

Pesatnya aktivitas digital tersebut turut meningkatkan potensi terjadinya akses tidak sah terhadap data pribadi. Berbagai kasus kebocoran data dalam sistem elektronik, termasuk pada platform *e-commerce*, menunjukkan bahwa data pribadi pengguna masih rentan disalahgunakan oleh pihak yang tidak bertanggung

---

[1] Evi, 2023, **Transformasi Transaksi Tunai ke Digital di Indonesia**, CV. AA Rizky, hlm. 25.

[2] Rosidi, A., Wedha, Y. Y., & Hendri, W. 2022. Mashur.**Transaksi Online Dimasa Pandemi Covid-19, Perspektif Hukum Positif (Ius Contitutum).** *Journal Ilmiah Rinjani: Media Informasi Ilmiah Universitas Gunung Rinjani*, *10* (1).

[3] Chic, S. A., dan Bilqisthi, M. F., 2024, **Tantangan dan Peluang Blockchain di Era Digital dalam Bidang Keamanan Data dan Transaksi Digital**, Journal of Comprehensive Science (JCS), Volume 3 Nomor 11, hlm. 120.

jawab[4]. Kebocoran data tersebut dapat menimbulkan berbagai dampak negatif, seperti penipuan digital, pencurian identitas (*identity theft*), serta kerugian ekonomi dan sosial bagi pemilik data[5]. Kondisi ini menegaskan bahwa perlindungan data pribadi merupakan isu yang sangat penting dalam penyelenggaraan sistem elektronik, khususnya dalam kegiatan *e-commerce*, sehingga diperlukan pengaturan dan kewajiban yang jelas bagi pengendali data untuk mencegah terjadinya akses tidak sah terhadap data pribadi[6].

Perlindungan data pribadi pada dasarnya merupakan bagian yang tidak terpisahkan dari perlindungan hak privasi individu di era digital. Hak atas privasi menjadi salah satu hak fundamental yang harus dijamin, terutama ketika aktivitas masyarakat semakin bergantung pada sistem elektronik. Oleh karena itu, negara memiliki kewajiban untuk memberikan jaminan perlindungan hukum terhadap data pribadi masyarakat dari berbagai bentuk penyalahgunaan oleh pihak lain[7]. Dalam konteks hukum nasional, Indonesia telah menetapkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi sebagai landasan hukum yang mengatur pemrosesan, pengelolaan, serta perlindungan data pribadi. Undang-undang ini bertujuan untuk memberikan kepastian hukum sekaligus menjamin

---

[4] Syawalina, R., Prasja, T. R., dan Aridhayandi, M. R., 2025, **Mengungkap Kasus Kebocoran Data Pada Platform E-Commerce: Analisis dan Mitigasi Risiko**, Karimah Tauhid, Volume 4 Nomor 7, hlm. 4910.

[5] Permadhi, P. L. O., & Udytama, I. W. W. W. 2024. **Problematika Hukum Terkait Digital nomads Ditinjau Dari Peraturan Perundang-Undangan Indonesia**. *Jurnal Hukum Saraswati (JHS)*, *6*(1), hlm. 664.

[6] Putri, A., Sari, N., Fajrina, P., dan Aisyah, S., 2025, **Keamanan Online dalam Media Sosial: Pentingnya Perlindungan Data Pribadi di Era Digital**, Jurnal Pengabdian Nasional Indonesia, Volume 6 Nomor 1, hlm. 40.

[7] Huda, H. U. N., Astaruddin, H. T., Nasution, M. I., dkk., 2024, **Data Pribadi, Hak Warga, dan Negara Hukum: Menjaga Privasi di Tengah Ancaman Digital**, Penerbit Widina, hlm. 40.

perlindungan terhadap hak-hak pemilik data pribadi dalam menghadapi berbagai risiko di ruang digital[8].

Dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi tersebut, pihak yang melakukan pemrosesan data pribadi dikenal sebagai Pengendali Data Pribadi. Pengendali data memiliki sejumlah kewajiban hukum yang harus dipenuhi dalam menjalankan aktivitas pemrosesan data, salah satunya adalah kewajiban untuk mencegah terjadinya akses tidak sah terhadap data pribadi. Ketentuan ini secara tegas diatur dalam Pasal 39 Undang-Undang Perlindungan Data Pribadi yang mewajibkan pengendali data untuk melindungi data pribadi melalui sistem keamanan yang andal, aman, dan bertanggung jawab. Dengan demikian, aspek pencegahan atau *preventive protection* menjadi prinsip yang sangat penting dalam kerangka perlindungan data pribadi, khususnya dalam memastikan bahwa data yang dikelola tidak mudah diakses, disalahgunakan, atau dibocorkan oleh pihak yang tidak berwenang[9].

Kendati Pasal 39 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah mengatur kewajiban pencegahan akses tidak sah terhadap data pribadi, ketentuan tersebut masih menimbulkan permasalahan dalam implementasinya. Permasalahan tersebut disebabkan oleh adanya frasa "sistem keamanan yang andal, aman, dan bertanggung jawab" yang belum dijelaskan secara rinci mengenai standar maupun parameter yang harus dipenuhi

[8] Yudistira, M., dan Ramadani, R., 2023, **Tinjauan Yuridis terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang Nomor 27 Tahun 2022 oleh KOMINFO**, UNES Law Review, Volume 5 Nomor 4, hlm. 3920.

[9] *Ibid*, hlm. 3922.

oleh Pengendali Data Pribadi[10]. Selain itu, Pasal 39 ayat (3) menyatakan bahwa upaya pencegahan tersebut dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan, tetapi hingga saat ini belum terdapat pengaturan teknis yang secara khusus mengatur standar keamanan data yang wajib diterapkan. Kondisi tersebut berpotensi menimbulkan kekaburan norma (*vague norm*) yang pada akhirnya dapat berdampak pada ketidakpastian hukum dalam pelaksanaan kewajiban perlindungan data pribadi[11].

Dalam praktik penyelenggaraan *e-commerce*, Pengendali Data Pribadi memproses data dalam jumlah besar dan dilakukan secara berkelanjutan, sehingga risiko terjadinya akses tidak sah menjadi semakin tinggi. Tanpa adanya standar keamanan yang jelas dan terukur, akan sulit untuk menentukan apakah Pengendali Data Pribadi telah memenuhi kewajiban hukumnya dalam mencegah akses tidak sah terhadap data pribadi[12]. Keadaan ini juga menimbulkan kendala dalam menilai dan menetapkan tanggung jawab hukum apabila terjadi kebocoran data pribadi. Oleh karena itu, diperlukan suatu analisis yuridis yang mendalam terhadap pengaturan kewajiban pencegahan akses tidak sah terhadap data pribadi dalam sistem *e-commerce* berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, guna memberikan kejelasan norma serta

[10] Vania, C., Markoni, M., Saragih, H., dan Widarto, J., 2023, **Tinjauan Yuridis terhadap Perlindungan Data Pribadi dari Aspek Pengamanan Data dan Keamanan Siber**, Jurnal Multidisiplin Indonesia, Volume 2 Nomor 3, hlm. 656.

[11] Chessya Tivani, W., 2025, **Perlindungan Hukum pada Pusat Data Nasional terhadap Kejahatan Peretasan Data**, Skripsi, Universitas Lampung, hlm. 35.

[12] Wiraguna, S. A., 2025, **Tanggung Jawab Hukum Platform E-Commerce atas Kebocoran Data Pribadi dalam Perspektif UU No. 27 Tahun 2022**, Jurnal Kajian Hukum dan Kebijakan Publik, Volume 2 Nomor 2, hlm. 1090.

mendukung terciptanya kepastian hukum dalam perlindungan data pribadi di Indonesia[13].

Penelitian mengenai kewajiban pencegahan akses tidak sah terhadap data pribadi menjadi sangat penting seiring dengan meningkatnya aktivitas ekonomi digital dan tingginya risiko kebocoran data dalam sistem elektronik. Perkembangan *e-commerce* yang semakin pesat menuntut adanya jaminan keamanan data pribadi pengguna sebagai bagian dari perlindungan hak privasi[14]. Di sisi lain, pengaturan mengenai kewajiban sistem keamanan data dalam Undang-Undang Perlindungan Data Pribadi masih memerlukan kajian lebih mendalam untuk menilai sejauh mana norma yang ada mampu memberikan kepastian hukum serta perlindungan yang efektif bagi pengguna *e-commerce*. Oleh karena itu, penelitian ini menjadi relevan untuk dilakukan guna mengkaji secara yuridis pengaturan kewajiban pencegahan akses tidak sah terhadap data pribadi oleh Pengendali Data Pribadi dalam sistem *e-commerce*, sehingga dapat memberikan kontribusi terhadap penguatan perlindungan hukum di bidang data pribadi[15].

Sejumlah penelitian terdahulu telah mengkaji mengenai perlindungan data pribadi dalam sistem elektronik maupun dalam aktivitas *e-commerce*. Penelitian yang dilakukan oleh Muhammad dan Nugroho membahas perlindungan hukum terhadap pengguna aplikasi *e-commerce* yang terdampak kebocoran data

---

[13] Delpiero, M., Reynaldi, F. A., Ningdiah, I. U., dan Muthmainnah, N., 2021, **Analisis Yuridis Kebijakan Privasi dan Pertanggungjawaban Online Marketplace**, Padjadjaran Law Review, Volume 9 Nomor 1, hlm. 20.

[14] Maharani, R., dan Prakoso, A. L., 2024, **Perlindungan Data Pribadi Konsumen oleh Penyelenggara Sistem Elektronik dalam Transaksi Digital**, Jurnal USM Law Review, Volume 7 Nomor 1, hlm. 335.

[15] Silalahi, J. A. S., Purba, Y. Y., dan Nasution, M. F., 2025, **Analisis Yuridis terhadap Mekanisme Perlindungan Data Pribadi**, Jurnal Minfo Polgan, Volume 14 Nomor 1, hlm. 606.

pribadi[16]. Penelitian tersebut menitikberatkan pada analisis berbagai peraturan perundang-undangan yang mengatur perlindungan data pribadi sebelum lahirnya Undang-Undang Perlindungan Data Pribadi, seperti Undang-Undang Informasi dan Transaksi Elektronik, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang penyelenggaraan Sistem dan Transaksi Elektronik, serta Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016. Selain itu, penelitian oleh Putri dan Fahrozi mengkaji upaya pencegahan kebocoran data konsumen serta pentingnya pengesahan Rancangan Undang-Undang Perlindungan Data Pribadi sebagai dasar hukum dalam memberikan kepastian hukum dan menuntut pertanggungjawaban penyelenggara *e-commerce*, dengan studi kasus pada platform *e-commerce*[17].

Kendati penelitian-penelitian tersebut telah memberikan kontribusi penting dalam kajian perlindungan data pribadi, pada umumnya masih bersifat deskriptif dan berfokus pada perlindungan hukum secara umum maupun urgensi pembentukan regulasi. Penelitian terdahulu belum secara spesifik menganalisis kewajiban pencegahan akses tidak sah terhadap data pribadi oleh Pengendali Data Pribadi sebagaimana diatur dalam Pasal 39 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Dengan demikian, penelitian ini memiliki unsur kebaruan, karena secara khusus mengkaji kewajiban preventif (*preventive protection*) yang harus dipenuhi oleh Pengendali Data Pribadi dalam mencegah

[16] Muhammad, M. O., dan Nugroho, L. D., 2021, **Perlindungan Hukum terhadap Pengguna Aplikasi E-Commerce yang Terdampak Kebocoran Data Pribadi**, Jurnal Pamator: Jurnal Ilmiah Universitas Trunojoyo, Volume 14 Nomor 2, hlm. 167.

[17] Putri, D. D. F., dan Fahrozi, M. H., 2021, **Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan RUU Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.com)**, Borneo Law Review, Volume 5 Nomor 1, hlm. 50.

akses tidak sah terhadap data pribadi dalam sistem *e-commerce* berdasarkan perspektif hukum perlindungan data pribadi di Indonesia.

Berdasarkan uraian di atas, penelitian ini berbeda dengan penelitian sebelumnya. Pada penelitian ini penulis berfokus untuk melakukan pembahasan dan penelitian dengan judul: "**Analisis Yuridis Kewajiban Pencegahan Akses Tidak Sah Terhadap Data Pribadi Dalam Transaksi E-Commerce Oleh Pengendali Data".**

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, maka rumusan masalah dalam penelitian ini adalah :

1. Pengaturan kewajiban pencegahan akses tidak sah terhadap data pribadi oleh Pengendali Data Pribadi menurut peraturan perundang-undangan di Indonesia adalah.
2. Kewajiban Pengendali Data Pribadi dalam mencegah akses tidak sah terhadap data pribadi dalam sistem *e-commerce* adalah.

1.3 Ruang Lingkup Masalah

Ruang lingkup masalah dalam penelitian ini difokuskan pada kajian yang terarah dan spesifik terkait kewajiban pencegahan akses tidak sah terhadap data pribadi oleh Pengendali Data Pribadi dalam sistem *e-commerce* berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang meliputi:

1. Kajian yuridis normatif terhadap ketentuan Pasal 39 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi serta peraturan perundang-

undangan lain yang berkaitan dengan perlindungan data pribadi dalam sistem elektronik.

2. Pengaturan hukum mengenai kewajiban Pengendali Data Pribadi dalam mencegah akses tidak sah terhadap data pribadi dalam penyelenggaraan sistem *e-commerce*.
3. Analisis terhadap potensi kekaburan norma (*vague norm*) dalam ketentuan mengenai kewajiban pencegahan akses tidak sah terhadap data pribadi serta implikasinya terhadap kepastian hukum.
4. Kajian mengenai efektivitas pengaturan hukum dalam memberikan kejelasan, kepastian hukum, dan perlindungan hukum bagi pemilik data pribadi dalam aktivitas *e-commerce*.

1.4 Tujuan Penelitian

1.4.1 Tujuan Umum

1. Untuk melaksanakan Tri Dharma Perguruan Tinggi, khususnya pada bidang penelitian yang dilakukan oleh mahasiswa.
2. Untuk menunjang perkembangan ilmu pengetahuan hukum, khususnya dalam bidang hukum siber (*cyber law*), hukum teknologi informasi, dan perlindungan data pribadi.
3. Sebagai salah satu syarat untuk menyelesaikan jenjang Pendidikan Strata 1 (S1) pada Fakultas Hukum Universitas Mahasaraswati Denpasar.

1.4.2 Tujuan Khusus

1. Untuk menganalisis pengaturan kewajiban pencegahan akses tidak sah terhadap data pribadi oleh Pengendali Data Pribadi menurut peraturan perundang-undangan di Indonesia.

2. Untuk menganalisis kewajiban Pengendali Data Pribadi dalam mencegah akses tidak sah terhadap data pribadi dalam sistem *e-commerce*.

1.5 Metode Penelitian

Metode penelitian adalah proses analisa yang meliputi metode, sistematika, dan pemikiran tertentu yang bertujuan untuk mempelajari gejala hukum tertentu kemudian mengusahakan pemecahan masalah yang timbul. Dalam penelitian ini, metode yang digunakan diarahkan untuk mengkaji norma hukum yang berkaitan dengan perlindungan data pribadi, khususnya mengenai kewajiban pencegahan akses tidak sah terhadap data pribadi oleh Pengendali Data Pribadi dalam sistem *e-commerce* berdasarkan peraturan perundang-undangan yang berlaku di Indonesia.

1.5.1 Jenis Penelitian

Penelitian ini merupakan penelitian hukum normatif yang berfokus pada pengkajian norma atau kaidah hukum yang berlaku, khususnya yang berkaitan dengan kewajiban pencegahan akses tidak sah terhadap data pribadi oleh Pengendali Data Pribadi dalam sistem *e-commerce*. Penelitian ini dilakukan dengan menelaah peraturan perundang-undangan, khususnya terhadap ketentuan dalam Pasal 39 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang mengatur kewajiban pencegahan akses tidak sah, serta bahan hukum lainnya yang relevan, guna menganalisis kejelasan norma (*legal clarity*), potensi kekaburan norma (*vague norm*), dan implikasinya terhadap kepastian hukum dalam perlindungan data pribadi.

1.5.2 Jenis Pendekatan

Adapun dalam penelitian ini menggunakan jenis pendekatan, yaitu :

1. Pendekatan Perundang-Undangan

   Menganalisis norma hukum berdasarkan teks peraturan yang ada. Pendekatan ini berfokus pada analisis norma hukum berdasarkan teks peraturan yang ada, seperti undang-undang, peraturan pemerintah, atau keputusan presiden. Metode ini digunakan untuk mendapatkan pemahaman tentang isi, maksud, dan tujuan suatu aturan hukum, serta bagaimana aturan tersebut tidak memiliki ambiguitas atau telah memiliki kepastian hukum.

1.5.3 Sumber Bahan Hukum

Sumber bahan hukum merupakan segala sesuatu yang menjadi rujukan dalam memperoleh bahan hukum yang digunakan untuk menganalisis permasalahan dalam penelitian.

1. Bahan Hukum Primer

Bahan hukum primer merupakan bahan hukum yang memiliki kekuatan mengikat karena berasal dari peraturan perundang-undangan yang berlaku. Dalam penelitian ini, bahan hukum primer yang digunakan meliputi:

a. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945
b. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi
c. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016
d. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

e. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

2. Bahan Hukum Sekunder

Bahan hukum sekunder merupakan bahan hukum yang memberikan penjelasan terhadap bahan hukum primer, seperti buku-buku literatur hukum, jurnal ilmiah, hasil penelitian terdahulu, artikel ilmiah, serta pendapat para ahli yang berkaitan dengan perlindungan data pribadi, sistem elektronik, dan kegiatan *e-commerce*.

3. Bahan Hukum Tersier

Bahan hukum tersier merupakan bahan hukum yang memberikan petunjuk maupun penjelasan terhadap bahan hukum primer dan sekunder, seperti kamus hukum, kamus bahasa, ensiklopedia, serta sumber lain yang relevan untuk membantu memahami istilah-istilah yang digunakan dalam penelitian ini.

1.5.4 Teknik Pengumpulan Bahan Hukum

Teknik pengumpulan bahan hukum pada penelitian normatif, yakni mengkaji, mencatat dengan menggunakan logika-logika hukum terhadap bahan hukum yang terkait. Metode pengumpulan bahan hukum yang digunakan dalam penelitian ini adalah studi kepustakaan bahan hukum tertulis, yaitu dengan cara mengumpulkan, membaca, dan mencatat bahan hukum berupa kutipan langsung maupun kutipan tidak langsung yang diperoleh dari buku-buku, jurnal ilmiah, hasil penelitian terdahulu, serta peraturan perundang-undangan yang berkaitan dengan permasalahan yang dianalisis penulis, yaitu kewajiban pencegahan akses tidak sah terhadap data pribadi oleh Pengendali Data Pribadi dalam sistem *e-*

commerce berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Teknik ini dilakukan untuk memperoleh data yang relevan, akurat, dan sistematis guna mendukung analisis hukum dalam penelitian ini.

1.5.5 Teknik Analisis Bahan Hukum

Untuk menganalisis bahan-bahan hukum yang telah terkumpul dapat dipergunakan berbagai teknik analisis seperti:

1. Teknik deskripsi adalah teknik dasar analisis yang tidak dapat dihindari penggunaannya. Deskripsi berarti uraian apa adanya terhadap suatu kondisi atau posisi dari proposisi-proposisi hukum atau non hukum[18];
2. Teknik interpretasi berupa penggunaan jenis-jenis penafsiran dalam ilmu hukum seperti penafsiran gramatikal, historis, sistematis, teleologis, kontekstual, dan lain-lain[19];
3. Teknik konstruksi berupa pembentukan konstruksi yuridis dengan melakukan analogi dan pembalikan proposisi (*a contrario*)[20];
4. Teknik evaluasi adalah penilaian berupa tepat atau tidak tepat, setuju atau tidak setuju, benar atau salah atau tidak sah oleh peneliti terhadap suatu pandangan, proposisi, pernyataan rumusan norma, keputusan, baik yang tertera dalam bahan hukum primer maupun bahan hukum sekunder[21];

---

[18] Solikin, N. 2021**. Pengatar metodelogi penelitia hukum.**

[19] Susanti, D. I., & Sh, M. 2021. **Penafsiran Hukum: Teori dan Metode.** Sinar Grafika (Bumi Aksara).

[20] Suwandi, D. 2023. ***Rekontruksi Frasa Wajib Yang Berimplikasi Terhadap Penyusunan Peraturan Perundang-Undangan Berbasis Nilai Keadilan*** (Doctoral dissertation, Universitas Islam Sultan Agung (Indonesia)).

[21] Sari, D. P., & Lisnawati, S. 2021. **Evaluasi Pembelajaran Pendidikan Agama Islam Di SMP Negeri 16 Ogan Komering Ulu pada Masa Pandemi Covid19.** *Jurnal Syntax Transformation*, *2*(04), 478-485.

5. Teknik argumentasi tidak bisa dilepaskan dari teknik evaluasi karena penilaian harus didasarkan pada alasan-alasan yang bersifat penalaran hukum. Dalam pembahasan permasalahan hukum, semakin banyak argumentasi maka semakin menunjukkan kedalaman penalaran hukum[22];
6. Teknik sistemisasi adalah upaya mencari keterkaitan rumusan suatu konsep hukum atau proposisi hukum antara peraturan perundang-undangan yang sederajat maupun yang tidak sederajat[23].

Penelitian ini menggunakan teknik deskripsi. Teknik deskripsi digunakan untuk menguraikan secara sistematis dan jelas mengenai pengaturan kewajiban pencegahan akses tidak sah terhadap data pribadi oleh Pengendali Data Pribadi berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi serta peraturan perundang-undangan lainnya yang berkaitan dengan perlindungan data pribadi dan sistem elektronik. Melalui teknik ini, penulis mendeskripsikan ketentuan hukum yang berlaku, konsep-konsep hukum, serta pendapat para ahli yang relevan guna memperoleh gambaran yang jelas mengenai perlindungan data pribadi dalam sistem e-commerce.

1.6 Sistematika Penulisan

Sistematika penulisan skripsi disusun untuk mempermudah penulis dalam memberikan penjabaran secara terperinci, sehingga pembahasan dapat tersusun secara sistematis dan terarah. Adapun sistematika penulisan dalam penelitian ini terdiri dari beberapa bab sebagai berikut:

---

[22] Satria Kurniawan Putra, S. T. 2025. **Argumentasi Hukum BAB.** *Pengantar Argumentasi Hukum*, 17.

[23] Selfianus Laritmas, S. H. 2026. **Hukum Perancangan Peraturan Perundang-Undangan: Teori, Praktik, dan Teknik Penyusunan.** PT. Revormasi Jangkar Philosophia.

BAB I : PENDAHULUAN

Pada Bab I ini penulis akan berfokus pada pengantar dan latar belakang penelitian. Penjelasan mengenai pentingnya perlindungan data pribadi dalam perkembangan teknologi digital dan *e-commerce*, rumusan masalah, tujuan penelitian, manfaat penelitian, serta metode penelitian yang digunakan dalam mengkaji permasalahan hukum yang diangkat.

BAB II : KAJIAN TEORITIS

Bab ini akan menjelaskan kajian teori yang digunakan untuk mengkaji permasalahan hukum yang diangkat dalam penelitian ini. Penulis akan mengidentifikasi teori, asas, dan konsep hukum yang relevan, seperti teori perlindungan hukum, teori kepastian hukum, asas perlindungan data pribadi, serta konsep Pengendali Data Pribadi dan sistem *e-commerce*.

BAB III : PEMBAHASAN

Pada bab ini, penulis akan membahas pengaturan hukum mengenai kewajiban pencegahan akses tidak sah terhadap data pribadi berdasarkan peraturan perundang-undangan di Indonesia, khususnya dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi serta peraturan terkait lainnya.
3.1 Pengaturan kewajiban perlindungan data pribadi dalam peraturan perundang-undangan di Indonesia
3.2 Analisis norma kewajiban pencegahan akses tidak sah terhadap data pribadi dalam Undang-Undang Perlindungan Data Pribadi

BAB IV : PEMBAHASAN

Bab ini akan fokus pada pembahasan mengenai kewajiban Pengendali Data Pribadi dalam mencegah akses tidak sah terhadap data pribadi dalam praktik

penyelenggaraan sistem *e-commerce*, serta analisis terhadap kejelasan norma dan implikasinya terhadap kepastian hukum.

4.1 Pelaksanaan kewajiban Pengendali Data Pribadi dalam sistem *e-commerce*

4.2 Analisis kejelasan norma (*legal clarity*) dan implikasi hukum dalam pencegahan akses tidak sah terhadap data pribadi

BAB V : PENUTUP

Pada bab terakhir ini, penulis menyampaikan hasil penelitian yang terdiri atas simpulan dan saran. Simpulan akan merangkum temuan utama dari penelitian, menjawab rumusan masalah yang telah diajukan, serta menekankan pentingnya perlindungan hukum terhadap data pribadi dalam sistem *e-commerce*.

5.1 Simpulan

5.2 Saran

BAB II

KAJIAN TEORITIS

2. 1 Landasan Teori

2.1.1Teori Kepastian Hukum

Kepastian hukum merupakan salah satu konsep fundamental dalam ilmu hukum yang bertujuan untuk memberikan kejelasan, ketegasan, dan keteraturan dalam penerapan hukum di masyarakat[24]. Menurut Gustav Radbruch, kepastian hukum (*rechtssicherheit*) merupakan salah satu dari tiga nilai dasar hukum selain keadilan (*gerechtigkeit*) dan kemanfaatan (*zweckmäßigkeit*). Kepastian hukum menghendaki agar hukum dibuat dalam bentuk yang jelas, tegas, dan dapat diprediksi sehingga dapat dijadikan pedoman oleh masyarakat dalam bertindak[25]. Sementara itu, E. Utrecht menyatakan bahwa kepastian hukum mengandung arti adanya aturan yang bersifat umum sehingga setiap individu mengetahui apa yang boleh dan tidak boleh dilakukan[26]. Sedangkan menurut Sudikno Mertokusumo, kepastian hukum merupakan jaminan bahwa hukum dijalankan dengan baik, jelas, konsisten, dan tidak menimbulkan multitafsir[27].

Kepastian hukum juga merupakan salah satu tujuan utama hukum, selain keadilan dan kemanfaatan. Dalam konteks ini, hukum tidak hanya berfungsi sebagai alat pengatur, tetapi juga sebagai sarana untuk menciptakan ketertiban

---

[24] Febrianti, M., dan Tarigan, E. K., 2025, **Relevansi Asas Kepastian Hukum**, Jurnal Mimbar Ilmu Hukum, Volume 4 Nomor 1, hlm. 15.

[25] Hotta, A. Y., 2025, **Pemahaman terhadap Asas Kepastian Hukum**, Jurnal Hukum Dinamika, Volume 1 Nomor 1, hlm. 25.

[26] Aulia, T., Arindi, S. K., dan Handayani, S. H. S., 2026, **Peran Hukum Platform E-Commerce dalam Transaksi Online**, Jurnal Penelitian Ilmiah Multidisipliner, Volume 3 Nomor 01, hlm. 50.

[27] Halilah, S., dan Arif, M. F., 2021, **Asas Kepastian Hukum Menurut Para Ahli**, Siyasah: Jurnal Hukum Tata Negara, Volume 4 Nomor II, hlm. 10.

dan stabilitas dalam kehidupan masyarakat. Tanpa adanya kepastian hukum, maka akan timbul ketidakpastian yang berpotensi menimbulkan konflik, ketidakadilan, serta kesulitan dalam penegakan hukum[28].

Dalam pembentukan norma hukum, kepastian hukum sangat berkaitan erat dengan kejelasan rumusan peraturan perundang-undangan. Suatu norma hukum harus dirumuskan secara tegas, tidak ambigu, dan memiliki batasan yang jelas agar dapat diterapkan secara efektif. Apabila suatu norma mengandung kekaburan atau *vague norm*, maka akan menimbulkan berbagai penafsiran yang berbeda, sehingga berpotensi menimbulkan ketidakpastian hukum dalam implementasinya[29].

Pentingnya kepastian hukum juga sangat terlihat dalam pengaturan perlindungan data pribadi, khususnya di era digital yang ditandai dengan meningkatnya penggunaan teknologi informasi dan sistem *e-commerce*. Dalam konteks ini, kepastian hukum diperlukan untuk memberikan jaminan perlindungan terhadap hak privasi individu serta memberikan pedoman yang jelas bagi para pihak yang memproses data pribadi, terutama Pengendali Data Pribadi[30].

Relevansi teori kepastian hukum dalam penelitian ini terletak pada analisis terhadap pengaturan kewajiban Pengendali Data Pribadi dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, khususnya terkait kewajiban pencegahan akses tidak sah terhadap data pribadi. Ketentuan seperti

---

[28] Tarigan, R. S., 2024, **Menuju Negara Hukum yang Berkeadilan**, Ruang Karya Bersama, hlm. 33.

[29] Selfianus Laritmas, 2026, **Hukum Perancangan Peraturan Perundang-Undangan: Teori, Praktik, dan Teknik Penyusunan**, PT. Revormasi Jangkar Philosophia, hlm. 58.

[30] Aulia, T., Arindi, S. K., dan Handayani, S. H. S., *Op.Cit.*, hlm. 52.

frasa "sistem keamanan yang andal, aman, dan bertanggung jawab" dalam Pasal 39 Undang-Undang Data Pribadi berpotensi menimbulkan kekaburan norma apabila tidak disertai dengan standar yang jelas. Oleh karena itu, teori kepastian hukum digunakan sebagai landasan untuk menilai apakah pengaturan tersebut telah memberikan kejelasan norma dan kepastian hukum dalam pelaksanaannya, terutama dalam sistem *e-commerce.*

2.1.2 Teori Perlindungan Hukum

Perlindungan hukum merupakan upaya untuk memberikan jaminan terhadap hak-hak subjek hukum agar terlindungi dari tindakan sewenang-wenang serta untuk menciptakan rasa aman dan keadilan dalam kehidupan bermasyarakat[31]. Menurut Satjipto Rahardjo, perlindungan hukum adalah upaya untuk melindungi kepentingan seseorang dengan cara memberikan kekuasaan kepadanya untuk bertindak dalam rangka kepentingannya tersebut[32]. Sementara itu, Philipus M. Hadjon membedakan perlindungan hukum menjadi dua bentuk, yaitu perlindungan hukum preventif dan represif. Perlindungan hukum preventif Perlindungan yang bertujuan untuk mencegah terjadinya pelanggaran sebelum peristiwa hukum/kerugian terjadi, sedangkan perlindungan hukum represif Perlindungan yang bertujuan untuk menyelesaikan sengketa, memulihkan hak-hak yang terlanggar, serta memberikan sanksi setelah terjadinya suatu pelanggaran hukum[33].

---

[31] Surya, A., Aryanlngrum, P., Wattimena, J. A. Y., dkk., 2025, **Perlindungan Hukum di Indonesia**, Penerbit Widina, hlm. 47.

[32] Sihombing, A., 2023, **Hukum Perlindungan Konsumen**, CV. Azka Pustaka, hlm. 62.

[33] Firda, N., 2024, **Perlindungan Hukum terhadap Para Pihak dalam Perjanjian Jual Beli Melalui Media Elektronik**, Skripsi, Universitas Islam Sultan Agung Semarang, hlm. 28.

Apabila kewajiban preventif sebagaimana diatur dalam Pasal 39 Undang-Undang Perlindungan Data Pribadi dilanggar dan mengakibatkan akses tidak sah atau kebocoran data pribadi, maka diperlukan perlindungan hukum represif untuk memulihkan hak Subjek Data Pribadi. Mekanisme represif dapat dilakukan melalui kewajiban Pengendali Data Pribadi untuk memberitahukan kegagalan pelindungan data, melakukan penanganan dan pemulihan, serta mempertanggungjawabkan pemrosesan data pribadi.

Selain itu, Pasal 12 Undang-Undang Perlindungan Data Pribadi memberikan hak kepada Subjek Data Pribadi untuk memperoleh ganti rugi atas pelanggaran pemrosesan data pribadi. Pengendali Data Pribadi juga dapat dikenai sanksi administratif apabila melanggar kewajiban pelindungan data. Dengan demikian, perlindungan hukum represif tidak hanya berfungsi memberikan sanksi kepada Pengendali Data Pribadi, tetapi juga memberikan pemulihan terhadap kerugian yang dialami Subjek Data Pribadi.

Dalam konteks transaksi e-commerce, mekanisme tersebut menunjukkan bahwa perlindungan data pribadi harus mencakup dua aspek, yaitu pencegahan sebelum terjadi pelanggaran dan pemulihan setelah terjadi pelanggaran. Oleh karena itu, hak ganti rugi menjadi salah satu instrumen penting untuk memberikan perlindungan dan kepastian hukum bagi Subjek Data Pribadi ketika terjadi akses tidak sah atau kebocoran data pribadi.

Dalam konteks hak privasi, perlindungan hukum menjadi sangat penting karena hak privasi merupakan bagian dari hak asasi manusia yang harus dijamin oleh negara. Perlindungan terhadap hak privasi mencakup perlindungan atas data pribadi individu agar tidak disalahgunakan oleh pihak lain tanpa persetujuan. Di

era digital saat ini, pemanfaatan teknologi informasi yang semakin berkembang pesat membawa konsekuensi terhadap meningkatnya risiko pelanggaran terhadap hak privasi, khususnya dalam pengumpulan, penyimpanan, dan pengolahan data pribadi melalui sistem elektronik[34].

Perlindungan hukum dalam konteks pemanfaatan teknologi informasi menjadi semakin kompleks seiring dengan berkembangnya berbagai platform digital, termasuk sistem *e-commerce*. Dalam sistem ini, data pribadi pengguna menjadi aset yang sangat penting, namun juga rentan terhadap berbagai ancaman seperti akses tidak sah, kebocoran data, dan penyalahgunaan informasi. Oleh karena itu, diperlukan pengaturan hukum yang mampu memberikan perlindungan yang efektif terhadap data pribadi, baik melalui mekanisme pencegahan maupun penegakan hukum[35].

Relevansi teori perlindungan hukum dalam penelitian ini terletak pada analisis terhadap kewajiban Pengendali Data Pribadi dalam melindungi data pribadi pengguna dalam sistem *e-commerce*. Kewajiban untuk mencegah akses tidak sah terhadap data pribadi sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi mencerminkan bentuk perlindungan hukum preventif. Dengan demikian, teori perlindungan hukum digunakan sebagai landasan untuk menilai sejauh mana pengaturan tersebut mampu memberikan perlindungan yang efektif terhadap hak privasi individu serta menjamin keamanan data pribadi dalam kegiatan *e-commerce*.

---

[34] Suari, K. R. A., dan Sarjana, I. M., 2023, **Menjaga Privasi di Era Digital**, Jurnal Analisis Hukum, Volume 6 Nomor 1, hlm. 135.

[35] Hidayat, W. H., dan Kholik, N., 2024, **Implikasi Hukum atas Perubahan Bisnis UMKM**, Jurnal Analisis Hukum, Volume 7 Nomor 1, hlm. 72.

2.1.3 Teori Penafsiran Hukum

Menurut Sudikno Mertokusumo dan A. Pitlo, interpretasi atau penafsiran hukum merupakan salah satu metode penemuan hukum yang memberi penjelasan yang gamblang mengenai teks undang-undang agar ruang lingkup kaidah dapat ditetapkan sehubungan dengan peristiwa tertentu.[36]

Lebih lanjut, Mertokusumo dan Pitlo mengidentifikasi enam metode penafsiran hukum atau interpretasi yang lazim digunakan oleh hakim. Enam metode yang dimaksud adalah interpretasi gramatikal atau bahasa, interpretasi teleologis atau sosiologis, interpretasi sistematis atau logis, interpretasi historis, interpretasi komparatif atau perbandingan, dan interpretasi futuristis. Hal tersebut berturut-turut diuraikan sebagai berikut:

1. Interpretasi gramatikal atau bahasa

   Interpretasi gramatikal atau bahasa adalah metode penafsiran atau interpretasi yang menekankan pada pentingnya kedudukan bahasa dalam memberikan makna terhadap suatu objek. Metode ini sering disebut sebagai metode penafsiran objektif yang merupakan metode penafsiran paling sederhana, yakni dengan menguraikannya menurut bahasa, susunan kata, atau bunyinya.

   Terkait interpretasi ini, Mertokusumo dan Pitlo menerangkan bahwa ada tiga pendekatan kontekstual yang dapat digunakan dalam metode penafsiran ini, yaitu:

[36] Sudikno Mertokusumo dan A. Pitlo, **Bab-Bab tentang Penemuan Hukum** (Bandung: Citra Aditya Bakti, 1993), hlm. 13.

a. *noscitur a socis* yang artinya suatu perkataan harus dinilai dari ikatan dalam kumpulan-kumpulannya;
b. *ejusdem generis* yang artinya perkataan yang digunakan dalam lingkungan atau kelompok yang sama;
c. *expressum facit cassare tacitum* yang artinya kata-kata yang dicantumkan secara tegas mengakhiri pencarian maksud dari satu perundang-undangan. Adapun contohnya adalah penyebutan subjek yang merujuk pada makna yang diartikan dalam undang-undang

2. Interpretasi teleologis atau sosiologis

Interpretasi teleologis atau sosiologis adalah metode penafsiran hukum atau interpretasi yang menetapkan makna undang-undang berdasarkan tujuan kemasyarakatan. [37]Dengan metode ini, undang-undang yang masih berlaku tetapi sudah usang diterapkan pada kebutuhan atau kepentingan masa kini, tidak peduli apakah hak itu dikenal pada saat diundang-undangkan atau tidak. Peraturan disesuaikan dengan situasi sosial baru. Dengan kata lain, peraturan hukum yang lama (masih berlaku) disesuaikan dengan keadaan baru atau diaktualisasikan.

3. Interpretasi sistematis atau logis

Interpretasi sistematis atau logis adalah metode penafsiran hukum yang menafsirkan undang-undang sebagai bagian dari keseluruhan sistem perundang-undangan dengan menghubungkannya dengan undang-undang lain. Interpretasi ini dilakukan karena sejatinya undang-undang

[37] Sudikno Mertokusumo dan A. Pitlo, **Ibid.**, **hlm**. **17**.

selalu berkaitan dengan peraturan perundang-undangan lainnya; tidak ada yang berdiri sendiri.

4. Interpretasi historis

   Interpretasi historis adalah metode penafsiran hukum yang menafsirkan makna peraturan perundang-undangan dengan meneliti sejarah pembentukannya. Ada dua macam interpretasi historis, yakni menurut sejarah undang-undang dan menurut sejarah hukum. Sebagai informasi tambahan, Interpretasi menurut sejarah undang-undang dikenal juga sebagai interpretasi subjektif. Hal ini disebabkan oleh penafsirannya disesuaikan pada pandangan subjektif pembentuk undang-undang.

5. Interpretasi komparatif atau perbandingan

   Interpretasi komparatif atau perbandingan adalah metode penafsiran yang dilakukan dengan membandingkan beberapa aturan hukum. Adapun tujuan hakim melakukan perbandingan tersebut adalah untuk mencari kejelasan makna dari suatu ketentuan undang-undang. Lebih lanjut menerangkan bahwa interpretasi ini dapat dilakukan dengan membandingkan penerapan asas-asas hukum atau *rechtsbeginselen* dalam peraturan perundang-undangan yang lain dan/atau aturan hukumnya *rechtsregel*, di samping perbandingan tentang sejarah pembentukan hukumnya.

6. Interpretasi futuristis

   Interpretasi futuristis adalah metode penafsiran hukum yang bersifat antisipasi dengan menggunakan penjelasan ketentuan undang-undang yang belum berlaku atau belum berkekuatan hukum tetap. Lebih lanjut

menerangkan bahwa metode penafsiran hukum dengan interpretasi futuristis ini lebih bersifat *ius constituendum* (hukum atau undang-undang yang dicitakan) daripada *ius constitutum* (hukum atau undang-undang yang berlaku saat ini.

Dalam penelitian ini penulis menggunakan teori penafsiran hukum sistematis atau logis dan Interpretasi komparatif atau perbandingan. teori penafsiran hukum sistematis atau logis yaitu teori yang menafsirkan undang-undang sebagai bagian dari keseluruhan sistem perundang-undangan dengan menghubungkannya dengan undang-undang lain. Sedangkan Interpretasi komparatif atau perbandingan adalah metode penafsiran yang dilakukan dengan membandingkan beberapa aturan hukum.

2. 2 Kajian Pustaka

2.2.1 Pengertian Akses Tidak Sah

Akses tidak sah merupakan suatu tindakan memasuki, memperoleh, atau menggunakan sistem elektronik maupun data yang terdapat di dalamnya tanpa hak, tanpa izin, atau melawan hukum[38]. Dalam konteks sistem elektronik, akses tidak sah merujuk pada segala bentuk intervensi terhadap sistem, jaringan, atau data oleh pihak yang tidak memiliki otorisasi. Tindakan ini dapat berupa peretasan (*hacking*), penyusupan sistem, hingga pengambilan data tanpa persetujuan pemiliknya[39].

[38] Puteri, C. B., 2025, **Analisis Putusan Hakim terhadap Tindak Pidana Akses Ilegal**, Skripsi, Universitas Malikussaleh, hlm. 44.

[39] Nasrullah, M., dan Ramadhan, R., 2025, **Dasar-Dasar Keamanan Informasi dan Siber**, Deepublish, hlm. 60.

Dalam hukum siber, akses ilegal terhadap data dikenal sebagai bentuk pelanggaran terhadap keamanan sistem informasi yang dapat mengancam kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) data. Konsep ini sejalan dengan istilah *unauthorized access* dalam keamanan sistem informasi, yaitu akses yang dilakukan oleh pihak yang tidak memiliki hak atau melampaui batas kewenangan yang diberikan. *Unauthorized access* sering menjadi pintu masuk terjadinya kejahatan siber lainnya, seperti pencurian data, manipulasi data, dan penyalahgunaan informasi[40].

Dalam hukum Indonesia, pengaturan mengenai akses tidak sah telah diatur dalam beberapa peraturan perundang-undangan. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 mengatur larangan akses tanpa hak terhadap sistem elektronik. Selain itu, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi juga menegaskan pentingnya perlindungan terhadap data pribadi dari akses yang tidak sah, khususnya melalui kewajiban Pengendali Data Pribadi untuk menjamin keamanan data yang dikelolanya. Dengan demikian, akses tidak sah merupakan salah satu bentuk ancaman utama dalam perlindungan data pribadi yang harus dicegah melalui pengaturan hukum dan penerapan sistem keamanan yang memadai[41].

[40] Pratama, A. M., Syaiful, M., dan Rahman, M. F., 2024, **Keamanan Data dan Informasi**, Kaizen Media Publishing, hlm. 48.

[41] Nur, A. W., Rijal, B. M. D. M., dan Mustafa, D. W., 2024, **Tanggung Jawab Pelaksana Sistem Elektronik**, Legal Journal of Law, Volume 3 Nomor 1, hlm. 20.

2.2.2 Pengertian Data Pribadi

Data pribadi adalah setiap data tentang seseorang yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasikan dengan informasi lainnya, baik secara langsung maupun tidak langsung melalui sistem elektronik maupun non-elektronik. Definisi ini sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang menempatkan data pribadi sebagai bagian dari hak privasi individu yang wajib dilindungi[42].

Dalam Undang-Undang tersebut, data pribadi dibedakan menjadi dua jenis, yaitu data pribadi yang bersifat umum dan data pribadi yang bersifat spesifik. Data pribadi umum meliputi nama lengkap, jenis kelamin, kewarganegaraan, agama, dan/atau data lain yang tidak termasuk kategori sensitif. Sementara itu, data pribadi spesifik mencakup data yang memiliki tingkat sensitivitas tinggi, seperti data kesehatan, data biometrik, data genetika, catatan kejahatan, data keuangan pribadi, serta data lain yang apabila disalahgunakan dapat menimbulkan dampak serius bagi individu.

Karakteristik data pribadi antara lain bersifat individual, melekat pada seseorang, serta memiliki nilai yang tinggi baik dari sisi ekonomi maupun sosial. Data pribadi juga bersifat dinamis karena dapat berubah seiring waktu dan perkembangan teknologi. Oleh karena itu, pengelolaan data pribadi harus dilakukan secara hati-hati dengan memperhatikan prinsip-prinsip perlindungan data, seperti keabsahan, transparansi, pembatasan tujuan, dan keamanan.

[42] Watkat, F. X., Ingratubun, M. T., dan Apriyanti, A., 2024, **Perlindungan Data Pribadi Melalui Sistem Hukum Pidana**, Jurnal Hukum Ius Publicum, Volume 5 Nomor 1, hlm. 155.

Pentingnya perlindungan data pribadi semakin meningkat di era digital, terutama dengan berkembangnya teknologi informasi dan sistem *e-commerce* yang melibatkan pengumpulan dan pemrosesan data dalam jumlah besar. Tanpa adanya perlindungan yang memadai, data pribadi dapat dengan mudah disalahgunakan oleh pihak yang tidak bertanggung jawab, yang pada akhirnya dapat merugikan pemilik data. Oleh karena itu, perlindungan data pribadi menjadi hal yang sangat penting untuk menjamin hak privasi individu serta menciptakan kepercayaan dalam penggunaan teknologi digital.

2.2.3 Pengertian Pengendali Data

Pengendali Data Pribadi adalah setiap orang, badan publik, atau organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali terhadap pemrosesan data pribadi. Definisi ini sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang menempatkan Pengendali Data Pribadi sebagai pihak utama yang bertanggung jawab atas pengelolaan data pribadi[43].

Dalam praktiknya, Pengendali Data Pribadi berbeda dengan Prosesor Data Pribadi. Pengendali Data Pribadi memiliki kewenangan untuk menentukan tujuan dan kebijakan pemrosesan data pribadi, sedangkan Prosesor Data Pribadi hanya bertindak untuk memproses data atas dasar instruksi dari Pengendali Data Pribadi. Dengan kata lain, Pengendali Data Pribadi memiliki peran strategis dalam

[43] Arrasuli, B. K., dan Fahmi, K., 2023, **Perlindungan Hukum terhadap Penyalahgunaan Data Pribadi**, UNES Journal of Swara Justisia, Volume 7 Nomor 2, hlm. 372.

menentukan bagaimana data pribadi dikumpulkan, digunakan, disimpan, dan dilindungi, sementara Prosesor Data Pribadi bersifat sebagai pelaksana teknis[44].

Peran dan tanggung jawab Pengendali Data Pribadi dalam pemrosesan data pribadi sangat luas, meliputi kewajiban untuk memastikan bahwa pemrosesan data dilakukan secara sah, transparan, dan sesuai dengan tujuan yang telah ditentukan. Selain itu, Pengendali Data Pribadi juga bertanggung jawab untuk menjamin keamanan data pribadi, termasuk mencegah terjadinya akses tidak sah, kebocoran data, dan penyalahgunaan informasi. Kewajiban ini menjadi sangat penting mengingat posisi Pengendali Data Pribadi sebagai pihak yang memiliki kendali penuh terhadap data yang diproses[45].

Dalam sistem elektronik, kedudukan Pengendali Data Pribadi sangat strategis karena menjadi pihak yang menentukan kebijakan dan standar dalam pengelolaan data pribadi. Dalam konteks *e-commerce*, Pengendali Data Pribadi biasanya adalah penyelenggara platform yang mengumpulkan dan mengelola data pengguna. Oleh karena itu, Pengendali Data Pribadi memiliki tanggung jawab hukum yang besar untuk memastikan bahwa data pribadi pengguna terlindungi secara optimal.

2.2.4 Pengertian E-Commerce

E-commerce atau perdagangan elektronik merupakan kegiatan transaksi jual beli barang dan/atau jasa yang dilakukan melalui media elektronik, khususnya

[44] Jebaru, R. A., dan Widiatno, M. W., 2026, **Perlindungan Hukum bagi Prosesor Data Pribadi**, Jurnal Pengabdian Masyarakat dan Riset Pendidikan, Volume 4 Nomor 3, hlm. 19565.

[45] Pradana, M. A. E., dan Saragih, H., 2024, **Prinsip Akuntabilitas dalam UU PDP terhadap GDPR**, Innovative Journal of Social Science Research, Volume 4 Nomor 4, hlm. 3415.

melalui jaringan internet. Menurut para ahli, *e-commerce* dapat diartikan sebagai proses pertukaran barang, jasa, dan informasi melalui jaringan elektronik yang memungkinkan terjadinya transaksi tanpa pertemuan langsung antara penjual dan pembeli[46].

Perdagangan elektronik memiliki beberapa karakteristik utama, antara lain tidak dibatasi oleh ruang dan waktu, memanfaatkan teknologi informasi sebagai media utama transaksi, serta melibatkan pertukaran data secara digital. Selain itu, *e-commerce* juga memungkinkan proses transaksi yang lebih cepat, efisien, dan menjangkau pasar yang lebih luas dibandingkan dengan perdagangan konvensional[47].

Jenis-jenis *e-commerce* dapat dibedakan berdasarkan pelaku transaksi, yaitu *Business to Business* (B2B), yaitu transaksi antara pelaku usaha dengan pelaku usaha lainnya; *Business to Consumer* (B2C), yaitu transaksi antara pelaku usaha dengan konsumen; serta *Consumer to Consumer* (C2C), yaitu transaksi antar konsumen melalui platform tertentu. Masing-masing jenis *e-commerce* memiliki karakteristik dan mekanisme yang berbeda, namun semuanya melibatkan penggunaan sistem elektronik dalam pelaksanaannya[48].

Dalam sistem *e-commerce*, penggunaan data pribadi menjadi hal yang tidak terpisahkan. Data pribadi digunakan untuk berbagai keperluan, seperti proses registrasi akun, verifikasi identitas, transaksi pembayaran, hingga

[46] Satory, A., dan Nuraeni, Y., 2024, **Regulasi E-Commerce**, Multilingual Journal of Universal Studies, Volume 4 Nomor 4, hlm. 66.

[47] Yulia, Y., 2024, **Perlindungan Hukum dalam Transaksi Kontrak E-Commerce**, Al Wasath Jurnal Ilmu Hukum, Volume 5 Nomor 1, hlm. 30.

[48] *Ibid*, hlm. 32.

pengiriman barang. Oleh karena itu, keberadaan data pribadi dalam sistem *e-commerce* memiliki nilai yang sangat penting, namun juga menimbulkan risiko apabila tidak dikelola dengan baik. Hal ini menjadikan perlindungan data pribadi sebagai aspek yang sangat krusial dalam penyelenggaraan sistem *e-commerce*, guna menjaga kepercayaan pengguna serta menjamin keamanan informasi pribadi mereka.

2.2.5 Pengertian Perlindungan Data Pribadi

Perlindungan data pribadi merupakan segala upaya untuk melindungi data pribadi seseorang agar tidak disalahgunakan oleh pihak yang tidak berwenang, serta untuk menjamin hak privasi individu dalam proses pengumpulan, pengolahan, penyimpanan, dan penyebaran data. Dalam konteks hukum, perlindungan data pribadi menjadi bagian dari perlindungan hak asasi manusia, khususnya hak atas privasi, yang harus dijamin oleh negara melalui pengaturan perundang-undangan[49].

Tujuan utama dari perlindungan data pribadi adalah untuk memberikan rasa aman kepada individu dalam penggunaan teknologi informasi, mencegah terjadinya penyalahgunaan data, serta menjamin bahwa data pribadi digunakan sesuai dengan tujuan yang sah dan telah disetujui oleh pemilik data. Selain itu, perlindungan data pribadi juga bertujuan untuk menciptakan kepercayaan masyarakat terhadap sistem elektronik, termasuk dalam aktivitas *e-commerce*[50].

Dalam pelaksanaannya, perlindungan data pribadi didasarkan pada beberapa prinsip utama, antara lain prinsip keabsahan dan persetujuan, prinsip

[49] Suharyanti, N. P. N., dan Sutrisni, N. K., 2021, **Urgensi Perlindungan Data Pribadi**, Prosiding Seminar Nasional FH Unmas, Volume 1 Nomor 1, hlm. 120.

[50] *Ibid*, hlm. 125.

transparansi, prinsip pembatasan tujuan, prinsip minimalisasi data, prinsip akurasi, serta prinsip keamanan data. Prinsip-prinsip ini menjadi pedoman bagi Pengendali Data Pribadi dalam mengelola data secara bertanggung jawab dan sesuai dengan ketentuan hukum yang berlaku[51].

Perlindungan hak privasi dalam sistem elektronik menjadi semakin penting seiring dengan meningkatnya penggunaan teknologi digital. Dalam sistem elektronik, data pribadi sangat rentan terhadap berbagai ancaman seperti akses tidak sah, kebocoran data, dan penyalahgunaan informasi. Oleh karena itu, perlindungan data pribadi tidak hanya bersifat normatif, tetapi juga harus didukung oleh sistem keamanan yang memadai untuk memastikan bahwa hak privasi individu tetap terjaga dalam lingkungan digital.

2.2.6 Pengertian Keamanan Data Pribadi

Keamanan data pribadi merupakan upaya untuk melindungi data pribadi dari berbagai ancaman, baik yang berasal dari dalam maupun luar sistem, sehingga data tersebut tetap aman, tidak rusak, tidak hilang, dan tidak diakses oleh pihak yang tidak berwenang. Dalam sistem elektronik, keamanan data pribadi menjadi aspek yang sangat penting karena data diproses dan disimpan secara digital yang rentan terhadap serangan siber[52].

Tujuan utama dari keamanan data dalam pengolahan informasi digital adalah untuk menjaga kerahasiaan data, memastikan keutuhan data, serta

---

[51] Pradana, M. A. E., dan Saragih, H., 2024, **Prinsip Akuntabilitas dalam Undang-Undang Perlindungan Data Pribadi terhadap GDPR dan Akibat Hukumnya**, Innovative: Journal of Social Science Research, Volume 4 Nomor 4, hlm. 3415.

[52] Aswandi, R., Muchin, P. R. N., dan Sultan, M., 2020, **Perlindungan Data dan Informasi Pribadi**, Jurnal Legislatif, hlm. 170.

menjamin ketersediaan data saat dibutuhkan. Hal ini sejalan dengan prinsip dasar keamanan data yang dikenal dengan konsep *confidentiality*, *integrity*, dan *availability*. *Confidentiality* berarti bahwa data hanya dapat diakses oleh pihak yang berwenang, *integrity* berarti bahwa data harus tetap utuh dan tidak mengalami perubahan yang tidak sah, sedangkan *availability* berarti bahwa data harus tersedia dan dapat diakses saat dibutuhkan oleh pihak yang berwenang[53].

Peran sistem keamanan sangat penting dalam mencegah terjadinya akses tidak sah terhadap data pribadi. Sistem keamanan yang baik harus mampu mendeteksi, mencegah, dan menanggulangi berbagai ancaman terhadap data, seperti peretasan, pencurian data, maupun kebocoran informasi. Oleh karena itu, penerapan teknologi keamanan seperti enkripsi, autentikasi, dan kontrol akses menjadi bagian penting dalam perlindungan data pribadi[54]. Dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, keamanan data menjadi salah satu kewajiban utama bagi Pengendali Data Pribadi. Pengendali data diwajibkan untuk menerapkan sistem keamanan yang andal, aman, dan bertanggung jawab guna melindungi data pribadi dari akses tidak sah[55].

---

[53] Pardosi, V. B. A., Deta, B., Nugroho, F., dan Vandika, A. Y., 2024, **Sistem Keamanan Informasi**, hlm. 52.

[54] Yudistira, M., dan Ramadani, R., 2023, **Tinjauan Yuridis terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 oleh KOMINFO**, UNES Law Review, Volume 5 Nomor 4, hlm. 3920.

[55] Prameswari, Y., 2026, **Penerapan UU PDP oleh Kreditur**, Dialog Legal, Volume 2 Nomor 1, hlm. 68.