

BAB I

PENDAHULUAN

1.1 Latar Belakang

Gaya Hidup masyarakat Indonesia termasuk komunikasi, transaksi, dan layanan publik, telah mengalami transformasi akibat perkembangan teknologi informasi. Komunikasi dan transaksi yang efektif merupakan hasil dari perkembangan teknologi informasi, telah berubah. Dengan penggunaan internet yang semakin luas, layanan platform digital juga terus berkembang. Penggunaan media sosial tentu saja tidak lepas dari dampak positif dan negatif yang didapatkan, baik dampak langsung kepada penggunanya atau pihak lain terkait dengan konten media sosial tersebut. Internet pun dapat berperan menjadi pedang bermata dua.¹

Peningkatan penggunaan internet juga telah menyebabkan ketergantungan yang semakin besar pada platform digital. Namun, pertumbuhan ini melibatkan risiko keamanan digital, yang semakin kompleks, terutama terkait dengan kebocoran data pribadi dan kerentanan dalam sistem elektronik. Pada tahun 2024, tercatat 21.769.496 kasus peretasan email di Indonesia, menjadikan negara ini sebagai sumber kebocoran data terbesar ketiga di ASEAN. Di tingkat nasional, Kementerian Komunikasi dan Informatika (Kominfo) menangani 124 kasus dugaan pelanggaran perlindungan data pribadi sepanjang 2019 hingga Mei 2024, dengan 111 kasus di antaranya berupa kebocoran data pribadi. Setiap kasus bahkan dapat melibatkan ratusan juta data penduduk, menunjukkan betapa masifnya dampak yang ditimbulkan. Fakta ini menegaskan bahwa pengguna platform digital berada dalam posisi yang rentan terhadap kerugian akibat kelalaian Penyelenggara Sistem Elektronik (PSE).

Tabel 1. 1 Kasus Kebocoran Data

Tahun	Jumlah Kasus Kebocoran Data
2019-2023	111 kasus
2024	21.769.496 akun email dibobol
2024	300 juta data pribadi bocor (PDNS)

Sumber: Kominfo & GoodStats, 2025

¹ Djaja Ermansyah, *Penyelesaian Sengketa Hukum Teknologi Informasi Dan Transaksi Elektronik*, Pustaka Timur, Jakarta, 2010), h. 17-25.

Selain itu, meningkatnya intensitas aktivitas digital juga memperluas potensi kerugian yang dapat dialami pengguna. Kerugian tersebut tidak hanya bersifat material, seperti kehilangan dana akibat pembobolan akun, tetapi juga bersifat immaterial, seperti kecemasan, tekanan psikologis, atau rusaknya reputasi akibat penyalahgunaan data pribadi.² Dalam beberapa kasus, kebocoran data bahkan dapat berdampak jangka panjang karena informasi yang telah tersebar di ruang digital sulit untuk dihapus sepenuhnya. Situasi ini memperlihatkan bahwa kerugian akibat kegagalan sistem elektronik tidak lagi dapat dipandang sebagai persoalan teknis semata, melainkan sebagai isu sosial yang menyentuh aspek keamanan, kenyamanan, dan martabat pengguna. Kebocoran data pribadi di Indonesia merupakan masalah serius yang berdampak pada berbagai aspek kehidupan masyarakat

Di tengah pesatnya digitalisasi, masyarakat kini semakin bergantung pada layanan berbasis teknologi untuk memenuhi kebutuhan sehari-hari mulai dari berbelanja, mengakses layanan kesehatan, hingga berinteraksi melalui media sosial. Ketergantungan ini membuat pengguna tanpa sadar menyerahkan banyak aspek kehidupan pribadinya kepada Penyelenggara Sistem Elektronik (PSE). Namun, tidak semua pengguna memiliki pemahaman yang memadai tentang risiko keamanan digital yang menyertai penggunaan platform tersebut. Ketimpangan literasi digital ini membuat posisi pengguna semakin rentan ketika terjadi kebocoran data, kegagalan sistem, atau penyalahgunaan informasi pribadi. Kondisi tersebut menunjukkan bahwa persoalan perlindungan hukum tidak hanya berkaitan dengan aspek teknis keamanan, tetapi juga menyangkut ketidakseimbangan posisi antara pengguna dan PSE yang semakin nyata dalam ekosistem digital saat ini.

Khususnya di sektor *e-commerce*, yang menjadi fokus utama penelitian ini, ketergantungan ini semakin akut karena melibatkan transaksi finansial, data pembayaran, dan informasi pribadi yang sensitif. Menurut laporan GoodStats (2024), nilai transaksi *e-commerce* di Indonesia mencapai Rp500 triliun pada 2024, dengan peningkatan 25% dari tahun sebelumnya, namun disertai peningkatan 30%

² Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, New York, 2019, h. 35.

kasus kebocoran data terkait platform belanja online. Platform *e-commerce* seperti Tokopedia, Shopee, atau Bukalapak tidak hanya memfasilitasi jual-beli, tapi juga mengumpulkan data besar-besaran untuk personalisasi layanan, yang jika bocor dapat memicu penipuan finansial, identity theft, dan kerugian ekonomi langsung bagi pengguna. Ahmad M. Ramli dalam bukunya menyatakan bahwa PSE di *e-commerce* memiliki tanggung jawab lebih tinggi karena sifat transaksionalnya, sebagaimana diatur dalam Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik, di mana kelalaian keamanan dapat dianggap sebagai pelanggaran perlindungan konsumen.

Perkembangan teknologi digital juga membawa perubahan besar dalam cara masyarakat memahami keamanan dan privasi. Banyak pengguna merasa bahwa penggunaan platform digital adalah bagian alami dari kehidupan modern sehingga mereka cenderung mengabaikan risiko yang mungkin timbul. Ketika sebuah aplikasi meminta akses data, sebagian besar pengguna hanya menekan tombol “setuju” tanpa membaca ketentuan yang berlaku. Fenomena ini menunjukkan bahwa hubungan antara pengguna dan PSE sering kali tidak berada pada posisi yang seimbang. Pengguna berada pada posisi yang lebih lemah karena keterbatasan informasi dan pemahaman, sementara PSE memiliki kendali penuh atas sistem, data, dan kebijakan internal yang mengatur penggunaan layanan.

Kebocoran data tidak hanya menjadi tantangan teknis, tetapi juga memiliki konsekuensi langsung bagi pengguna, seperti pencurian identitas, penyalahgunaan akun, dan penipuan digital. Menurut laporan GoodStats, 300 juta data pribadi dicuri dalam insiden di Pusat Data Nasional Sementara (PDNS) pada tahun 2024. Insiden berskala besar ini menunjukkan bahwa bahkan sistem elektronik pemerintah pun tidak sepenuhnya aman, sehingga meningkatkan risiko bagi pengguna platform digital.³ Di tengah kompleksitas tersebut, masyarakat semakin membutuhkan jaminan bahwa negara hadir untuk melindungi hak-hak mereka sebagai pengguna layanan digital. Namun, realita di lapangan menunjukkan bahwa penegakan hukum

³ Zakia Machfir, '300 Juta Data Pribadi Tersebar, Kapan Indonesia Merdeka Dari Serangan Siber?', GoodStats (online), 2 Juli 2024, <https://goodstats.id/article/300-juta-data-pribadi-tersebar-pusat-data-nasional-sementara-pdns-dibobol-kapan-indonesia-merdeka-dari-serangan-siber-5Adzr>.

di bidang teknologi informasi masih menghadapi berbagai tantangan, mulai dari keterbatasan mekanisme pengawasan hingga belum optimalnya koordinasi antar lembaga. Banyak kasus kebocoran data yang tidak diikuti dengan kejelasan mengenai pihak yang bertanggung jawab atau bentuk pemulihan yang diberikan kepada korban. Kondisi ini menimbulkan pertanyaan mendasar mengenai efektivitas perlindungan hukum yang tersedia saat ini.

Walaupun Indonesia telah menetapkan kerangka hukum seperti Undang-Undang Informasi dan Transaksi Elektronik Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik dan Undang-Undang Perlindungan Data Pribadi, masih ada beberapa masalah dalam menerapkannya.⁴

PSE diwajibkan oleh undang-undang untuk memastikan bahwa sistem elektronik mereka andal, aman, dan dapat dipertanggungjawabkan. Namun, terdapat banyak kasus yang menunjukkan bahwa sejumlah PSE tidak memenuhi standar tersebut. Ketika kerugian terjadi, pengguna seringkali kesulitan untuk menuntut pertanggungjawaban akibat mekanisme penyelesaian sengketa yang tidak efektif. Hal ini didukung oleh studi-studi sebelumnya yang menyoroti perlindungan hukum yang lemah bagi pengguna dalam praktiknya. Kesenjangan antara norma hukum dan implementasi di lapangan menimbulkan pertanyaan mengenai efektivitas perlindungan hukum yang tersedia. Banyak pengguna tidak memahami hak-haknya, sementara PSE sering kali tidak transparan dalam pengelolaan data dan keamanan sistem. Kondisi ini menciptakan ketidakseimbangan posisi antara pengguna dan PSE, sehingga perlindungan hukum menjadi semakin penting untuk diteliti secara mendalam.

Kasus kebocoran data pada platform digital swasta menjadi bukti nyata ketidakmampuan PSE dalam melindungi data pengguna. Salah satu contoh paling menonjol adalah insiden kebocoran data Tokopedia pada Mei 2020. Sebanyak 91

⁴ Bintang RIZky Alfathi, 'Laporan Kebocoran Data Indonesia 2024', GoodStats (online), 5 Februari 2025, https://data.goodstats.id/statistic/indonesia-peringkat-ke-3-negara-asean-dengan-kebocoran-data-terbanyak-AtcAs#google_vignette.

juta akun pengguna dan 7 juta akun merchant diretas, dengan data yang dijual di dark web seharga sekitar US\$5.000. Data yang bocor mencakup user ID, email, nama lengkap, tanggal lahir, jenis kelamin, nomor telepon, dan password yang masih di-hash.⁵ Insiden ini tidak hanya menimbulkan risiko pencurian identitas dan penipuan, tetapi juga menyoroti kelalaian PSE dalam menerapkan standar keamanan siber yang memadai, sebagaimana diwajibkan oleh regulasi seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik

Dalam kasus Tokopedia, Komunitas Konsumen Indonesia (KKI) mengajukan gugatan perbuatan melawan hukum ke Pengadilan Negeri Jakarta Pusat dengan Nomor Perkara 235/PDT.G/2020/PN.JKT.PST terhadap Menteri Komunikasi dan Informatika serta PT Tokopedia. Gugatan ini menuntut pencabutan pendaftaran PSE Tokopedia, denda administratif Rp100 miliar, serta pernyataan permintaan maaf secara publik di media massa. Putusan pengadilan menyatakan bahwa Tokopedia telah melakukan wanprestasi karena gagal memenuhi kewajiban kontraktual sebagai PSE untuk menjaga kerahasiaan dan keamanan data pribadi pengguna, sebagaimana diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (Pasal 15 UU ITE) dan Pasal 3 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Meskipun Tokopedia mengklaim bahwa password tetap terlindungi melalui hashing, fakta bahwa data pribadi tersebar luas menimbulkan kerugian immaterial berupa risiko phishing, penipuan keuangan, dan hilangnya kepercayaan publik terhadap platform *e-commerce*.

Kasus ini menjadi yurisprudensi penting dalam hukum Indonesia, menunjukkan bahwa pengguna platform digital memiliki hak untuk mengajukan gugatan perdata langsung terhadap PSE, baik secara individu maupun melalui *class action*, serta melibatkan Kementerian Komunikasi dan Informatika (Kominfo) sebagai regulator pengawas. Namun, hingga kini, banyak korban masih kesulitan memperoleh

⁵ Ramiz Afif Naufal, “*Tanggung Jawab PT. Tokopedia Dalam Kasus Kebocoran Data Pribadi Pengguna*”, Skripsi, Fakultas Hukum Universitas Islam Indonesia, Yogyakarta, 2020, h.9.

kompensasi nyata karena mekanisme penyelesaian sengketa yang rumit dan kurangnya transparansi dari pihak platform. Dalam perspektif hukum perdata, kerugian yang dialami pengguna dapat dikategorikan sebagai kerugian materiil seperti kehilangan dana akibat penipuan dan immateriil seperti stres psikologis atau rusaknya reputasi. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang diberlakukan pasca-insiden ini semakin memperkuat dasar hukum untuk menuntut ganti rugi, di mana Pasal 46 UU PDP mengatur bahwa pengendali data pribadi termasuk PSE bertanggung jawab atas kegagalan perlindungan data, termasuk kebocoran akibat kelalaian.⁶

Dari sudut pandang administratif, Kominfo sebagai otoritas pengawas PSE memiliki wewenang untuk memberikan sanksi, termasuk pencabutan izin operasional jika PSE terbukti lalai. Dalam kasus Tokopedia, meskipun tidak ada pencabutan izin, Kominfo melakukan audit dan memerintahkan perbaikan sistem keamanan. Namun, efektivitas sanksi ini masih dipertanyakan, karena insiden serupa terus berulang di platform lain. Secara pidana, kebocoran data dapat dikenai Pasal 32 UU ITE yang mengancam pidana hingga 10 tahun penjara bagi pihak yang dengan sengaja mengakses sistem elektronik tanpa hak, meskipun dalam kasus ini, pelaku utama adalah hacker eksternal, PSE tetap dapat diminta pertanggungjawaban atas kelalaian keamanan.

Kasus Tokopedia juga menegaskan pola umum di Indonesia: PSE cenderung minim investasi keamanan siber dibandingkan keuntungan bisnis. Menurut laporan analis independen, kebocoran data tidak hanya menimbulkan kerugian langsung bagi pengguna seperti pencurian dana atau penipuan online, tetapi juga kerugian jangka panjang berupa rusaknya reputasi digital, stres psikologis, dan hilangnya kepercayaan terhadap ekosistem digital secara keseluruhan. Kondisi ini semakin ironis karena Indonesia telah memiliki kerangka hukum komprehensif seperti UU PDP, namun penegakan hukum terhadap PSE masih bersifat reaktif dan jarang memberikan efek jera. Banyak korban kesulitan membuktikan kausalitas kerugian,

⁶ Ragil Putri Anindya dan Achmad Edi Subiyanto, "Tanggung Jawab Platform Tokopedia dalam Kasus Kebocoran Data Menurut Undang-Undang Tentang Perlindungan Data Pribadi," *Journal Of Artificial Intelligence and Digital Business (RIGGS)* 4, No. 3, 2025, h. 1105-1112.

sementara PSE kerap mengandalkan klausul "*force majeure*" atau "*safe harbour*" untuk menghindari pertanggungjawaban penuh.⁷

Melihat tingginya angka kebocoran data, lemahnya implementasi regulasi, dan besarnya kerugian yang dialami pengguna, penelitian mengenai perlindungan hukum pengguna platform digital terhadap kerugian yang ditimbulkan oleh PSE menjadi sangat relevan. Oleh karena itu, penulis memilih judul “**Perlindungan Hukum Pengguna Platform Digital terhadap Kerugian yang Ditimbulkan oleh Penyelenggara Sistem Elektronik**” yang berfokus pada *e-commerce* dengan analisis komprehensif mengenai pengaturan hukum tentang batasan kerugian yang berlaku serta bentuk tanggung jawab dari PSE.

1.2. Rumusan Masalah

1. Bagaimana batasan kerugian yang ditimbulkan oleh penyelenggara *e-commerce* akibat kebocoran data pribadi konsumen yang dapat dimintakan pertanggung jawaban hukum?
2. Bagaimana bentuk tanggung jawab hukum penyelenggara *e-commerce* atas kebocoran data yang dialami konsumen?

1.3. Tujuan penelitian

1. Mengetahui pengaturan mengenai batasan kerugian yang ditimbulkan oleh Penyelenggara Sistem Elektronik yang dapat dimintakan pertanggung jawaban hukum.
2. Mengetahui bentuk tanggung jawab hukum PSE atas kerugian yang dialami pengguna sistem elektronik.

⁷ Muhammad Fathur, “Tanggung Jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen,” in *2nd National Conference on Law Studies: Legal Development Towards A Digital Society Era*, 2020, 978-979.

1.4. Manfaat penelitian

1.4.1 Manfaat Teoritis

Secara teoritis, penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan ilmu hukum, khususnya dalam bidang hukum siber, perlindungan data pribadi, dan tanggung jawab Penyelenggara Sistem Elektronik (PSE). Penelitian ini memperkaya literatur akademik dengan analisis mengenai kesenjangan antara norma hukum yang berlaku dengan implementasi di lapangan, sehingga dapat menjadi referensi bagi mahasiswa, dosen, maupun peneliti lain yang mengkaji isu serupa. Selain itu, penelitian ini juga memperkuat pemahaman mengenai konsep tanggung jawab hukum PSE dalam konteks kerugian pengguna platform digital, serta memberikan landasan teoritis untuk pengembangan kajian hukum di era digital.

1.4.2 Manfaat Praktis

Secara praktis, penelitian ini diharapkan dapat memberikan masukan konstruktif bagi berbagai pihak. Bagi Penyelenggara Sistem Elektronik, penelitian ini dapat menjadi bahan evaluasi untuk meningkatkan standar keamanan sistem, kepatuhan terhadap regulasi, serta transparansi dalam pengelolaan data pribadi. Bagi pengguna platform digital, penelitian ini memberikan pemahaman mengenai hak-hak hukum yang dimiliki serta mekanisme perlindungan yang tersedia ketika terjadi kerugian akibat kegagalan sistem elektronik. Bagi perguruan tinggi, penelitian ini berkontribusi pada pengembangan kurikulum dan mata kuliah terkait hukum digital, sekaligus memperkuat posisi institusi sebagai pusat kajian yang responsif terhadap perkembangan teknologi dan tantangan hukum kontemporer.

1.5. Tinjauan Pustaka

1.5.1 Landasan Konseptual

1.5.1.1 Konsep Penyelenggara Sistem Elektronik (PSE)

Penyelenggara Sistem Elektronik dapat dibagi menjadi dua ruang lingkup meliputi:⁸

⁸ Pemerintah Pusat Indonesia, “Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik,” Pub. L. No. 71 (2018).

1. Penyelenggara Sistem Elektronik Lingkup Publik

Penyelenggara sistem elektronik dalam lingkup publik adalah pelaksanaan sistem elektronik oleh entitas yang merupakan bagian dari instansi penyelenggara negara atau oleh institusi yang ditunjuk oleh instansi penyelenggara negara. Badan publik mencakup lembaga-lembaga seperti eksekutif, legislatif, yudikatif, serta badan-badan lain yang memiliki fungsi dan tugas utama yang terkait dengan administrasi negara. Sumber dana badan publik dapat berasal dari Anggaran Pendapatan dan Belanja Negara atau Anggaran Pendapatan dan Belanja Daerah, dan organisasi nonpemerintah juga dapat termasuk jika sebagian atau seluruh pendanaannya berasal dari sumber-sumber tersebut, seperti sumbangan masyarakat atau pendanaan asing.

Sebuah badan publik dapat berperan sebagai Penyelenggara Sistem Elektronik Lingkup Publik, yang mengacu pada penyelenggaraan sistem elektronik oleh instansi penyelenggara negara atau institusi yang ditunjuk oleh instansi penyelenggara negara. Selanjutnya, dalam peran ini, badan publik dapat berfungsi sebagai Pengendali Data Pribadi, yang merujuk pada setiap individu, badan publik, atau organisasi internasional yang, baik secara mandiri maupun bersama-sama, menentukan tujuan dan mengendalikan proses pemrosesan Data Pribadi.

2. Penyelenggara Sistem Elektronik Lingkup Privat Penyelenggara Sistem Elektronik Lingkup Privat merujuk kepada suatu badan yang mengelola sistem elektronik dan dapat berupa individu, badan usaha, atau kelompok masyarakat. Menurut Pasal 2 ayat (5) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggara Sistem Elektronik, definisi ini mencakup dua kriteria utama:

- a. Penyelenggara Sistem Elektronik yang diatur atau diawasi oleh kementerian atau lembaga pemerintah sesuai dengan ketentuan peraturan perundang-undangan; dan
- b. Penyelenggara Sistem Elektronik yang memiliki portal, situs, atau aplikasi dalam jaringan melalui internet yang digunakan untuk berbagai keperluan

Dalam literatur hukum Indonesia, istilah Penyelenggara Sistem Elektronik (PSE) merujuk pada pihak yang menyelenggarakan, mengelola, atau

mengoperasikan sistem elektronik untuk kepentingan publik maupun privat. Meskipun definisi formalnya terdapat dalam peraturan perundang-undangan, sejumlah buku dan jurnal hukum memberikan penjelasan akademik yang lebih luas. PSE adalah setiap pihak yang menyediakan layanan berbasis sistem elektronik, baik untuk pemrosesan data, penyimpanan, distribusi informasi, maupun penyediaan layanan digital lainnya. Makarim menekankan bahwa PSE memiliki tanggung jawab hukum terkait keamanan sistem, perlindungan data pribadi, dan keandalan layanan.⁹

Kajian lain oleh Rizal Simanjuntak menunjukkan bahwa platform digital memiliki karakteristik unik sebagai “*intermediary*” yang memfasilitasi interaksi antar pengguna, namun pada saat yang sama memiliki kekuasaan untuk mengatur perilaku pengguna melalui kebijakan internal.¹⁰ Simanjuntak menekankan bahwa posisi platform sebagai perantara sering kali menimbulkan ambiguitas tanggung jawab hukum, terutama ketika terjadi kerugian akibat konten atau aktivitas pengguna. Hal ini membuat regulasi PSE menjadi semakin penting untuk memastikan adanya kepastian hukum bagi pengguna.

Konsep perlindungan data pribadi dalam ranah hukum berlandaskan pada sejumlah prinsip fundamental, seperti keabsahan dalam proses pengumpulan data, keterbukaan dalam setiap tahap pemrosesan, serta pemberian hak kendali kepada individu atas informasi yang mereka miliki. Di berbagai negara, perlindungan data pribadi diatur melalui peraturan perundang-undangan yang menetapkan hak-hak subjek data sekaligus kewajiban bagi organisasi yang mengelola data tersebut. Salah satu contoh paling menonjol adalah *General Data Protection Regulation* (GDPR) di Uni Eropa, yang menetapkan standar perlindungan data pribadi yang sangat ketat dan menjatuhkan sanksi berat bagi setiap pelanggaran. Model regulasi

⁹ Edmon Makarim, *Hukum Siber Indonesia*, RajaGrafindo Persada, Jakarta, 2019. h. 12-15

¹⁰ Rizal Simanjuntak, “Platform Digital Sebagai Intermediary dan Implikasi Tanggung Jawab Hukumnya,” *Jurnal Hukum & Teknologi* 5, No. 2, 2020, h. 101–118.

seperti ini kini mulai diadopsi oleh banyak negara di dunia sebagai upaya memperkuat keamanan dan tata kelola data pribadi.¹¹

Indonesia masih berada pada tahap transisi menuju rezim perlindungan data yang komprehensif. Berbeda dengan negara-negara Eropa yang telah memiliki tradisi panjang dalam perlindungan privasi, Indonesia baru mulai membangun ekosistem hukum yang terintegrasi. Oleh karena itu, implementasi Undang-Undang Perlindungan Data Pribadi (UU PDP) membutuhkan dukungan regulasi turunan, pedoman teknis, serta peningkatan literasi digital masyarakat agar hak privasi dapat terlindungi secara menyeluruh. Di sisi lain, Bambang Prasetyo menjelaskan bahwa hak privasi dalam konteks digital tidak lagi hanya berkaitan dengan kerahasiaan data, tetapi juga menyangkut *informational self-determination*, yaitu kemampuan individu untuk mengontrol bagaimana data pribadinya dikumpulkan, digunakan, dan disebar. Konsep ini penting karena banyak pengguna platform digital tidak sepenuhnya memahami konsekuensi dari persetujuan yang mereka berikan, sehingga posisi tawar mereka terhadap Penyelenggara Sistem Elektronik (PSE) menjadi semakin lemah.¹²

1.5.1.2 Konsep Perdagangan Elektronik (*e-commerce*)

Perdagangan elektronik atau *e-commerce* merupakan bentuk transaksi jual beli barang maupun jasa yang dilakukan melalui sistem elektronik berbasis internet. Dalam praktiknya, *e-commerce* mencakup berbagai model seperti *Business to Business* (B2B), *Business to Consumer* (B2C), dan *Consumer to Consumer* (C2C). Karakteristik utama dari *e-commerce* adalah adanya kontrak elektronik, penggunaan tanda tangan digital, serta keterlibatan pihak ketiga seperti payment gateway dan jasa logistik. Di Indonesia, regulasi mengenai *e-commerce* diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi

¹¹ M. Abdullah Sidiq, "Perlindungan Hukum Terhadap Rumah Sakit Atas Kebocoran Data Rekam Medik Elektronik yang Dilakukan Oleh Peretas," *AKADEMIK: Jurnal Mahasiswa Humanis* 5, No. 2, 2025, h. 605–20, <https://doi.org/10.37481/jmh.v5i2.1336>.

¹² Bambang Prasetyo, "Hak Privasi dan Pengendalian Data Pribadi Dalam Era Digital," *Jurnal Hukum & Pembangunan* 50, No. 3, 2020, h. 512–530,

Elektronik (UU ITE), Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik (PMSE), serta Permendag Nomor 50 Tahun 2020 yang mengatur kewajiban pendaftaran pelaku usaha, transparansi harga, dan perlindungan konsumen. Perlindungan hukum dalam transaksi *e-commerce* harus bersifat preventif dan represif agar konsumen tidak dirugikan oleh kelalaian penyelenggara sistem elektronik.¹³

Perdagangan elektronik atau *e-commerce* merupakan bentuk transaksi jual beli barang dan/atau jasa yang dilakukan secara elektronik melalui jaringan komputer, khususnya internet. *E-commerce* didefinisikan sebagai proses pembelian, penjualan, transfer, atau pertukaran produk, jasa, dan/atau informasi melalui jaringan komputer, termasuk internet. Definisi ini menekankan bahwa *e-commerce* bukan hanya sekadar transaksi jual beli, melainkan mencakup seluruh proses bisnis yang mendukungnya, seperti pemasaran digital, pembayaran elektronik, pengiriman, dan layanan pelanggan.¹⁴

Konsep *e-commerce* juga memiliki karakteristik utama, yaitu adanya kontrak elektronik, penggunaan tanda tangan digital, serta keterlibatan pihak ketiga seperti *payment gateway* dan jasa logistik. *E-commerce* bukan hanya alat transaksi, melainkan juga strategi bisnis yang memungkinkan perusahaan menjangkau pasar global, mengurangi biaya operasional, dan meningkatkan efisiensi rantai pasok. Dengan demikian, *e-commerce* menjadi fondasi penting dalam era ekonomi digital yang mendukung pertumbuhan usaha mikro, kecil, dan menengah (UMKM) serta meningkatkan daya saing perusahaan.

Dalam konteks Indonesia, *e-commerce* diatur secara khusus melalui Undang-Undang Nomor 7 Tahun 2014 tentang Perdagangan yang mendefinisikan perdagangan melalui sistem elektronik sebagai perdagangan yang transaksinya

¹³ Didik Kusuma Yadi, Muhammad Sood, dan Dwi Martini, "Perlindungan Hukum Bagi Para Pihak Dalam Transaksi E-Commerce Menurut Tata Hukum Indonesia," *Commerce Law* 2, No. 1, 2022, h. 23.

¹⁴ E Turban et al., *Electronic Commerce 2018: A Managerial and Social Networks Perspective*, Springer, Ninth edition, Swiss, 2018, h. 27-35.

dilakukan melalui serangkaian perangkat dan prosedur elektronik.¹⁵ Perkembangan *e-commerce* di Indonesia semakin pesat didorong oleh penetrasi internet dan penggunaan *smartphone*, sehingga menjadi bagian integral dari transformasi digital ekonomi nasional.

Perkembangan teknologi saat ini semakin memperkaya konsep *e-commerce* melalui integrasi dengan kecerdasan buatan (*Artificial Intelligence*), *big data analytics*, dan *Internet of Things* (IoT). Teknologi-teknologi ini memungkinkan personalisasi pengalaman belanja, prediksi perilaku konsumen, serta otomatisasi proses bisnis yang lebih efisien. Hal ini menjadikan *e-commerce* tidak hanya sebagai sarana transaksi, tetapi juga sebagai ekosistem bisnis yang dinamis dan adaptif terhadap perubahan perilaku konsumen di era digital.

Keunggulan utama *e-commerce* terletak pada kemampuannya menghilangkan batasan waktu dan tempat sehingga transaksi dapat dilakukan kapan saja dan di mana saja. Selain itu, *e-commerce* memungkinkan personalisasi layanan, analisis data konsumen yang lebih akurat, serta integrasi dengan media promosi visual dan digital marketing. Namun demikian, konsep *e-commerce* juga menghadapi berbagai tantangan, seperti isu keamanan data, perlindungan konsumen, kepastian hukum, serta persaingan yang semakin ketat.¹⁶ Oleh karena itu, keberhasilan implementasi *e-commerce* sangat bergantung pada dukungan regulasi yang kuat, infrastruktur teknologi yang memadai.

Selain itu, konsep *e-commerce* juga mencakup dimensi transformasi model bisnis yang bersifat disruptif. *E-commerce* tidak hanya mengubah cara transaksi dilakukan, tetapi juga merombak struktur rantai pasok tradisional menjadi model yang lebih efisien dan langsung (*direct-to-consumer*). Melalui platform digital, produsen dapat berinteraksi langsung dengan konsumen tanpa perantara yang berlebihan, sehingga mengurangi biaya distribusi dan meningkatkan margin

¹⁵ Johannes Johny Koynja et al., "Transaksi Perdagangan Melalui Sistem Elektronik Oleh Pelaku Usaha E-Commerce Dalam Memenuhi Target Penerimaan Perpajakan," *Jurnal Kompilasi Hukum* 4, No. 2, 2019, h. 78–84.

¹⁶ Ayatullah Sadali, *Buku Ajar E-Commerce*, Ruang Aksara Media, Yogyakarta, 2024, h.35

keuntungan. Perubahan ini mendorong munculnya fenomena disintermediation yang menjadi ciri khas ekonomi digital kontemporer.¹⁷

Dalam perspektif hukum, konsep *e-commerce* menuntut adanya keseimbangan yang tepat antara inovasi ekonomi dan perlindungan hukum terhadap konsumen. Sebagai bentuk perdagangan modern, *e-commerce* memerlukan kerangka regulasi yang adaptif agar dapat mendorong pertumbuhan sekaligus melindungi kepentingan konsumen dari praktik yang merugikan, seperti penyalahgunaan data, penipuan, dan ketidakseimbangan kekuatan antara pelaku usaha dengan pengguna sehingga pemahaman mendalam terhadap konsep *e-commerce* menjadi dasar penting dalam menganalisis tanggung jawab hukum Penyelenggara Sistem Elektronik terhadap kerugian yang dialami pengguna platform digital.

Selain dimensi teknologi dan model bisnis, konsep *e-commerce* juga mencakup aspek sosial dan budaya yang signifikan. E-commerce telah mengubah pola konsumsi masyarakat dari transaksi konvensional berbasis tatap muka menjadi transaksi digital yang serba cepat dan praktis. Perubahan ini tidak hanya memengaruhi perilaku belanja, tetapi juga membentuk budaya konsumsi baru yang menekankan kemudahan, kecepatan, dan pengalaman personalisasi.¹⁸ Di Indonesia, fenomena ini terlihat dari maraknya penggunaan aplikasi belanja online yang berhasil menjangkau masyarakat di berbagai lapisan, termasuk daerah pedesaan sekalipun, sehingga memperluas akses pasar bagi pelaku UMKM.

Di sisi lain, perkembangan *e-commerce* juga membawa implikasi terhadap keberlanjutan dan tanggung jawab sosial perusahaan. Platform *e-commerce* kini dituntut tidak hanya untuk memberikan keuntungan ekonomi, tetapi juga untuk memperhatikan aspek lingkungan, etika bisnis, dan tanggung jawab sosial (*Corporate Social Responsibility*). Isu seperti pengemasan berlebih, emisi karbon

¹⁷ Horst Treiblmaier and Christian Sillaber, "The Impact of Blockchain on E-Commerce: A Framework for Salient Research Topics," *Electronic Commerce Research and Applications* 48, No. 1, 2021, h. 1–11, <https://doi.org/https://doi.org/10.1016/j.elerap.2021.101054>.

¹⁸ Wafiq Mawardah, Heni Safitroh, and Didik Tri Setiyoko, "Analisis Transformasi Pola Konsumsi Masyarakat Pada Era Digital," *Jurnal Pengabdian Masyarakat Dan Riset Pendidikan* 4, No. 4, 2026, h. 22031–22035.

dari pengiriman, serta praktik kerja yang adil dalam rantai pasok menjadi perhatian utama konsumen modern.

1.5.1.3 Konsep Kerugian

Dalam hukum perdata, kerugian (*schade*) dipahami sebagai setiap bentuk kehilangan yang dialami seseorang akibat tindakan pihak lain. Subekti menjelaskan bahwa kerugian dapat berupa kerugian materiil (kehilangan harta, uang, atau nilai ekonomi) dan kerugian immateriil (penderitaan, rasa malu, atau hilangnya kenyamanan). Kerugian menjadi dasar bagi seseorang untuk menuntut ganti rugi apabila terbukti adanya perbuatan melawan hukum atau *wanprestasi*. Kerugian pengguna platform digital mencakup dampak finansial, psikologis, dan sosial akibat kebocoran data pribadi atau kegagalan sistem PSE, seperti pencurian identitas, penipuan, atau hilangnya kepercayaan. Ganti rugi diatur melalui tanggung jawab perdata berdasarkan KUH Perdata Pasal 1365 dan Undang-Undang Perlindungan Data Pribadi Pasal 65, di mana subjek data berhak atas kompensasi atas kerugian materiil maupun immateriil.¹⁹

Dalam konteks layanan digital, kerugian pengguna tidak lagi dipahami hanya sebagai kerugian ekonomi yang bersifat langsung, tetapi juga mencakup kerugian immaterial yang berdampak pada aspek psikologis, sosial, dan reputasional. Menurut Sutan Remy Sjahdeini, kerugian immaterial sering kali lebih sulit dipulihkan karena menyangkut martabat dan rasa aman individu. Dalam ekosistem digital, kerugian seperti pencurian identitas, penyalahgunaan data pribadi, atau penyebaran informasi sensitif dapat menimbulkan dampak jangka panjang yang tidak selalu dapat diukur dengan nilai uang. Dalam perspektif perlindungan konsumen, konsumen digital berada dalam posisi yang lebih lemah karena keterbatasan informasi dan ketidakseimbangan kekuatan dengan penyedia layanan. Kerugian yang dialami konsumen sering kali tidak hanya berupa kerugian finansial, tetapi juga hilangnya rasa aman dan kepercayaan terhadap layanan digital

¹⁹ Lenny Maria Arintonang and Rara Handayani, “Analisis Hukum Terhadap Kebocoran Data Pribadi dan Penyalahgunaan Identitas dalam Perbankan Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi,” *Ranah Research* 7, No. 5, 2025, h. 3146.

Sementara itu, Ahmad M. Ramli menekankan bahwa kerugian dalam transaksi elektronik memiliki karakteristik khusus karena melibatkan hubungan antara pengguna dan sistem yang bekerja secara otomatis. Ketika terjadi kegagalan sistem atau kebocoran data, pengguna sering kali tidak dapat membuktikan secara langsung unsur kesalahan PSE. Oleh karena itu, Ramli mengusulkan penerapan prinsip *strict liability* dalam kasus tertentu, di mana PSE tetap bertanggung jawab meskipun tidak terbukti lalai, selama kerugian terjadi akibat kegagalan sistem elektronik yang mereka kelola.²⁰

Sahat Maruli dalam penelitiannya mengklasifikasikan kerugian menjadi finansial (kehilangan dana transaksi atau pencurian akun), psikologis (stres akibat pembusukan identitas), dan sosial (kerusakan reputasi). Kebocoran data pribadi sering memicu penipuan berat, seperti pemalsuan KTP untuk kredit ilegal, yang merugikan pengguna secara berkelanjutan. Studi empiris menunjukkan kelemahan sistem keamanan PSE mengurangi kerugian ini, dengan korban kesulitan membuktikan kausalitas.²¹ Dalam konteks transaksi elektronik, kerugian pengguna dapat timbul akibat kegagalan sistem, penyalahgunaan data pribadi, penipuan digital, atau layanan yang tidak sesuai. Kerugian dalam sistem elektronik memiliki karakteristik khusus karena sering kali melibatkan kerugian data, akses ilegal, atau gangguan layanan, yang tidak selalu mudah dihitung secara materiil. Oleh karena itu, PSE wajib menerapkan standar keamanan untuk mencegah kerugian tersebut.

Ganti rugi merupakan mekanisme hukum untuk memulihkan keadaan korban seperti sebelum kerugian terjadi. Menurut R. Setiawan, ganti rugi dapat mencakup biaya, kerugian, dan bunga, sebagaimana diatur dalam Pasal 1243–1249 KUH Perdata. Dalam hubungan kontraktual, ganti rugi diberikan ketika pihak yang berkewajiban tidak memenuhi prestasi atau melakukan kelalaian yang merugikan pihak lain.²² Undang-Undang Perlindungan Data Pribadi Nomor 27 Tahun 2022 (UU PDP) Pasal 65 memberikan hak ganti rugi kepada subjek data atas pelanggaran

²⁰ Ahmad M Ramli, *Cyber Law dan Perlindungan Konsumen dalam Transaksi Elektronik*, Refika Aditama, Jakarta, 2020, h. 25-28.

²¹ Sahat Maruli Tua Situmeang, “Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna dalam Perspektif Hukum Siber,” *SASI* 27, No. 1, 2021, h. 38.

²² R Setiawan, *Pokok-Pokok Hukum Perikatan*, Binacipta, Bandung, 2014, h. 30-33.

pengolahan data, termasuk tuntutan perdata tanpa batas waktu klaim. Integrasi dengan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UUPK) Pasal 19 memungkinkan konsumen menuntut ganti rugi akibat transaksi elektronik gagal, sementara UU ITE Pasal 26 dan Pasal 15 mewajibkan PSE penyelesaian kecuali *force majeure*. Wijaya dan Anggriawan menekankan prinsip restitusi utuh, di mana PSE harus mengembalikan kerugian plus bunga.²³

Kerugian pengguna platform digital sering kali berlapis, mencakup tidak hanya finansial seperti hilangnya dana transaksi, tapi juga identitas *theft* yang memicu pinjaman ilegal berbasis KTP palsu, di mana Undang-Undang Perlindungan Data Pribadi Nomor 27 Tahun 2022 Pasal 65 memberikan hak ganti rugi materiil-immateriil tanpa batas klaim waktu. Arief Sidharta (2020) menjelaskan bahwa besaran ganti rugi dihitung berdasarkan *restitutio in integrum* yaitu mengembalikan korban ke posisi semula termasuk bunga dan biaya litigasi, relevan untuk kasus PSE seperti *breach* Akulaku yang rugikan jutaan pengguna.²⁴ Dalam literatur perlindungan data pribadi, kerugian pengguna tidak hanya berupa kerugian ekonomi, tetapi juga kerugian immateriil seperti hilangnya privasi, rasa aman, dan reputasi. Kebocoran data dapat menimbulkan kerugian jangka panjang, termasuk penyalahgunaan identitas dan kerugian finansial. Oleh karena itu, PSE wajib memberikan pemberitahuan dan menyediakan mekanisme pemulihan bagi pengguna.

Penelitian Sutedi menunjukkan bahwa kerugian dalam transaksi elektronik sering kali bersifat non-fisik, seperti hilangnya data, pencurian identitas, atau kerugian ekonomi tidak langsung. Artikel tersebut menegaskan bahwa PSE dapat dimintai pertanggungjawaban apabila tidak memenuhi kewajiban keamanan sistem elektronik, dan pengguna berhak menuntut ganti rugi berdasarkan prinsip *strict liability* atau kelalaian. Kajian empiris oleh Novianti dan Prabowo menunjukkan bahwa sebagian besar korban kebocoran data di Indonesia tidak menerima bentuk pemulihan yang memadai, baik secara material maupun immaterial. Banyak PSE

²³ Alvian Dwiangga Wijaya dan Teddy Prima Anggriawan, "Perlindungan Hukum terhadap Data Pribadi dalam Penggunaan Aplikasi di Smartphone," *Journal Inicio Legis* 3, No. 1, 2022, h. 63–72.

²⁴ Arief Sidharta, *Hukum Perdata Tentang Wanprestasi*, Rajawali Pers, Jakarta, 2020, h. 59.

hanya memberikan permintaan maaf tanpa mekanisme kompensasi yang jelas. Hal ini menunjukkan adanya kesenjangan antara norma hukum yang mengatur tanggung jawab PSE dan implementasi di lapangan.²⁵ Penelitian tersebut menegaskan perlunya standar ganti rugi yang lebih tegas, termasuk kewajiban notifikasi, kompensasi finansial, dan dukungan pemulihan identitas digital.

Menurut M. Yahya Harahap, ganti rugi dipahami sebagai kerugian nyata (*fietelijke nadeel*) yang timbul akibat adanya *wanprestasi*. Kerugian nyata tersebut ditentukan melalui perbandingan antara keadaan yang seharusnya terjadi apabila debitur memenuhi prestasinya dengan keadaan yang muncul akibat kelalaian atau pelanggaran tersebut. Lebih lanjut, Harahap menjelaskan bahwa besaran ganti rugi pada prinsipnya harus mencerminkan nilai yang wajar, yaitu sebanding dengan nilai prestasi yang menjadi objek perjanjian dan keadaan yang menyebabkan terjadinya *wanprestasi*. Pendapat lain juga menyatakan bahwa ganti rugi seharusnya diberikan sebesar kerugian nyata yang dialami kreditur, termasuk kekurangan manfaat atau keuntungan yang semestinya dapat diperoleh. Dengan demikian, konsep kerugian bersifat relatif karena selalu didasarkan pada perbandingan antara dua kondisi: keadaan yang diharapkan dan keadaan yang terjadi akibat *wanprestasi*.²⁶

1.5.1.4 Konsep Platform Digital

Platform digital pada dasarnya berfungsi sebagai jembatan yang menghubungkan berbagai pihak dalam ekosistem digital, memungkinkan interaksi yang mulus antara pengguna, penjual, dan penyedia layanan melalui algoritma cerdas dan data besar. Menurut Situmeang, platform digital bukan sekadar alat teknologi, melainkan revolusi ekonomi yang mengubah cara pasar bekerja dengan menciptakan efek jaringan, semakin banyak pengguna, semakin berharga platform tersebut seperti yang terlihat pada Tokopedia atau Shopee di Indonesia.²⁷

²⁵ Novianti dan Prabowo, "Analisis Dampak Kebocoran Data Pribadi Terhadap Konsumen Digital Di Indonesia," *Jurnal Perlindungan Konsumen Indonesia* 4, No. 1, 2022, h. 45–60.

²⁶ M. Yahya Harahap, *Hukum Acara Perdata Tentang Gugatan, Persidangan, Penyitaan, Pembuklisan, Dan Putusan Pengadilan*, Sinar Grafika, Jakarta, 2010, h. 79.

²⁷ Situmeang, "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna dalam Perspektif Hukum Siber," *SASI* 27, No. 1, 2021, h. 38–40.

Konsep platform digital muncul bersamaan dengan perubahan dalam ekonomi dan teknologi informasi. Platform digital dijelaskan dalam literatur teknologi dan hukum sebagai infrastruktur berbasis Internet yang memfasilitasi interaksi, transaksi, penyebaran konten, atau pertukaran data antara pengguna. Dalam karya mereka “The Platform Society”, Van Dijck, Poell, dan De Waal

menggambarkan platform digital yaitu *“platforms are programmable digital architectures designed to organize interactions between users, geared toward the systematic collection, algorithmic processing, circulation, and monetization of user data. They further explain that platforms operate within a broader “platform ecosystem” dominated by infrastructural services of big tech companies”*.

Platform digital kini menjadi bagian tak terpisahkan dari kehidupan masyarakat modern, berfungsi sebagai ekosistem sosio-teknis yang menghubungkan pengguna, penyedia layanan, dan pihak ketiga. Berbagai platform seperti Facebook, Instagram, YouTube, TikTok, dan Tokopedia di Indonesia memainkan peran penting dalam menunjang komunikasi, aktivitas perdagangan, serta interaksi sosial. Secara ekonomi, kehadiran platform-platform tersebut telah mengubah dinamika persaingan dengan menyediakan titik akses pasar yang terpusat, sehingga memungkinkan pelaku usaha tumbuh dengan cepat dan bahkan mendominasi pasar. Ekonomi berbasis platform sendiri ditandai oleh model transaksional, inovatif, dan hibrida yang mampu memfasilitasi beragam bentuk interaksi dan aktivitas ekonomi.

Platform digital merujuk pada wujud penyelenggaraan sistem elektronik yang memfasilitasi interaksi, transaksi, atau layanan antar pengguna melalui teknologi digital, sebagaimana dijelaskan dalam kajian hukum yang berkaitan dengan UU ITE jo. PP 71/2019. PSE didefinisikan sebagai setiap orang, penyelenggara negara, badan usaha, atau masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik secara sendiri-sendiri atau bersama-sama untuk keperluan sendiri maupun pihak lain. Definisi ini bersumber

dari Pasal 1 angka 6a UU ITE jo. PP Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.²⁸

Platform digital merupakan infrastruktur berbasis teknologi yang menghubungkan penyedia dan pengguna layanan, seperti *e-commerce* atau media sosial, dengan tanggung jawab hukum atas konten ilegal atau transaksi. Menurut jurnal hukum, platform ini termasuk PSE swasta yang menyediakan perdagangan barang/jasa secara online, dengan kewajiban pendaftaran dan pengelolaan data. Kajian empiris transkripsi platform dalam ekonomi digital, namun memerlukan regulasi untuk melindungi pengguna. platform digital tidak pernah benar-benar netral. Mereka membentuk ruang interaksi sosial melalui algoritma, moderasi konten, dan desain teknis yang menentukan apa yang dapat atau tidak dapat dilakukan pengguna.

Shoshana Zuboff dalam karyanya *The Age of Surveillance Capitalism*, menjelaskan bahwa “*the platforms are not merely intermediaries or service providers; they are the new means of behavioral modification*”. Platform digital bekerja melalui mekanisme pengumpulan data masif yang kemudian diolah menjadi prediksi perilaku pengguna. Perspektif ini memperluas pemahaman bahwa platform bukan sekadar penyedia layanan, tetapi juga aktor ekonomi yang mengendalikan arsitektur informasi dan mempengaruhi keputusan pengguna melalui desain algoritmik.²⁹

1.5.1.5 Konsep Pengguna Sistem Elektronik

Pengguna sistem elektronik merupakan pihak yang memanfaatkan layanan berbasis teknologi digital untuk berbagai kepentingan, baik pribadi maupun profesional. Dalam kerangka hukum Indonesia, pengguna ditempatkan sebagai subjek hukum yang memiliki hak dan kewajiban dalam berinteraksi dengan Penyelenggara Sistem Elektronik (PSE). Hak tersebut mencakup perlindungan

²⁸ Cello Pratama Ramadhan et al., “Analisis Kewajiban Penyelenggara Sistem Elektronik dalam Memberikan Perlindungan Bagi Anak : Konteks UU Nomor 1 Tahun 2024,” *Demokrasi: Jurnal Riset Ilmu Hukum, Sosial, dan Politik* 2, No. 2, 2025, h. 21–27.

²⁹ Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Public Affairs, New York, h. 10-13.

data pribadi, keamanan transaksi, serta kepastian hukum atas layanan yang digunakan. Menurut Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, pengguna berhak atas transparansi dalam pengumpulan dan pemrosesan data, serta memiliki kendali atas informasi yang mereka serahkan kepada PSE.³⁰

Posisi pengguna sering kali lebih lemah dibandingkan PSE. Hal ini disebabkan oleh keterbatasan pemahaman teknis dan akses terhadap kebijakan internal platform. Sebagian besar pengguna cenderung menerima syarat dan ketentuan tanpa membaca secara detail, sehingga mereka tidak sepenuhnya memahami konsekuensi hukum dari persetujuan yang diberikan. Hak privasi dalam era digital tidak hanya menyangkut kerahasiaan data, tetapi juga *informational self-determination*, yaitu kemampuan individu untuk mengontrol bagaimana data pribadinya dikumpulkan, digunakan, dan disebarkan.

Selain itu, pengguna sistem elektronik memiliki kerentanan yang tinggi terhadap kerugian, baik materiil maupun immateriil. Kebocoran data pribadi dapat menimbulkan pencurian identitas, penipuan digital, hingga kerusakan reputasi. Situmeang menjelaskan bahwa penyalahgunaan data pribadi merupakan bentuk kejahatan siber yang sempurna karena dampaknya berlapis dan sulit dipulihkan. Dalam konteks ini, pengguna bukan hanya konsumen pasif, melainkan pihak yang rentan terhadap risiko sistemik akibat lemahnya perlindungan hukum dan standar keamanan PSE³¹

1.5.2 Landasan Yuridis

Adapun landasan yuridis yang menjadi ajuan dalam penelitian ini yaitu:

³⁰ Aritonang dan Handayani, “Analisis Hukum Terhadap Kebocoran Data Pribadi dan Penyalahgunaan Identitas dalam Perbankan Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.” *Ranah Research* 7, No.5, 2025, h. 3146–3158

³¹ Situmeang, “Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna dalam Perspektif Hukum Siber.” *SASI* 27, No.1, 2021, h. 38-52.

1.5.2.1 Undang-Undang Dasar 1945 (UUD)

- a. Pasal 28G ayat (1): Menjamin kehormatan, martabat, dan perlindungan hukum pribadi.
- b. Pasal 28I ayat (1): Perlindungan data pribadi sebagai hak asasi manusia.

1.5.2.2 Undang-Undang (UU)

- a. Kitab Undang-Undang Hukum Perdata (KUHPerdata):
 - 1) Pasal 1365: Perbuatan melawan hukum yang merugikan privasi.
 - 2) Pasal 1243–1249: Wanprestasi dan bentuk ganti rugi (biaya, kerugian, dan bunga)
- b. Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia (HAM) Pasal 29 ayat (1): Hak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda.
- c. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP):
 - 1) Pasal 16: Persetujuan eksplisit untuk data sensitif (biometrik, kesehatan).
 - 2) Pasal 65: Hak atas kompensasi kerugian materiil dan immateriil tanpa batas waktu klaim.
- d. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE):
 - 1) Pasal 15: PSE wajib menjamin keandalan, keamanan, dan pertanggungjawaban sistem.
 - 2) Pasal 26 ayat (1): Penggunaan data pribadi harus atas persetujuan.
 - 3) Pasal 26 ayat (2): Hak gugatan atas kerugian dari pelanggaran data pribadi.
- e. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UUPK) Pasal 19: Hak ganti rugi atas kerugian dari penggunaan barang/jasa, termasuk layanan digital
- f. Undang-Undang Nomor 36 Tahun 1999 tentang Perlindungan privasi dan data pribadi dalam telekomunikasi

1.5.2.3 Peraturan Pemerintah (PP)

- a. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik Pasal 3 ayat (1): PSE wajib menyelenggarakan sistem yang andal dan aman.
- b. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

1.5.2.4 Peraturan Menteri (Permen)

- a. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik
- b. Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Swasta

1.5.3 Landasan Teori

1.5.3.1 Teori Perlindungan Hukum

Perlindungan hukum dapat dipahami sebagai bentuk pengayoman terhadap hak-hak asasi manusia yang mengalami kerugian akibat tindakan pihak lain. Perlindungan ini diberikan kepada masyarakat agar mereka dapat menikmati secara utuh hak-hak yang dijamin oleh hukum. Dengan kata lain, perlindungan hukum mencakup serangkaian langkah dan mekanisme yang wajib ditempuh oleh aparat penegak hukum untuk memastikan terciptanya rasa aman baik secara mental maupun fisik dari berbagai bentuk gangguan maupun ancaman yang berasal dari siapa pun.³² Fungsi utama hukum adalah melindungi kepentingan manusia, dan untuk mencapai tujuan tersebut hukum harus dijalankan secara profesional. Pelaksanaan hukum yang baik memungkinkan terciptanya keadaan yang tertib, damai, dan berjalan sebagaimana mestinya. Ketika terjadi pelanggaran, hukum wajib ditegakkan melalui mekanisme penegakan hukum yang efektif. Penegakan hukum menuntut adanya kepastian hukum, karena kepastian hukum merupakan bentuk perlindungan yang dapat diuji secara yudisial terhadap tindakan

³² Satjipto Rahardjo, *Ilmu Hukum*, Citra Aditya Bakti, Bandung 2000, h. 25.

sewenang-wenang. Masyarakat sangat mengharapkan kepastian hukum, sebab dengan adanya kepastian tersebut kehidupan sosial dapat berlangsung secara tertib, aman, dan damai.

Penelitian dalam jurnal hukum administrasi menekankan bahwa perlindungan hukum merupakan bagian dari prinsip negara hukum (*rechtsstaat*). Perlindungan hukum diberikan melalui instrumen peraturan perundang-undangan, pelayanan publik, dan mekanisme pengawasan.³³ Dalam kajian perlindungan konsumen, perlindungan hukum dipahami sebagai upaya negara untuk menjamin hak-hak konsumen dari praktik yang merugikan. Penelitian dalam jurnal Yuridika menunjukkan bahwa perlindungan hukum mencakup hak atas keamanan, kenyamanan, dan keselamatan dalam menggunakan barang atau jasa. Konsep ini dapat diperluas ke ranah digital, di mana pengguna platform digital diposisikan sebagai konsumen yang berhak atas keamanan data dan keandalan layanan.³⁴

Teori perlindungan hukum mencakup tindakan yang bertujuan untuk menjamin keamanan atau memberikan perlindungan, misalnya bagi orang-orang yang berada dalam posisi lemah.³⁵ Perlindungan hukum adalah upaya untuk memberikan pengayoman kepada masyarakat agar hak-haknya tidak dilanggar oleh tindakan sewenang-wenang, baik oleh pemerintah maupun pihak lain. Hadjon membedakan perlindungan hukum menjadi preventif (pencegahan) dan represif (penyelesaian sengketa). Konsep ini sangat relevan dalam konteks hubungan antara pengguna dan Penyelenggara Sistem Elektronik (PSE), di mana pengguna membutuhkan mekanisme hukum yang mampu mencegah dan menyelesaikan kerugian akibat layanan digital.

Tujuan negara dalam melaksanakan fungsi perlindungan hukum adalah untuk menciptakan keseimbangan antara kepentingan hukum individu dengan kepentingan hukum individu lainnya. Menurut Philipus M. Hadjon, sarana perlindungan hukum dapat dikelompokkan menjadi dua kategori yaitu:

³³ Suteki, "Perlindungan Hukum dalam Perspektif Negara Hukum," *Jurnal Hukum dan Pembangunan* 48, No. 3, 2018, h. 55–68.

³⁴ D. P. Sari, "Perlindungan Hukum Bagi Konsumen Dalam Transaksi Elektronik," *Yuridika* 34, No. 2, 2019, h. 210–225.

³⁵ C. S. T Kansil, *Pengantar Ilmu Hukum*, Balai Pustaka, Jakarta, 2006, h. 67-73.

1. Sarana Perlindungan Hukum Preventif

Sarana perlindungan hukum preventif bertujuan untuk mencegah pelanggaran hukum sebelum terjadi. Pemerintah melindungi warganya dari pelanggaran hukum dengan menerapkan peraturan perundang-undangan dan melibatkan lembaga penegak hukum. Langkah-langkah ini bertujuan untuk mencegah konflik dengan menetapkan pedoman hukum dan aturan perilaku yang harus dipatuhi. Ini termasuk peraturan hukum yang mengatur perilaku dan memberikan kewenangan kepada pemerintah untuk mengatur lembaga penegak hukum agar dapat mencegah pelanggaran hukum melalui tindakan pencegahan.

2. Sarana Perlindungan Hukum Represif

Perlindungan hukum represif merupakan upaya terakhir untuk memberikan sanksi dalam bentuk denda atau hukuman penjara serta tindakan lain setelah terjadi sengketa atau pelanggaran. Tujuannya adalah untuk menyelesaikan sengketa tersebut. Pengadilan umum dan administratif melaksanakan perlindungan hukum represif.

Perlindungan hukum represif berlaku setelah suatu peristiwa dianggap sebagai pelanggaran hukum. Dengan kata lain: Jika suatu tindakan melanggar hak orang lain, mekanisme penegakan hukum akan diaktifkan sebagai upaya terakhir.³⁶ Hal ini dilakukan melalui tindakan fisik atau pidana, denda, serta sanksi administratif seperti penarikan atau penghentian penggunaan objek tertentu. Perlindungan hukum dalam kasus represif Perlindungan hukum represif bertujuan untuk memulihkan keadaan sebelum pelanggaran hak tertentu dengan menjatuhkan sanksi terhadap pihak yang melakukan pelanggaran.

Satjipto Rahardjo memandang perlindungan hukum sebagai upaya untuk menciptakan keadilan dan ketertiban dalam masyarakat. Menurutnya, hukum harus berfungsi melindungi manusia dari tindakan yang merugikan, sehingga perlindungan hukum tidak hanya bersifat normatif, tetapi juga harus diwujudkan dalam praktik.³⁷ Dalam konteks digital, pandangan ini menekankan bahwa

³⁶ P. M Hadjon, *Perlindungan Hukum Bagi Rakyat Indonesia*, Peradaban, Malang, 2007, h. 43-48.

³⁷ Rahardjo, *Ilmu Hukum*, Citra Aditya Bakti, Bandung, 2000, h. 29-36.

perlindungan hukum terhadap pengguna platform digital harus diwujudkan melalui regulasi yang efektif dan penegakan hukum yang responsif.

Dalam literatur hukum HAM, hak privasi dipahami sebagai hak untuk mengontrol informasi pribadi dan membatasi akses pihak lain terhadap data yang bersifat personal. Menurut Jimly Asshiddiqie, hak privasi merupakan bagian dari hak-hak fundamental yang wajib dijamin oleh negara sebagai konsekuensi dari prinsip negara hukum.³⁸ Pusat Data Nasional (PDN) merupakan sebuah inisiatif dari Kementerian Komunikasi dan Informatika (Kominfo) Indonesia yang bertujuan untuk mengintegrasikan dan mengelola data dari berbagai instansi pemerintah secara terpusat guna mendukung segala implementasi kebijakan berbasis data. Dengan PDN, data dari berbagai instansi pemerintah dapat diintegrasikan, diolah dan dianalisis dengan lebih cepat dan lebih baik

Dalam perspektif hukum tata negara, Ni'matul Huda menekankan bahwa hak privasi merupakan bagian dari hak konstitusional yang tidak dapat dikurangi dalam keadaan apa pun (*non-derogable rights*).³⁹ Hal ini berarti negara memiliki kewajiban aktif untuk memastikan bahwa setiap bentuk pemrosesan data pribadi dilakukan secara sah, proporsional, dan tidak melanggar martabat manusia. Pandangan ini memperkuat argumentasi bahwa perlindungan data pribadi bukan sekadar isu teknis, tetapi merupakan bagian dari perlindungan hak asasi yang fundamental.

1.5.3.2 Teori Pertanggung Jawaban

PSE bertanggung jawab atas hukum kerugian transaksi elektronik, seperti kegagalan operasional agen elektronik, kecuali terbukti kelalaian pengguna. Prinsip safe harbour dalam UU ITE memungkinkan PSE melepaskan tanggung jawab jika telah menerapkan tata kelola preventif, seperti sarana pelaporan dan pendaftaran PSE. Kajian menunjukkan PSE wajib menjamin jaminan, integritas, dan ketersediaan data, dengan sanksi administratif hingga pidana untuk pelanggaran. Dalam perspektif hukum Indonesia, PSE didefinisikan secara eksplisit dalam Pasal

³⁸ Jimly Asshiddiqie, *Pengantar Ilmu Hukum Tata Negara*, Konstitusi Press, Jakarta, 2006, h. 16.

³⁹ Ni'matul Huda, *Hukum Tata Negara Indonesia*, Rajawali Pers, Jakarta, 2019, h. 42.

1 angka 6a UU ITE jo. PP 71/2019 sebagai pihak yang menyediakan, mengelola, atau mengoperasikan sistem elektronik untuk kepentingan umum atau pribadi, mencakup baik lingkup publik (pemerintah) maupun privat (platform swasta seperti Gojek). Edmon Makarim menambahkan bahwa PSE bertanggung jawab atas keandalan sistem, di mana kegagalan seperti downtime atau breach data dapat menimbulkan liabilitas hukum langsung kepada pengguna yang dirugikan.⁴⁰

Penyelenggara Sistem Elektronik (PSE), baik yang berasal dari sektor publik maupun privat, memikul tanggung jawab yang sangat besar dalam memastikan keamanan data yang berada di bawah pengelolaannya, terutama sejak diberlakukannya Undang-Undang Perlindungan Data Pribadi (UU PDP). Regulasi tersebut mengatur kewajiban PSE secara rinci dan komprehensif, sehingga memberikan landasan hukum yang jelas mengenai bentuk-bentuk tanggung jawab yang harus dipenuhi oleh setiap PSE dalam melindungi data pribadi pengguna. Sejalan dengan teori Edmon Makarim yang menjelaskan bahwa PSE memiliki tanggung jawab hukum yang melekat pada aktivitas pengelolaan sistem elektronik. Menurutnya, setiap PSE wajib memastikan bahwa sistem elektronik yang mereka operasikan memenuhi prinsip keandalan, keamanan, integritas, dan ketersediaan data. Kegagalan memenuhi prinsip tersebut dapat menimbulkan tanggung jawab hukum, baik dalam bentuk tanggung jawab perdata, administratif, maupun pidana. Makarim menekankan bahwa PSE harus menerapkan standar keamanan yang memadai, termasuk enkripsi, audit sistem, dan pengelolaan risiko, sebagai bagian dari kewajiban hukum untuk melindungi pengguna dari kerugian. PSE menangani tanggung jawab perdata atas ganti rugi kerugian pengguna, administratif seperti pencabutan izin, dan pidana untuk pelanggaran pelanggaran data. Prinsip safe harbour memungkinkan jaminan jika PSE membuktikan upaya preventif, seperti ketentuan penggunaan yang jelas dan pemantauan konten ilegal. Studi kasus dalam jurnal menunjukkan efektivitas tergantung implementasi regulasi⁴¹.

⁴⁰ Shelomita Putri Amelia, "Tanggung Jawab Hukum Penyelenggara Sistem Elektronik Terhadap Kebocoran Data Pribadi Pengguna," *STUDIA* 1, No. 2, 2025, h. 132.

⁴¹ Anthon Rumburen dan Yohana Watofa, "Analysis of the Responsibilities of the Organizer of the Electronic System in Case of Data Breach," *Awang Long Law Review* 7, No. 2, 2025, h. 481.

Dalam perspektif hukum perdata, Subekti menjelaskan bahwa tanggung jawab timbul ketika suatu pihak menimbulkan kerugian akibat kelalaian atau *wanprestasi*. Konsep ini dapat diterapkan pada PSE, karena hubungan antara pengguna dan PSE pada dasarnya merupakan hubungan kontraktual melalui *terms of service*. Jika PSE lalai menjaga keamanan sistem elektronik sehingga menimbulkan kerugian, maka PSE dapat dimintai pertanggungjawaban berdasarkan asas perbuatan melawan hukum atau *wanprestasi*. Dengan demikian, tanggung jawab PSE tidak hanya bersifat teknis, tetapi juga merupakan konsekuensi dari hubungan hukum dengan pengguna.⁴²

Dari sudut pandang komparatif, model tanggung jawab platform di Eropa melalui DSA (*Digital Services Act*) 2022 memberikan inspirasi bagi Indonesia, di mana PSE wajib lakukan due diligence preventif seperti audit rutin dan transparansi algoritma untuk hindari sanksi hingga 6% omzet global, pendekatan yang bisa memperkuat Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Penelitian Wonohadidjojo di Syiah Kuala Law Journal menyoroti hambatan struktural PSE lokal melawan dominasi global seperti *Google*, merekomendasikan reformasi sanksi pidana Pasal 46 UU ITE agar lebih efektif cegah kerugian pengguna.⁴³ Tanggung jawab PSE tidak hanya terbatas pada aspek teknis, tetapi juga mencakup kewajiban etis dan kontraktual untuk menjaga integritas data pengguna, di mana kelalaian seperti lemahnya enkripsi dapat memicu tuntutan perdata berdasarkan Pasal 1365 KUHPerdata.

Ahmadi Miru dalam bukunya *Hukum Perlindungan Konsumen* menjelaskan bahwa pelaku usaha wajib memberikan keamanan, kenyamanan, dan keselamatan kepada konsumen dalam menggunakan barang atau jasa. Jika konsep ini diterapkan pada PSE, maka platform digital sebagai penyedia layanan elektronik berkewajiban memastikan bahwa pengguna tidak mengalami kerugian akibat kegagalan sistem atau penyalahgunaan data. Miru menegaskan bahwa pelaku usaha

⁴² Subekti, *Pokok-Pokok Hukum Perdatajak*, Intermasa, Jakarta, 2008, h. 32-37.

⁴³ Christopher Howard Wonohadidjojo and Richard C Adam, "Legal Protection of Electronic System Providers Concerning Unfair Business Competition in Digital Payment Systems," *Syiah Kuala Law Journal* 9, No. 3, 2025, h. 10–25.

dapat dimintai pertanggungjawaban apabila tidak memberikan informasi yang benar, tidak menjaga keamanan data, atau tidak menyediakan mekanisme penyelesaian sengketa yang layak.⁴⁴ Dapat disimpulkan bahwa PSE bertanggung jawab terhadap kerugian pengguna yang timbul akibat kegagalan sistem, kelemahan keamanan, atau pengelolaan data yang tidak sesuai standar. PSE harus menyediakan sistem yang mampu meminimalkan risiko kerugian finansial maupun non-finansial, seperti kerugian reputasi atau pelanggaran privasi. Apabila terjadi kejadian seperti bocornya data, PSE tidak hanya berkewajiban memberi pemberitahuan kepada pengguna, tetapi juga melakukan pemulihan dan, dalam keadaan tertentu, memberikan kompensasi.

1.5.3.3 Teori Kepastian Hukum

Kepastian hukum adalah prinsip fundamental dalam sistem hukum yang menekankan bahwa hukum harus jelas, konsisten, dan dapat diprediksi sehingga masyarakat mengetahui hak dan kewajibannya. Menurut Gustav Radbruch, kepastian hukum merupakan salah satu dari tiga nilai dasar hukum selain keadilan dan kemanfaatan. Dalam konteks perlindungan pengguna platform digital, kepastian hukum berarti adanya aturan yang jelas mengenai tanggung jawab Penyelenggara Sistem Elektronik (PSE) serta mekanisme ganti rugi ketika terjadi kebocoran data atau kerugian lain. Tanpa kepastian hukum, pengguna akan kesulitan menuntut haknya karena aturan yang kabur atau tidak konsisten dalam penerapan.⁴⁵

Di Indonesia, kepastian hukum terkait perlindungan data pribadi mulai diperkuat dengan hadirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang memberikan dasar hukum jelas mengenai hak subjek data dan kewajiban pengendali data. Namun, dalam praktiknya masih terdapat kesenjangan antara norma hukum dan implementasi, sehingga kepastian hukum belum sepenuhnya terwujud. Hal ini terlihat dari

⁴⁴ A Miru, *Hukum Perlindungan Konsumen*, RajaGrafindo Persada, Jakarta, 2011, h. 49.

⁴⁵ Mario Julyano dan Aditya Yuli Sulistyawan, "Pemahaman Terhadap Asas Kepastian Hukum Melalui Konstruksi Penalaran Positivisme Hukum," *CREPINDO: Jurnal Mengenai Dasar-Dasar Pemikiran Hukum: Filsafat Dan Ilmu Hukum* 1, No. 1, 2019, h. 13–22.

banyaknya kasus kebocoran data yang tidak diikuti dengan kompensasi nyata bagi korban.

Kepastian hukum dalam konteks perlindungan data pribadi juga dapat dilihat dari perspektif perbandingan hukum. Di Uni Eropa, General Data Protection Regulation (GDPR) memberikan standar kepastian hukum yang sangat tinggi dengan mengatur secara rinci kewajiban pengendali data, hak subjek data, serta sanksi yang tegas dan proporsional. Pendekatan GDPR menjamin predictability bagi pelaku usaha sekaligus memberikan kepastian perlindungan bagi individu. Berbeda dengan itu, meskipun UU PDP telah mengadopsi beberapa prinsip GDPR, implementasi di Indonesia masih menghadapi tantangan serius berupa regulasi turunan yang belum lengkap dan koordinasi antarlembaga yang kurang efektif.⁴⁶

Kesenjangan antara norma dan praktik kepastian hukum semakin terlihat dalam kasus-kasus kebocoran data yang masif di Indonesia. Banyak Penyelenggara Sistem Elektronik (PSE) yang gagal memenuhi kewajiban notifikasi dan kompensasi kepada korban, sehingga menimbulkan ketidakpastian hukum yang berkepanjangan. Hal ini tidak hanya merugikan pengguna secara individu, tetapi juga melemahkan kepercayaan publik terhadap ekosistem digital secara keseluruhan. Ketidakpastian semacam ini bertentangan dengan prinsip Radbruch yang menekankan bahwa hukum harus dapat diprediksi agar dapat berfungsi sebagai pedoman perilaku masyarakat.⁴⁷

Dalam hubungannya dengan teori pertanggungjawaban hukum, kepastian hukum berperan sebagai fondasi untuk menentukan bentuk dan batas pertanggungjawaban PSE. Tanpa kepastian mengenai standar keamanan yang harus dipenuhi serta besaran ganti rugi yang dapat dituntut, penegakan prinsip *liability based on fault* maupun *strict liability* menjadi sulit dilakukan. Oleh karena itu, penguatan kepastian hukum bukan hanya menjadi kebutuhan normatif, melainkan

⁴⁶ Mediodceci Lustarini, "Kepastian Hukum Pelindungan Data Pribadi Pasca Pengesahan UU Nomor 27 Tahun 2022," *Kementerian Komunikasi Dan Informatika* 1, No. 1, 2022, h. 1–15.

⁴⁷ Muhammad Rizky, Rini Apriyani, dan Nur Aripkha, "Perlindungan Hukum Dan Kepastian Hukum Terhadap Perdagangan Data Pribadi Dalam UU PDP," *Mahkamah: Jurnal Riset Ilmu Hukum* 3, No. 1, 2026, h. 118–28.

juga prasyarat bagi efektivitas teori pertanggungjawaban hukum dalam melindungi pengguna platform digital.

Kaitan antara teori kepastian hukum dengan teori perlindungan hukum dan teori pertanggungjawaban hukum sangat erat. Menurut Philipus M. Hadjon, perlindungan hukum yang efektif baru dapat terwujud apabila didasarkan pada kepastian hukum yang kuat. Tanpa kepastian, mekanisme preventif maupun represif yang dibangun oleh negara akan kehilangan arah dan daya paksa. Dalam konteks pertanggungjawaban PSE, kepastian hukum menjadi instrumen penting untuk menentukan standar kelalaian, besaran ganti rugi, serta prosedur penyelesaian sengketa yang harus diikuti oleh para pihak. Ketidakpastian justru akan memperlemah posisi pengguna sebagai pihak yang lebih lemah dalam hubungan kontraktual digital.⁴⁸

Dalam perspektif hukum positif Indonesia, asas kepastian hukum telah diakui sebagai prinsip negara hukum sebagaimana tercermin dalam Pasal 1 ayat (3) Undang-Undang Dasar 1945. Namun, penerapannya dalam ranah digital masih menghadapi berbagai hambatan struktural, seperti tumpang tindih regulasi antara UU ITE, UU PDP, PP 71 Tahun 2019, dan Permendag Nomor 50 Tahun 2020. Fragmentasi pengaturan ini menyebabkan PSE dan pengguna sering mengalami kebingungan mengenai hak dan kewajiban masing-masing. Akibatnya, kepastian hukum yang seharusnya menjadi pilar utama perlindungan konsumen digital justru menjadi salah satu kelemahan terbesar dalam sistem hukum Indonesia saat ini.

Kepastian hukum dalam perspektif filosofis hukum tidak dapat dipisahkan dari konsep *rechtsstaat* (negara hukum). Menurut A.V. Dicey, kepastian hukum merupakan salah satu pilar utama negara hukum yang menjamin bahwa kekuasaan negara dibatasi oleh hukum yang jelas dan tidak sewenang-wenang.⁴⁹ Dalam konteks digital, prinsip ini menuntut agar regulasi mengenai tanggung jawab Penyelenggara Sistem Elektronik (PSE) tidak hanya bersifat simbolis, melainkan memberikan pedoman yang operasional dan dapat ditegakkan secara konsisten.

⁴⁸ Hadjon, *Op.Cit.*, h. 58.

⁴⁹ Albert Venn Dicey, *Pengantar Studi Hukum Konstitusi*. Diterjemahkan oleh Nurhadi. Bandung: Nusa Media, 2019, h.78-90

Tanpa kepastian semacam ini, pengguna platform digital akan terus berada dalam ketidakpastian hukum, meskipun telah terdapat berbagai undang-undang yang mengaturnya.

Teori kepastian hukum juga berkembang dalam kajian hukum modern yang menekankan pentingnya predictability dan stability dalam sistem hukum digital. Menurut Fuller dalam *The Morality of Law*, “*a good legal system must satisfy eight principles of legality (inner morality of law). Among them are the principles of clarity (the law must be clear and understandable) and non-contradiction (the law must not contain contradictory rules)*”. Penerapan teori ini dalam regulasi *e-commerce* dan perlindungan data pribadi di Indonesia masih menghadapi tantangan, karena banyak ketentuan yang bersifat umum dan belum diikuti oleh peraturan pelaksana yang detail. Hal ini menyebabkan PSE memiliki ruang interpretasi yang luas, sementara pengguna kesulitan memperoleh kepastian mengenai hak ganti rugi mereka.⁵⁰

Penerapan teori kepastian hukum dalam era digital juga menuntut adanya harmonisasi antara norma hukum substantif dan prosedural. Norma substantif yang mengatur hak dan kewajiban PSE serta pengguna harus diimbangi dengan norma prosedural yang jelas, seperti mekanisme pelaporan kebocoran data, prosedur ganti rugi, dan jangka waktu penyelesaian sengketa. Tanpa harmonisasi tersebut, kepastian hukum akan tetap bersifat formal semata dan gagal memberikan perlindungan yang substantif bagi pengguna platform digital.

Teori kepastian hukum pada akhirnya menjadi fondasi filosofis sekaligus praktis dalam penelitian ini. Dengan menganalisis regulasi yang ada melalui kacamata teori Radbruch, penelitian ini berupaya mengungkap kesenjangan antara idealisme hukum dan realitas penerapannya di sektor *e-commerce*. Hasil analisis diharapkan dapat memberikan rekomendasi konkrit bagi pembuat kebijakan untuk menyempurnakan kerangka hukum, sehingga kepastian hukum tidak lagi menjadi retorika semata, melainkan menjadi instrumen nyata dalam melindungi hak

⁵⁰ Lon L. Fuller, *The Morality of Law: Revised Edition*, Yale University Press, Virginia, 1969, h.100

pengguna platform digital dari kerugian akibat kelalaian Penyelenggara Sistem Elektronik.

1.6 Penelitian Terdahulu

Penelitian terdahulu adalah sarana pembantu bagi peneliti sebagai acuan penelitian untuk memperbanyak teori yang digunakan peneliti serta mengkaji penelitian yang akan dilakukan. Peneliti menggunakan penelitian terdahulu sebagai referensi. Peneliti juga melakukan sintesis terhadap beberapa penelitian terdahulu dengan topik yang akan digunakan sebagai referensi pada bagian berikut.

1. Skripsi Ari Naldi, 2025 dari UIN Suska Riau⁵¹

Ari Naldi (2025) dalam skripsinya di Universitas Islam Negeri Sultan Syarif Kasim Riau dengan judul “Kajian Yuridis Terhadap Perlindungan Data Pribadi Konsumen dalam Bisnis Financial Technology di Indonesia “ meneliti perlindungan hukum terhadap data pribadi konsumen dalam bisnis financial technology. Penelitian ini menunjukkan bahwa regulasi yang ada belum sepenuhnya mampu melindungi konsumen dari kebocoran data dan penyalahgunaan identitas, terutama karena lemahnya pengawasan serta rendahnya literasi digital masyarakat. Skripsi ini menekankan perlunya penguatan regulasi dan mekanisme pengawasan agar konsumen *fintech* memiliki jaminan hukum yang lebih jelas.

2. Tesis Wisnu Kuncoro Jati, 2025 dari IAIN Salatiga⁵²

Wisnu Kuncoro Jati (2025) melalui tesis di IAIN Salatiga dengan judul “: Analisis Terhadap Hak Privasi di Era Digital dalam UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi Perspektif *Digital Constitutionalism*” mengkaji hak privasi di era digital dengan perspektif *Digital Constitutionalism*. Penelitian ini menyoroti efektivitas Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dalam menjamin hak privasi warga negara. Hasil

⁵¹ Ari Naldi, “*Kajian Yuridis Terhadap Perlindungan Data Pribadi Konsumen Dalam Bisnis Financial Technology Di Indonesia*”, Skripsi, Fakultas Hukum Universitas Islam Negeri Sultan Syarif Kasim Riau, Riau, 2025, h.17.

⁵² Wisnu Kuncoro Jati, “*Analisis Terhadap Hak Privasi Di Era Digital Dalam Undang-Undang No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi Perspektif Digital Constitutionalism*”, Tesis, Fakultas Hukum IAIN Salatiga, Salatiga, 2025, h. 23.

penelitian menunjukkan bahwa meskipun UU PDP telah memberikan kerangka hukum, implementasinya masih menghadapi tantangan besar, terutama dalam hal kepastian hukum, mekanisme pengawasan, dan kesadaran masyarakat terhadap hak privasi digital

3. Disertasi Andriyanto Adhi Nugroho, 2025 dari Universitas Trisakti⁵³

Andriyanto Adhi Nugroho (2025) dalam disertasinya di Universitas Trisakti berjudul “Pelindungan Data Pribadi Konsumen dalam Era Digital” membahas perlindungan data pribadi konsumen dalam era digital. Penelitian ini menekankan pentingnya inovasi hukum dan tata kelola data yang komprehensif untuk menghadapi tantangan kebocoran data dan penyalahgunaan informasi pribadi. Disertasi ini menyimpulkan bahwa perlindungan hukum terhadap konsumen digital harus diperkuat melalui regulasi yang lebih tegas, mekanisme kompensasi yang jelas, serta peningkatan transparansi dari Penyelenggara Sistem Elektronik (PSE).

Tabel 1. 2 Penelitian Terdahulu

Penelitian Terdahulu	Persamaan	Perbedaan
Skripsi Ari Naldi, 2025 dengan judul “Kajian Yuridis Terhadap Perlindungan Data Pribadi Konsumen dalam Bisnis Financial Technology di Indonesia”	Menyoroti kerugian konsumen akibat kebocoran data, lemahnya pengawasan, dan rendahnya literasi digital masyarakat.	Membandingkan dengan GDPR (standar Eropa) untuk menyoroti kelemahan Indonesia, sedangkan penelitianmu fokus pada batasan kerugian dan bentuk pertanggungjawaban hukum PSE
Tesis Wisnu Kuncoro Jati (2025) dengan judul “: Analisis Terhadap Hak Privasi di Era Digital dalam UU No.	Menganalisis efektivitas UU PDP dalam melindungi hak privasi digital, termasuk tantangan implementasi,	Menggunakan perspektif teori Digital Constitutionalism (konstitusionalisme digital) untuk hak privasi

⁵³ Andriyanto Adhi Nugroho, “Pelindungan Data Pribadi Konsumen Dalam Era Digital”, Disertasi, Fakultas Hukum UPN Veteran Jakarta, Jakarta, 2025, h. 19.

27 Tahun 2022 tentang Perlindungan Data Pribadi Perspektif <i>Digital Constitutionalism</i>	kepastian hukum, dan kesadaran masyarakat.	secara filosofis, sementara penelitianmu lebih praktis pada kerugian konkret akibat kelalaian PSE dan batasan tuntutan
Disertasi Andriyanto Adhi Nugroho (2025) berjudul “Pelindungan Data Pribadi Konsumen dalam Era Digital”	Menggunakan pendekatan yuridis normatif untuk menganalisis regulasi seperti UU PDP, dan menyoroti pentingnya transparansi PSE serta mekanisme kompensasi yang jelas	Tingkat penelitian lebih tinggi dengan fokus pada inovasi hukum dan kelembagaan, bukan pada batasan kerugian yang dapat dimintakan pertanggungjawaban

Penelitian terdahulu menunjukkan bahwa isu perlindungan hukum terhadap data pribadi pengguna platform digital telah banyak dikaji, namun masih terdapat kesenjangan yang signifikan. Ari Naldi melalui skripsinya menyoroti lemahnya perlindungan hukum konsumen fintech, tetapi terbatas pada sektor keuangan digital. Wisnu Kuncoro Jati dalam tesisnya mengkaji hak privasi dengan perspektif *Digital Constitutionalism*, namun lebih menekankan aspek normatif tanpa membahas tanggung jawab PSE terhadap kerugian nyata pengguna. Sementara itu, disertasi Andriyanto Adhi Nugroho membahas perlindungan data pribadi konsumen secara umum, tetapi belum memberikan analisis detail mengenai bentuk kerugian materiil maupun immateriil serta mekanisme ganti rugi yang dapat dituntut berdasarkan UU ITE, UU PDP, dan PP 71/2019. Dengan demikian, penelitian ini hadir untuk mengisi kekosongan dengan menganalisis secara komprehensif tanggung jawab hukum Penyelenggara Sistem Elektronik terhadap kerugian pengguna platform digital, sekaligus mengaitkan regulasi terbaru dengan praktik kasus kebocoran data di Indonesia.

1.7 Metode Penelitian

1.7.1 Jenis Penelitian

Penelitian ini menggunakan penelitian hukum normatif (*normative legal research*) yaitu penelitian yang berfokus pada kajian terhadap norma hukum yang tertulis dalam peraturan perundang-undangan, doktrin para ahli, dan putusan pengadilan. Penelitian hukum normatif dipilih karena isu yang dikaji perlindungan hukum pengguna platform digital dan tanggung jawab Penyelenggara Sistem Elektronik (PSE) merupakan persoalan yang bersumber dari norma hukum positif, bukan fenomena empiris.

Menurut Suyanto penelitian hukum normatif adalah penelitian yang mengkaji hukum sebagai sistem norma, dengan ruang lingkup meliputi inventarisasi hukum positif, analisis asas hukum, sistematika hukum, sinkronisasi vertikal/horizontal, sejarah hukum, dan perbandingan hukum.⁵⁴ Penelitian ini bersifat kepustakaan, menggunakan bahan hukum primer, sekunder, dan tersier serta bertujuan menghasilkan argumentasi hukum atau rekomendasi normatif untuk menyelesaikan masalah hukum. Pendekatan ini memungkinkan peneliti untuk menilai apakah regulasi yang ada telah memberikan perlindungan yang memadai bagi pengguna platform digital, terutama dalam konteks kerugian akibat kegagalan sistem elektronik.

1.7.2 Metode Pendekatan

Penelitian ini menggunakan beberapa metode pendekatan agar analisis yang dihasilkan komprehensif dan mendalam. Pendekatan tersebut yaitu:

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

Pendekatan perundang-undangan adalah pendekatan penelitian hukum yang dilakukan dengan menelaah semua undang-undang dan regulasi yang bersangkut paut dengan isu hukum yang sedang ditangani. Pendekatan ini bertujuan untuk mempelajari konsistensi, kesesuaian, serta filosofi di balik peraturan perundang-undangan, sehingga peneliti dapat menemukan

⁵⁴ Suyanto, *Metode Penelitian Hukum Pengantar Penelitian Normatif, Empiris Dan Gabungan*, UNIGRES PRESS, Gresik, 2023, h. 24.

kesenjangan antara norma hukum dan kenyataan di lapangan. Pendekatan ini digunakan untuk menelaah peraturan perundang-undangan yang mengatur PSE, perlindungan data pribadi, dan perlindungan konsumen. Pendekatan ini penting karena perlindungan hukum pengguna platform digital sangat ditentukan oleh norma yang tertulis dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), dan Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Swasta.

b. Pendekatan Konseptual (*Conceptual Approach*)

Pendekatan konseptual digunakan untuk membangun kerangka berpikir yang kokoh mengenai konsep-konsep hukum yang menjadi dasar analisis penelitian ini. Dalam penelitian hukum normatif, pendekatan konseptual sangat penting karena memberikan pemahaman mendalam mengenai makna, ruang lingkup, dan hubungan antar konsep hukum yang relevan. Pendekatan ini tidak hanya menguraikan definisi, tetapi juga menelusuri bagaimana konsep tersebut berkembang dalam doktrin hukum, teori hukum, dan literatur akademik. Dalam konteks penelitian ini, terdapat beberapa konsep kunci yang harus dipahami secara mendalam, yaitu perlindungan hukum, kerugian, tanggung jawab hukum, hak privasi, dan Penyelenggara Sistem Elektronik (PSE). Pendekatan konseptual membandingkan teori perlindungan hukum Hadjon dengan konteks digital,⁵⁵

c. Pendekatan Kasus (*Case Approach*)

Pendekatan kasus (*case approach*) dalam penelitian ini digunakan untuk menelaah bagaimana norma hukum mengenai perlindungan pengguna dan tanggung jawab Penyelenggara Sistem Elektronik (PSE) diterapkan dalam praktik melalui analisis terhadap berbagai insiden kebocoran data dan kegagalan sistem elektronik yang terjadi di Indonesia. Pendekatan ini penting

⁵⁵ Hadjon, *Op.Cit.*, h. 49

karena memperlihatkan kesenjangan antara norma hukum yang ideal dengan realitas implementasi di lapangan.

1.7.3 Sumber Bahan Hukum

Sumber bahan hukum untuk penelitian ini terdiri dari:

a. Bahan Hukum Primer

Bahan hukum primer adalah bahan hukum yang memiliki kekuatan mengikat, meliputi:

- 1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo. UU 19/2016
- 2) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi
- 3) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik
- 4) Permenkominfo Nomor 5 Tahun 2020 tentang PSE Lingkup Privat

b. Bahan Hukum Sekunder

Bahan hukum sekunder merupakan sumber yang berfungsi memberikan penjelasan, pemahaman, serta interpretasi terhadap bahan hukum primer. Kehadiran bahan hukum sekunder membantu peneliti memperluas perspektif dan menafsirkan norma-norma hukum yang terdapat dalam peraturan perundang-undangan.⁵⁶ Melalui literatur seperti buku, artikel ilmiah, hasil penelitian, maupun tulisan akademik lainnya, peneliti dapat memperoleh konteks teoretis dan analitis yang lebih mendalam. Oleh karena itu, bahan hukum sekunder berperan penting dalam memperkaya analisis terhadap isu yang diteliti dan memastikan bahwa kajian terhadap bahan hukum primer dilakukan secara komprehensif dan argumentatif.

c. Bahan Hukum Tersier

Bahan hukum tersier merupakan sumber yang berfungsi memberikan arahan dan penjelasan tambahan terhadap bahan hukum primer

⁵⁶ Suteki, "Perlindungan Hukum Dalam Perspektif Negara Hukum." *Jurnal Hukum Dan Pembangunan* 48, No. 3, 2018, h. 55–68.

maupun sekunder. Sumber ini biasanya berupa kamus hukum, ensiklopedia, atau kamus bahasa Indonesia yang membantu peneliti memahami istilah-istilah teknis atau konsep hukum yang sulit ditafsirkan secara langsung dari peraturan atau literatur akademik. Selain itu, bahan hukum tersier juga dapat diperoleh melalui berbagai sumber digital, seperti laman resmi pemerintah, basis data hukum, maupun jurnal ilmiah yang relevan dengan topik penelitian. Kehadiran bahan hukum tersier sangat membantu peneliti untuk memastikan ketepatan makna, memperjelas konteks, dan memperkuat pemahaman konseptual dalam proses analisis hukum

1.7.4 Teknik Pengumpulan Bahan Hukum

Penelitian ini menggunakan dua cara yaitu:

- a. *Online*, pengumpulan bahan hukum secara online merupakan bagian dari studi kepustakaan (*library research*) yang dilakukan dengan memanfaatkan berbagai sumber digital melalui penelusuran internet. Metode ini memungkinkan peneliti mengakses beragam data sekunder yang relevan, seperti jurnal ilmiah, artikel akademik, peraturan perundang-undangan, dan dokumen resmi yang tersedia pada basis data daring. Melalui pencarian digital ini, peneliti dapat memperoleh informasi yang lebih luas, mutakhir, dan terverifikasi untuk mendukung analisis dalam penelitian yang sedang dilakukan
- b. *Offline*, pengumpulan bahan hukum ini dalam studi kepustakaan (*library research*) dilakukan dengan menghimpun bahan hukum secara langsung melalui kunjungan ke berbagai sumber fisik, seperti toko buku, perpustakaan umum, maupun perpustakaan kampus termasuk perpustakaan Universitas Gresik. Melalui metode ini, peneliti dapat mengakses buku-buku hukum, jurnal cetak, laporan penelitian, dan dokumen akademik lainnya yang relevan dengan topik penelitian

1.7.5 Teknik Analisis Bahan Hukum

Teknik analisis bahan hukum dalam penelitian ini menggunakan analisis deskriptif kualitatif, yaitu metode yang menafsirkan bahan hukum melalui penalaran hukum tanpa menggunakan data numerik. Proses analisis dimulai dengan menginventarisasi seluruh bahan hukum primer, sekunder, dan tersier yang relevan, kemudian mengklasifikasikannya berdasarkan isu penelitian seperti perlindungan hukum, tanggung jawab PSE, dan kerugian pengguna. Setelah bahan hukum terstruktur, peneliti melakukan penafsiran hukum menggunakan beberapa metode interpretasi, antara lain interpretasi gramatikal untuk memahami makna tekstual norma, interpretasi sistematis untuk melihat hubungan antar pasal dalam satu regulasi maupun antar regulasi yang berbeda, serta interpretasi teleologis untuk memahami tujuan pembentuk undang-undang dalam mengatur perlindungan pengguna platform digital. Seluruh hasil interpretasi tersebut kemudian dianalisis secara deduktif, yaitu menarik kesimpulan dari norma umum menuju jawaban atas rumusan masalah penelitian. Dengan pendekatan ini, peneliti dapat menilai konsistensi, kecukupan, dan efektivitas pengaturan hukum yang berlaku, sekaligus mengidentifikasi kelemahan atau kekosongan hukum yang berdampak pada perlindungan pengguna platform digital.

1.8 Sistematika Penulisan

Sistematika penulisan dalam proposal ini disusun untuk memberikan alur pembahasan yang runtut, logis, dan mudah dipahami. Setiap bab dirancang saling berkaitan sehingga mampu menggambarkan keseluruhan proses penelitian secara komprehensif, mulai dari latar belakang permasalahan hingga metode yang digunakan. Penulisan dibagi ke dalam empat bab utama yang saling berkaitan dan membentuk alur pembahasan yang runtut, mulai dari pengantar penelitian hingga kesimpulan akhir. Adapun sistematika penulisan tersebut adalah sebagai berikut::

Bab I Pendahuluan

Bab ini berisi uraian mengenai dasar dan arah penelitian. Di dalamnya mencakup latar belakang, yang menjelaskan alasan pentingnya penelitian dilakukan

serta konteks permasalahan yang diangkat. Rumusan masalah yang merumuskan pertanyaan penelitian secara jelas dan terarah, tujuan penelitian yang menggambarkan sasaran yang ingin dicapai. Manfaat penelitian, baik bagi peneliti, akademisi, maupun pihak terkait lainnya. Tinjauan Pustaka yang memuat teori, konsep, dan penelitian terdahulu yang relevan. Metode Penelitian, yang terdiri dari jenis penelitian, metode pendekatan, sumber bahan hukum, teknik pengumpulan bahan hukum, dan teknik analisis bahan hukum, dan sistematika penulisan yang menjelaskan struktur keseluruhan skripsi.

Bab II Pembahasan Batasan Kerugian Akibat Kebocoran Data Pribadi Konsumen *E-Commerce*

Bab ini menguraikan hasil analisis terhadap rumusan masalah pertama. Pembahasan disusun dalam beberapa sub-bab yang terdiri dari pembahasan konsep dan klasifikasi kerugian dalam hukum yang meliputi pengertian kerugian dalam hukum perdata, jenis kerugian dalam materiil dan immaterial, serta kerugian dalam konteks digital. Selanjutnya diuraikan dasar hukum kerugian dalam sistem elektronik yang mencakup kerugian dalam perspektif KUHPerdata (perbuatan melawan hukum dan wanprestasi), kerugian dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), kerugian dalam Peraturan Pemerintah Nomor 71 Tahun 2019, serta kerugian dalam Undang-Undang Perlindungan Data Pribadi (UU PDP). Kemudian dibahas batasan kerugian yang dapat dimintakan pertanggungjawaban yang meliputi unsur kerugian yang dapat dituntut, hubungan kausalitas dalam sistem elektronik, dan pembatasan tanggung jawab (*safe harbour* dan *force majeure*). Selanjutnya dianalisis kerugian dalam perspektif perlindungan konsumen digital yang mencakup pengguna sebagai konsumen dalam sistem elektronik, hak ganti rugi dalam Undang-Undang Perlindungan Konsumen, ketimpangan posisi antara PSE dan pengguna, serta keterbatasan perlindungan konsumen digital. Bab ini ditutup dengan analisis kritis pengaturan batasan kerugian di Indonesia yang membahas fragmentasi pengaturan dan ketidakpastian hukum, keterbatasan pengakuan terhadap kerugian immaterial, problematika pembuktian dalam sistem elektronik, serta kelemahan dalam mekanisme penegakan hukum

Bab III Pembahasan Tanggung Jawab Hukum Penyelenggara *E-Commerce* Atas Kebocoran Data Konsumen

Bab ini membahas rumusan masalah kedua secara mendalam. Bab ini diawali dengan pembahasan konsep pertanggungjawaban hukum dalam sistem elektronik yang meliputi pengertian pertanggungjawaban hukum, prinsip-prinsip pertanggungjawaban hukum, serta pertanggungjawaban hukum dalam sistem elektronik. Selanjutnya diuraikan mengenai bentuk pertanggungjawaban penyelenggara sistem elektronik yang meliputi pertanggungjawaban perdata, administratif, pidana, dan pertanggungjawaban dalam konteks perlindungan data pribadi. Kemudian dibahas dasar penentuan tanggung jawab penyelenggara sistem elektronik yang meliputi prinsip tanggung jawab berdasarkan kesalahan, prinsip praduga bertanggung jawab, prinsip tanggung jawab mutlak, serta penentuan prinsip yang tepat dalam sistem elektronik. Selanjutnya dianalisis pertanggungjawaban yang mencakup praktik pertanggungjawaban oleh penyelenggara sistem elektronik, kendala dalam penegakan pertanggungjawaban, dan penyelesaian sengketa dalam sistem elektronik. Bab ini ditutup dengan analisis kritis pertanggungjawaban penyelenggara sistem elektronik yang membahas ketidakefektifan sistem pertanggungjawaban berbasis kesalahan, kelemahan perlindungan hukum terhadap pengguna, kebutuhan pergeseran prinsip pertanggungjawaban, serta perlunya penguatan regulasi dan mekanisme penegakan hukum.

Bab IV Penutup

Bab ini memuat kesimpulan dari seluruh pembahasan skripsi serta saran-saran yang bersifat konstruktif bagi pemerintah, Penyelenggara Sistem Elektronik, pengguna platform digital, serta peneliti selanjutnya.

Dengan sistematika tersebut, penelitian ini diharapkan mampu memberikan gambaran yang utuh, terstruktur, dan mudah dipahami mengenai perlindungan hukum pengguna platform digital terhadap kerugian yang ditimbulkan oleh Penyelenggara Sistem Elektronik.