

Perlindungan Hukum dan Ganti Kerugian Bagi Korban Kebocoran Data Pribadi dalam Transaksi Digital: Perspektif Hukum Perdata Indonesia

Lolita Permanasari, Indawati

Fakultas Hukum Universitas Bhayangkara Surabaya

Correspondence: lolita@ubhara.ac.id, indawati@ubhara.ac.id

Article Info	Abstract
Keywords: Personal Data Protection, Compensation, Civil Liability. Submitted: 03-08-2026 Revised: 03-08-2026 Accepted: 13-10-2026 Published: 14-10-2026	<i>Personal data breaches in digital transactions raise legal concerns regarding the protection of data subjects and compensation mechanisms. Although Law Number 27 of 2022 on Personal Data Protection (PDP Law) grants data subjects the right to obtain compensation, the construction of civil liability, evidentiary mechanisms, and parameters for assessing damages remain insufficiently regulated. This study aims to analyze the right of data subjects to claim compensation, the relationship between the PDP Law and the Indonesian Civil Code, and the civil liability of data controllers from the perspective of Indonesian civil law. This normative legal research employs statutory, conceptual, case, and comparative approaches through library research. The findings demonstrate that the PDP Law and the Indonesian Civil Code operate complementarily, allowing breach of contract and unlawful act claims to be applied according to the legal relationship between the parties. This study proposes a risk-based civil liability model through the application of a presumption of liability against data controllers to strengthen the protection and recovery of victims' rights arising from personal data breaches.</i>
	Abstrak
Kata Kunci: Pelindungan Data Pribadi, Ganti Kerugian, Pertanggungjawaban Perdata.	Kebocoran data pribadi dalam transaksi digital menimbulkan persoalan hukum mengenai perlindungan hak subjek data dan mekanisme ganti kerugian. Meskipun Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) telah memberikan hak kepada subjek data untuk memperoleh ganti kerugian, konstruksi pertanggungjawaban perdata, mekanisme pembuktian, dan parameter kerugian belum diatur secara komprehensif. Penelitian ini bertujuan menganalisis hak subjek data dalam menuntut ganti kerugian, hubungan UU PDP dengan Kitab Undang-Undang Hukum Perdata (KUHPperdata), serta mekanisme pertanggungjawaban pengendali data dalam perspektif hukum perdata Indonesia. Penelitian menggunakan metode hukum normatif dengan pendekatan perundang-undangan, konseptual, kasus, dan perbandingan melalui studi kepustakaan. Hasil penelitian menunjukkan bahwa UU PDP dan KUHPperdata memiliki hubungan yang saling melengkapi, sehingga gugatan wanprestasi dan perbuatan melawan hukum dapat digunakan sesuai karakteristik hubungan hukum para pihak. Penelitian ini menawarkan rekonstruksi pertanggungjawaban perdata berbasis risiko melalui penerapan praduga tanggung jawab terhadap pengendali data untuk memperkuat perlindungan dan pemulihan hak korban kebocoran data pribadi.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong terjadinya transformasi fundamental dalam berbagai sektor kehidupan masyarakat, terutama pada aktivitas ekonomi berbasis digital. Perdagangan melalui *electronic commerce (e-commerce)*, layanan keuangan digital (*financial technology*), *cloud computing*, layanan kesehatan elektronik, hingga penggunaan kecerdasan buatan (*artificial intelligence*) telah mengubah pola interaksi antara pelaku usaha dengan konsumen. Dalam ekosistem tersebut, data pribadi tidak lagi dipandang semata-mata sebagai informasi mengenai identitas seseorang, melainkan telah berkembang menjadi aset ekonomi (*economic asset*) yang memiliki nilai komersial tinggi. Pengumpulan, penyimpanan, analisis, dan pemanfaatan data pribadi menjadi fondasi utama dalam pengembangan model bisnis digital yang berorientasi pada personalisasi layanan, pemasaran berbasis perilaku konsumen (*behavioral advertising*), serta pengambilan

keputusan berbasis data (*data-driven decision making*).¹

Fenomena tersebut membawa konsekuensi hukum yang signifikan. Semakin masifnya aktivitas pemrosesan data pribadi, secara implisit cenderung membuka jalan untuk meningkatkan potensi penyalahgunaan data, akses tanpa hak, pencurian identitas (*identity theft*), penipuan digital (*online fraud*), hingga perdagangan data pribadi secara ilegal. Dalam konteks ini, kebocoran data pribadi tidak hanya menimbulkan kerugian ekonomi, tetapi juga mengancam hak atas privasi sebagai bagian dari hak asasi manusia. Sehingga perlindungan terhadap data pribadi tidak lagi dipandang sebagai isu teknis keamanan siber semata, melainkan telah berkembang menjadi bagian dari perlindungan hak konstitusional warga negara.²

Dalam ruang lingkup domestik, jaminan terhadap perlindungan privasi memperoleh legitimasi konstitusional melalui Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang memberikan perlindungan atas diri pribadi, keluarga, kehormatan, martabat, serta rasa aman dari ancaman terhadap hak-hak individu. Meskipun ketentuan tersebut tidak secara eksplisit menyebutkan data pribadi, Mahkamah Konstitusi dalam berbagai pertimbangannya telah menempatkan hak atas privasi sebagai bagian yang tidak terpisahkan dari hak konstitusional warga negara. Atas dasar hal itu, perlindungan data pribadi merupakan perwujudan konkret dari penghormatan terhadap hak privasi yang wajib dijamin oleh negara.

Urgensi perlindungan hukum terhadap data pribadi semakin mengemuka setelah berbagai insiden kebocoran data berskala besar yang terjadi dalam beberapa tahun terakhir. Berbagai laporan menunjukkan bahwa jutaan data masyarakat Indonesia pernah mengalami kebocoran, baik yang berasal dari penyelenggara sistem elektronik sektor publik maupun sektor privat. Kebocoran data tersebut meliputi informasi identitas penduduk, data pelanggan layanan digital, data kesehatan, data perbankan, hingga data transaksi elektronik.³ Karakteristik kebocoran data di era digital memiliki dimensi yang berbeda dibandingkan kerugian dalam hubungan hukum konvensional. Kerugian yang dialami korban sering kali bersifat tidak langsung (*indirect loss*), berkelanjutan (*continuing harm*), bahkan sulit diukur secara ekonomi karena menyangkut hilangnya kontrol individu atas data pribadinya.⁴

Persoalan tersebut menunjukkan bahwa kerugian akibat kebocoran data pribadi tidak dapat direduksi hanya sebagai kerugian materiil. Penyalahgunaan data pribadi dapat memunculkan dampak psikologis berupa rasa cemas, hilangnya rasa aman, kerusakan reputasi, diskriminasi digital, hingga pencurian identitas yang dapat berlangsung dalam jangka waktu panjang. Dalam perkembangan hukum perlindungan data modern, kerugian immateriil akibat pelanggaran privasi semakin memperoleh pengakuan sebagai bentuk kerugian yang layak mendapatkan kompensasi. Oleh sebab itu, konsep ganti kerugian dalam sengketa kebocoran data memerlukan pendekatan yang lebih luas dibandingkan paradigma hukum perdata klasik yang cenderung berorientasi pada kerugian ekonomi semata, berdasarkan Regulation (EU) 2016/679 (General Data Protection Regulation/GDPR), khususnya Pasal 82 jo. Recital 146.

Sebagai bentuk respons terhadap perkembangan tersebut, Indonesia mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) yang menjadi tonggak penting dalam pembentukan rezim hukum perlindungan data nasional. UU PDP mengatur prinsip-prinsip pemrosesan data pribadi, hak-hak subjek data, kewajiban pengendali dan prosesor data, mekanisme pengawasan, serta sanksi administratif maupun pidana terhadap pelanggaran pengelolaan data pribadi. Salah satu aspek penting yang diperkenalkan oleh UU PDP adalah pengakuan terhadap hak subjek data untuk memperoleh ganti kerugian apabila terjadi pelanggaran terhadap data pribadinya.

Meskipun demikian, pengaturan mengenai hak atas ganti kerugian dalam UU PDP masih menyisakan sejumlah persoalan konseptual maupun praktis. UU PDP belum memberikan parameter yang jelas mengenai bentuk kerugian yang dapat dimintakan kompensasi, metode penilaian kerugian

¹ Daniel J. Solove, *Understanding Privacy* (Cambridge: Harvard University Press, 2008), hlm.1-5.

² OECD, *The OECD Privacy Framework* (Paris: OECD Publishing, 2013), hlm.15-18.

³ Melinda Putri Lutfi et.al, "Urgensi Perlindungan Hukum Terhadap Data Privasi Nasabah Bank Di Era Perkembangan Digital", *Jurnal Multidisiplin Ilmu Akademik*, Vol.1, No.5 (Oktober 2024): 210-218

⁴ Suratman Hukum, et.al, "The Urgency of Legal Regulation for Personal Data Protection in Indonesia in the Big Data Era", *Hakim: Jurnal Ilmu Hukum Dan Sosial*, Vol 3, No. 1 (Februari 2025): 974-992.

immateriil, standar pembuktian hubungan kausal antara kebocoran data dan kerugian yang dialami korban, maupun mekanisme penentuan besaran ganti rugi oleh pengadilan. Kekosongan pengaturan tersebut berpotensi menimbulkan ketidakpastian hukum karena hakim masih harus merujuk pada rezim hukum perdata umum yang diatur dalam Kitab Undang-Undang Hukum Perdata (KUHPerdata).⁵

Dalam perspektif hukum perdata Indonesia, kebocoran data pribadi dapat melahirkan dua konstruksi pertanggungjawaban hukum yang berbeda, yaitu wanprestasi dan perbuatan melawan hukum (*onrechtmatige daad*). Gugatan wanprestasi dimungkinkan apabila hubungan antara subjek data dengan pengendali data lahir dari suatu hubungan kontraktual, misalnya dalam penggunaan layanan *marketplace*, perbankan digital, atau penyelenggara jasa keuangan berbasis teknologi. Sebaliknya, gugatan berdasarkan Pasal 1365 KUHPerdata dapat diajukan apabila pelanggaran terhadap data pribadi memenuhi unsur-unsur perbuatan melawan hukum, baik terdapat hubungan kontraktual maupun tidak. Dualisme dasar gugatan tersebut memunculkan persoalan mengenai batas penerapan masing-masing rezim pertanggungjawaban, khususnya ketika suatu kebocoran data sekaligus merupakan pelanggaran terhadap kewajiban kontraktual dan kewajiban hukum yang bersumber dari peraturan perundang-undangan.

Permasalahan lain yang belum memperoleh perhatian memadai adalah mengenai hubungan antara UU PDP sebagai *lex specialis* dengan KUHPerdata sebagai hukum perdata umum. Secara teoritis, keberadaan UU PDP tidak serta-merta mengesampingkan penerapan KUHPerdata, karena UU PDP lebih banyak mengatur hak dan kewajiban dalam pemrosesan data pribadi tanpa memberikan konstruksi yang lengkap mengenai mekanisme pertanggungjawaban perdata. Hubungan kedua rezim hukum tersebut seharusnya dipahami secara komplementer. UU PDP memberikan dasar normatif mengenai hak atas perlindungan data pribadi, sedangkan KUHPerdata menyediakan instrumen hukum mengenai pembuktian, hubungan kausal, bentuk pertanggungjawaban, serta penentuan besaran ganti kerugian. Pendekatan integratif ini menjadi penting untuk menghindari terjadinya kekosongan hukum (*legal vacuum*) dalam penyelesaian sengketa kebocoran data pribadi.⁶

Di sisi lain, perkembangan teknologi digital telah melahirkan tantangan baru yang belum sepenuhnya diantisipasi oleh sistem hukum nasional. Penggunaan kecerdasan buatan generatif (*generative artificial intelligence*), pemanfaatan big data *analytics*, perdagangan data oleh data broker, serta praktik transfer data lintas negara (*cross-border data transfer*) semakin memperumit konstruksi pertanggungjawaban hukum pengendali data. Risiko kebocoran data tidak lagi hanya berasal dari serangan siber (*cyber attack*), tetapi juga dapat timbul akibat penggunaan algoritma, pemrosesan otomatis, atau kerja sama lintas yurisdiksi yang melibatkan banyak pihak. Pada kondisi ini, pembuktian unsur kesalahan (*fault liability*) sebagaimana dikenal dalam hukum perdata klasik menjadi semakin sulit dilakukan oleh korban karena sebagian besar informasi mengenai pengelolaan sistem berada dalam penguasaan pengendali data.⁷

Menurut hemat penulis, kondisi tersebut menunjukkan perlunya rekonstruksi konsep pertanggungjawaban perdata terhadap kebocoran data pribadi. Model pertanggungjawaban yang hanya bertumpu pada pembuktian kesalahan oleh korban tidak lagi memadai untuk menghadapi karakteristik risiko teknologi digital yang kompleks dan asimetris. Pengendali data sebagai pihak yang menguasai sistem informasi, menentukan tujuan pemrosesan data, serta memperoleh manfaat ekonomi dari pemanfaatan data pribadi seharusnya memikul beban tanggung jawab yang lebih besar berdasarkan prinsip akuntabilitas (*accountability principle*) sebagaimana berkembang dalam rezim perlindungan data modern. Dengan demikian, pengembangan konsep pembalikan beban pembuktian secara terbatas (*limited reversal of burden of proof*) atau *presumption of liability* patut dipertimbangkan sebagai bentuk penguatan perlindungan hukum bagi subjek data dalam sengketa perdata akibat kebocoran data pribadi.

Berangkat dari uraian tersebut, penelitian ini mengkaji tiga permasalahan pokok, yaitu: (1)

⁵ Daniel Johnson Goenawan, et.al. "PMH di Era Digital: Pertanggungjawaban Perdata atas Penyalahgunaan Data Pribadi". *Al-Zayn : Jurnal Ilmu Sosial & Hukum*, Vol. 4, No.1 (Januari 2026): 205-213

⁶ Rosa Agustina, *Perbuatan Melawan Hukum* (Jakarta: Pascasarjana Fakultas Hukum Universitas Indonesia, 2003), 37-45.

⁷ Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford: Oxford University Press, 2015), 247-259.

bagaimana hak subjek data untuk memperoleh ganti kerugian menurut UU PDP; (2) bagaimana hubungan normatif antara UU PDP dan KUHPerdata dalam penyelesaian sengketa kebocoran data pribadi; serta (3) bagaimana konstruksi gugatan wanprestasi dan perbuatan melawan hukum terhadap pengendali data dalam perspektif hukum perdata Indonesia. Penelitian ini menawarkan kebaruan (*novelty*) berupa rekonstruksi model pertanggungjawaban perdata yang mengintegrasikan ketentuan UU PDP dengan doktrin hukum perdata Indonesia melalui pendekatan berbasis risiko (*risk-based civil liability*), sehingga diharapkan mampu memberikan kepastian hukum sekaligus memperkuat perlindungan hak subjek data pada era ekonomi digital.

METODE

1. Pendekatan

Penelitian ini merupakan penelitian hukum normatif (*normative legal research*) yang berorientasi pada pengkajian norma-norma hukum positif, asas hukum, doktrin, serta konsep-konsep hukum yang berkaitan dengan perlindungan hukum dan pertanggungjawaban perdata terhadap kebocoran data pribadi dalam transaksi digital. Penelitian hukum normatif dipilih karena fokus utama penelitian ini tidak diarahkan untuk menguji perilaku masyarakat maupun efektivitas penerapan hukum secara empiris, melainkan untuk menganalisis sinkronisasi, konsistensi, serta konstruksi norma hukum yang mengatur hak subjek data dalam memperoleh ganti kerugian akibat pelanggaran perlindungan data pribadi. Pendekatan ini relevan mengingat persoalan hukum yang dikaji berpusat pada adanya kekosongan norma (*normative gap*) mengenai mekanisme gugatan perdata pasca berlakunya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), khususnya mengenai hubungan antara ketentuan dalam UU PDP dengan rezim wanprestasi dan perbuatan melawan hukum dalam Kitab Undang-Undang Hukum Perdata (KUHPerdata).⁸

Pendekatan penelitian yang digunakan terdiri atas beberapa pendekatan hukum (*multi-approach*), yaitu *statute approach*, *conceptual approach*, *case approach*, dan *comparative approach*. Pendekatan perundang-undangan (*statute approach*) dilakukan dengan menelaah berbagai ketentuan peraturan perundang-undangan yang mengatur mengenai perlindungan data pribadi, transaksi elektronik, serta pertanggungjawaban perdata, antara lain Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Kitab Undang-Undang Hukum Perdata, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024, serta Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Melalui pendekatan ini, penelitian berupaya mengidentifikasi adanya harmonisasi maupun potensi konflik norma dalam pengaturan pertanggungjawaban hukum terhadap pengendali data pribadi.⁹

Selain pendekatan peraturan perundang-undangan, penelitian ini juga menggunakan pendekatan konseptual (*conceptual approach*). Pendekatan ini dilakukan melalui pengkajian berbagai doktrin dan teori hukum yang berkembang dalam literatur mengenai perlindungan data pribadi, hak privasi, pertanggungjawaban perdata, serta teori perlindungan hukum. Penggunaan pendekatan konseptual dimaksudkan untuk membangun argumentasi hukum mengenai kedudukan hak atas data pribadi sebagai bagian dari hak keperdataan yang melekat pada setiap individu serta untuk menganalisis konsep ganti kerugian akibat pelanggaran data pribadi yang belum diatur secara rinci dalam UU PDP. Dalam konteks ini, penelitian tidak hanya mendasarkan analisis pada norma hukum positif, tetapi juga mempertimbangkan perkembangan doktrin hukum modern mengenai *privacy rights*, *civil liability*, dan prinsip akuntabilitas (*accountability principle*) yang berkembang dalam rezim perlindungan data internasional.¹⁰

Penelitian ini juga menggunakan pendekatan kasus (*case approach*) melalui analisis terhadap berbagai kasus kebocoran data pribadi yang terjadi di Indonesia sebagai bahan untuk memahami kecenderungan permasalahan hukum dalam praktik. Pendekatan kasus tidak hanya

⁸ Peter Mahmud Marzuki, *Penelitian Hukum*, (Jakarta: Kencana Prenada Media Group, 2021), 55–60.

⁹ *Ibid*, hlm. 133–141.

¹⁰ Johnny Ibrahim, *Teori dan Metodologi Penelitian Hukum Normatif* (Malang: Bayumedia Publishing, 2006), 300–310.

diarahkan pada putusan pengadilan yang telah memperoleh kekuatan hukum tetap, tetapi juga terhadap berbagai peristiwa kebocoran data yang menjadi perhatian publik dan memunculkan tuntutan pertanggungjawaban hukum terhadap pengendali data. Analisis terhadap kasus-kasus tersebut diperlukan untuk mengidentifikasi bentuk kerugian yang dialami subjek data, pola pertanggungjawaban yang diterapkan, serta hambatan pembuktian yang dihadapi korban dalam mengajukan gugatan perdata. Pendekatan ini menjadi penting mengingat implementasi UU PDP masih berada pada tahap awal sehingga praktik peradilan mengenai sengketa kebocoran data pribadi belum berkembang secara memadai.¹¹

Selanjutnya, penelitian ini menggunakan pendekatan perbandingan (*comparative approach*) dengan mengkaji prinsip-prinsip pertanggungjawaban perdata dalam *General Data Protection Regulation* (GDPR) Uni Eropa sebagai salah satu instrumen perlindungan data pribadi yang banyak dijadikan rujukan dalam pembentukan UU PDP. Perbandingan tersebut difokuskan pada pengaturan mengenai hak subjek data untuk memperoleh kompensasi, konsep *controller liability*, pembagian tanggung jawab antara *controller* dan *processor*, serta penerapan prinsip akuntabilitas dalam pembuktian pelanggaran data pribadi. Pendekatan komparatif dimaksudkan bukan untuk mengadopsi secara langsung sistem hukum asing, melainkan untuk memperoleh perspektif mengenai praktik terbaik (*best practices*) yang dapat menjadi bahan evaluasi terhadap sistem pertanggungjawaban hukum perdata di Indonesia.¹²

2. Bahan Dan Alat Utama

Bahan hukum yang digunakan dalam penelitian ini terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer meliputi seluruh peraturan perundang-undangan yang berkaitan dengan perlindungan data pribadi, transaksi elektronik, hukum perdata, serta berbagai instrumen hukum internasional yang relevan. Bahan hukum sekunder terdiri atas buku-buku, artikel jurnal ilmiah nasional maupun internasional, hasil penelitian, pendapat para ahli, serta karya ilmiah lain yang membahas perlindungan data pribadi, hukum perdata, hukum siber, dan hak atas privasi. Adapun bahan hukum tersier berupa kamus hukum, ensiklopedia hukum, serta berbagai sumber referensi lain yang memberikan penjelasan terhadap istilah-istilah hukum yang digunakan dalam penelitian ini.¹³

3. Teknik Pengumpulan Data

Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*) dengan menelusuri berbagai literatur, dokumen hukum, putusan pengadilan, publikasi ilmiah, serta peraturan perundang-undangan yang memiliki relevansi dengan isu penelitian. Seluruh bahan hukum kemudian diinventarisasi, diklasifikasikan berdasarkan pokok bahasan, dan dianalisis secara sistematis untuk menemukan hubungan antara norma hukum yang satu dengan norma hukum lainnya. Teknik ini memungkinkan peneliti memperoleh pemahaman yang utuh mengenai perkembangan konsep perlindungan hukum terhadap data pribadi sekaligus mengidentifikasi adanya kekosongan maupun inkonsistensi pengaturan dalam sistem hukum Indonesia.¹⁴

4. Teknik Analisis

Analisis bahan hukum dilakukan secara kualitatif dengan menggunakan metode penafsiran hukum (*legal interpretation*) dan penalaran hukum (*legal reasoning*) yang bersifat preskriptif. Penelitian tidak hanya mendeskripsikan ketentuan hukum yang berlaku, tetapi juga melakukan evaluasi kritis terhadap kecukupan norma dalam memberikan perlindungan hukum bagi korban kebocoran data pribadi. Analisis dilakukan melalui penafsiran gramatikal, sistematis, dan teleologis terhadap ketentuan UU PDP serta KUHPperdata untuk memperoleh konstruksi hukum yang mampu menjawab persoalan pertanggungjawaban perdata dalam transaksi digital. Selanjutnya, hasil analisis digunakan sebagai dasar dalam merumuskan model rekonstruksi pertanggungjawaban perdata yang lebih adaptif terhadap perkembangan teknologi informasi dan karakteristik risiko kebocoran data pribadi pada era ekonomi digital. Sehingga penelitian ini tidak

¹¹ Peter Mahmud Marzuki, *Op.Cit.*, hlm. 158–162.

¹² Farah Naurah Khansa, "Penguatan Hukum Dan Urgensi Otoritas Pengawas Independen Perlindungan Data Pribadi," *Rewang Rencang: Jurnal Hukum Lex Generalis*, Vol. 2, No. 8 (Agustus 2021): 18-22

¹³ Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat* (Jakarta: RajaGrafindo Persada, 2015), hlm. 12-15.

¹⁴ *Ibid*, hlm. 21-24.

hanya menghasilkan deskripsi mengenai hukum positif (*ius constitutum*), tetapi juga menawarkan rekomendasi pengembangan hukum (*ius constituendum*) sebagai upaya memperkuat efektivitas perlindungan hukum terhadap subjek data di Indonesia.¹⁵

HASIL

Hak Subjek Data Untuk Menuntut Ganti Kerugian Dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi

Perlindungan terhadap data pribadi pada hakikatnya merupakan bentuk perlindungan terhadap hak privat (*right to privacy*) yang melekat pada setiap individu. Dalam perkembangan hukum modern, data pribadi tidak lagi dipandang sebagai sekadar informasi identitas seseorang, melainkan sebagai bagian dari hak kepribadian (*personality rights*) yang memiliki dimensi hukum, ekonomi, dan sosial. Seiring berkembangnya transaksi digital, data pribadi telah menjadi komoditas bernilai ekonomi tinggi yang dimanfaatkan oleh berbagai penyelenggara sistem elektronik untuk kepentingan penyediaan layanan, analisis perilaku konsumen, pemasaran digital, hingga pengembangan teknologi kecerdasan buatan. Kondisi tersebut menyebabkan risiko pelanggaran terhadap data pribadi semakin meningkat, sehingga negara dituntut untuk menghadirkan instrumen hukum yang mampu menjamin perlindungan hak-hak subjek data secara efektif.¹⁶

Dalam sistem hukum Indonesia, perlindungan terhadap data pribadi memperoleh legitimasi konstitusional melalui Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang menjamin hak setiap orang atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan rasa aman. Meskipun konstitusi tidak menyebutkan istilah "data pribadi" secara eksplisit, hak atas data pribadi merupakan manifestasi dari hak atas privasi yang telah diakui sebagai bagian dari hak asasi manusia. Oleh karena itu, setiap pelanggaran terhadap data pribadi pada dasarnya merupakan pelanggaran terhadap hak konstitusional warga negara yang menimbulkan konsekuensi hukum, baik dalam ranah administrasi, pidana, maupun perdata.

Penguatan perlindungan tersebut diwujudkan melalui Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi (UU PDP). Kehadiran UU PDP menandai perubahan paradigma pengaturan data pribadi di Indonesia dari pendekatan sektoral menuju rezim hukum yang lebih komprehensif. Salah satu inovasi penting dalam UU PDP adalah pengakuan terhadap hak subjek data untuk memperoleh ganti kerugian apabila terjadi pelanggaran terhadap pemrosesan data pribadi yang mengakibatkan kerugian bagi dirinya. Pengakuan hak ini menunjukkan bahwa pembentuk undang-undang tidak lagi menempatkan perlindungan data hanya sebagai kewajiban administratif bagi pengendali data, melainkan juga sebagai hubungan hukum privat yang memberikan hak keperdataan kepada subjek data untuk menuntut pemulihan atas kerugian yang dialaminya.

Hak untuk memperoleh ganti kerugian memiliki arti strategis karena merupakan instrumen yang menjembatani kepentingan perlindungan hak individu dengan prinsip pertanggungjawaban hukum (*civil liability*). Dalam perspektif hukum perdata, pemberian ganti kerugian bertujuan untuk mengembalikan keadaan korban pada posisi seandainya pelanggaran tersebut tidak pernah terjadi (*restitutio in integrum*). Akan tetapi, penerapan prinsip tersebut dalam perkara kebocoran data pribadi menghadapi tantangan yang berbeda dibandingkan sengketa perdata konvensional. Hal ini disebabkan kerugian akibat kebocoran data sering kali tidak hanya berupa kerugian ekonomi yang dapat dihitung secara pasti, tetapi juga meliputi hilangnya kontrol atas data pribadi, gangguan psikologis, kerusakan reputasi, penyalahgunaan identitas, hingga ancaman keamanan di masa mendatang. Sehingga konsep ganti kerugian dalam perkara perlindungan data pribadi memerlukan pendekatan yang lebih luas daripada sekadar kompensasi atas kerugian materiil.¹⁷

Permasalahan mendasar dalam UU PDP terletak pada belum dirumuskannya parameter yang jelas mengenai bentuk dan ruang lingkup kerugian yang dapat dimintakan ganti rugi. UU PDP mengakui adanya hak untuk menuntut ganti kerugian, tetapi tidak mengatur secara rinci apakah kerugian tersebut hanya terbatas pada kerugian materiil atau juga mencakup kerugian immateriil.

¹⁵ Peter Mahmud Marzuki, *Op.Cit.*, hlm. 213-220.

¹⁶ Desi Patul Hotima, Diki Zukriadi, "Tanggung Jawab Hukum Perdata atas Penggunaan Citra Publik Figur dalam Foto Buatan AI", *Al-Muamalat: Jurnal Ilmu Hukum & Ekonomi Syariah Vol. 11 No 1*, (Januari-Juni 2026): 93-105.

¹⁷ Rosa Agustina, *Op.Cit.*, hlm. 128-132

Kekosongan norma ini berpotensi menimbulkan perbedaan penafsiran dalam praktik peradilan. Di satu sisi, hakim dapat menggunakan ketentuan umum dalam KUHPerdata untuk memberikan kompensasi terhadap kerugian immateriil, tetapi di sisi lain tidak adanya pedoman khusus dapat menimbulkan inkonsistensi dalam penentuan besaran ganti rugi. Akibatnya, efektivitas perlindungan hukum terhadap subjek data sangat bergantung pada keberanian hakim dalam melakukan penafsiran progresif terhadap UU PDP dan KUHPerdata secara sistematis.

Menurut penulis, kelemahan tersebut menunjukkan bahwa UU PDP masih mengadopsi pendekatan normatif yang berorientasi pada pengakuan hak (*recognition of rights*), tetapi belum sepenuhnya membangun mekanisme pemulihan hak (*remedial mechanism*). Padahal, dalam rezim perlindungan data modern, hak atas ganti kerugian tidak hanya dimaksudkan sebagai bentuk kompensasi terhadap korban, tetapi juga sebagai instrumen untuk mendorong kepatuhan (*compliance*) pengendali data dalam menerapkan prinsip akuntabilitas dan keamanan sistem informasi. Tanpa mekanisme ganti rugi yang efektif, pengendali data cenderung memandang biaya pelanggaran sebagai risiko bisnis biasa sehingga tidak memiliki insentif yang memadai untuk meningkatkan standar perlindungan data.

Apabila dibandingkan dengan *General Data Protection Regulation* (GDPR) Uni Eropa, terdapat perbedaan yang cukup signifikan. Pasal 82 GDPR secara tegas memberikan hak kepada setiap orang yang mengalami kerugian materiil maupun non-materiil akibat pelanggaran GDPR untuk memperoleh kompensasi dari *controller* maupun *processor*. Ketentuan tersebut diperkuat oleh *Recital* 146 GDPR yang menegaskan bahwa konsep kerugian harus ditafsirkan secara luas agar tujuan perlindungan hak subjek data dapat tercapai secara efektif. Pendekatan tersebut menunjukkan bahwa perlindungan data pribadi tidak hanya bertujuan memberikan sanksi kepada pelaku pelanggaran, tetapi juga memastikan bahwa korban memperoleh pemulihan yang memadai.

Sebaliknya, UU PDP belum memberikan pengaturan eksplisit mengenai kerugian non-materiil. Kondisi ini dapat menimbulkan persoalan pembuktian karena korban kebocoran data sering kali mengalami kerugian yang bersifat potensial (*potential harm*) atau berkelanjutan (*continuing harm*). Sebagai contoh, kebocoran nomor induk kependudukan, data biometrik, atau informasi keuangan mungkin tidak langsung menimbulkan kerugian ekonomi pada saat data tersebut bocor. Namun, data tersebut dapat digunakan untuk pencurian identitas, pembukaan rekening secara ilegal, penipuan digital, atau penyalahgunaan lainnya di masa mendatang. Jika hakim hanya mengakui kerugian yang telah nyata terjadi (*actual damage*), maka perlindungan hukum yang diberikan kepada subjek data menjadi tidak efektif.

Persoalan lain berkaitan dengan beban pembuktian. Dalam hukum acara perdata Indonesia berlaku asas *actori incumbit probatio*, yaitu pihak yang mendalilkan suatu hak wajib membuktikannya. Dalam sengketa kebocoran data, penerapan asas tersebut menempatkan korban pada posisi yang kurang menguntungkan karena sebagian besar bukti mengenai penyebab kebocoran, sistem keamanan, dan prosedur pemrosesan data berada dalam penguasaan pengendali data. Korban umumnya hanya mengetahui bahwa data pribadinya telah bocor tanpa memiliki akses terhadap bukti teknis yang diperlukan untuk membuktikan adanya kelalaian pengendali data.

Dalam sudut pandang penulis, kondisi tersebut menunjukkan perlunya pengembangan doktrin *presumption of liability* dalam penyelesaian sengketa kebocoran data pribadi. Melalui pendekatan ini, apabila terbukti telah terjadi kebocoran data yang berada dalam penguasaan pengendali data, maka pengendali data dianggap bertanggung jawab sampai ia dapat membuktikan bahwa kebocoran tersebut terjadi di luar kesalahannya dan seluruh kewajiban keamanan telah dipenuhi sesuai standar yang berlaku. Pendekatan demikian lebih mencerminkan prinsip akuntabilitas yang menjadi dasar pengelolaan data pribadi dalam UU PDP serta sejalan dengan perkembangan hukum perlindungan data di berbagai negara.

Hak subjek data untuk memperoleh ganti kerugian tidak dapat dipahami hanya sebagai hak prosedural untuk mengajukan gugatan ke pengadilan. Hak tersebut merupakan bagian dari mekanisme perlindungan hukum yang bertujuan memulihkan hak korban sekaligus mendorong pengendali data untuk meningkatkan standar tata kelola data pribadi. Efektivitas hak atas ganti kerugian akan sangat ditentukan oleh harmonisasi antara UU PDP, KUHPerdata, hukum acara perdata, serta pembentukan yurisprudensi yang memberikan kepastian mengenai bentuk kerugian, standar pembuktian, dan mekanisme penentuan kompensasi bagi korban kebocoran data pribadi.

Hubungan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi Dengan KUHperdata Dalam Konstruksi Gugatan Wanprestasi Terhadap Pengendali Data

Pengaturan mengenai hak subjek data untuk memperoleh ganti kerugian dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) pada dasarnya tidak dapat dilepaskan dari sistem hukum perdata Indonesia. Meskipun UU PDP telah mengakui adanya hak bagi subjek data untuk menuntut ganti kerugian akibat pelanggaran pelindungan data pribadi, undang-undang tersebut belum mengatur secara komprehensif mengenai mekanisme pertanggungjawaban perdata, standar pembuktian, maupun bentuk ganti kerugian yang dapat dimohonkan oleh korban. Akibatnya, penyelesaian sengketa perdata akibat kebocoran data pribadi tetap memerlukan penerapan ketentuan umum dalam Kitab Undang-Undang Hukum Perdata (KUHPerdata), khususnya mengenai hukum perikatan, wanprestasi, dan perbuatan melawan hukum.

Dalam teori perundang-undangan, hubungan antara UU PDP dan KUHPerdata dapat dipahami melalui asas *lex specialis derogat legi generali*. Asas ini mengandung makna bahwa ketentuan yang bersifat khusus mengesampingkan ketentuan yang bersifat umum sepanjang mengatur objek hukum yang sama.¹⁸ Dalam konteks pelindungan data pribadi, UU PDP merupakan pengaturan khusus yang menetapkan hak dan kewajiban para pihak dalam kegiatan pemrosesan data pribadi, sedangkan KUHPerdata tetap menjadi dasar umum yang mengatur konsekuensi hukum apabila terjadi pelanggaran terhadap hubungan hukum tersebut. Oleh karena itu, penerapan kedua rezim hukum tersebut bukanlah bersifat saling meniadakan, melainkan saling melengkapi (*complementary legal regime*). UU PDP memberikan legitimasi terhadap hak subjek data, sedangkan KUHPerdata menyediakan instrumen hukum untuk menegakkan hak tersebut melalui mekanisme gugatan perdata.

Hubungan komplementer tersebut menjadi semakin penting karena UU PDP belum merumuskan secara rinci bentuk pertanggungjawaban perdata pengendali data (*data controller*). Ketentuan mengenai hak memperoleh ganti kerugian dalam UU PDP lebih menitikberatkan pada pengakuan hak (*recognition of rights*) daripada mekanisme pemulihan hak (*remedial mechanism*). Akibatnya, hakim dalam memeriksa sengketa kebocoran data pribadi tetap harus merujuk pada ketentuan KUHPerdata untuk menentukan apakah pelanggaran yang dilakukan pengendali data merupakan wanprestasi atau perbuatan melawan hukum, bagaimana hubungan kausal dibuktikan, serta bagaimana besaran ganti rugi ditentukan. Kondisi ini menunjukkan bahwa keberlakuan UU PDP tidak menghapus eksistensi KUHPerdata sebagai hukum dasar dalam penyelesaian sengketa keperdataan.

Secara yuridis, gugatan wanprestasi dapat diajukan apabila hubungan hukum antara subjek data dan pengendali data lahir dari suatu perjanjian. Dalam transaksi digital, hubungan kontraktual tersebut umumnya diwujudkan melalui perjanjian elektronik (*electronic contract*) atau syarat dan ketentuan penggunaan layanan (*terms and conditions*) yang disetujui oleh pengguna pada saat mendaftarkan akun atau menggunakan suatu platform digital. Walaupun persetujuan tersebut sering kali diberikan melalui mekanisme *click-wrap agreement*, secara hukum perjanjian tersebut tetap mengikat para pihak berdasarkan asas *pacta sunt servanda* sebagaimana diatur dalam Pasal 1338 ayat (1) KUHPerdata. Ketika pengendali data menjanjikan keamanan, kerahasiaan, dan pelindungan terhadap data pribadi pengguna, kewajiban tersebut menjadi bagian dari prestasi yang wajib dipenuhi.

Dalam praktik transaksi digital, kewajiban pengendali data tidak hanya terbatas pada penyediaan layanan utama, tetapi juga mencakup kewajiban menjaga kerahasiaan dan keamanan data pribadi yang dipercayakan oleh pengguna. Kewajiban tersebut memperoleh dasar hukum ganda, yaitu berasal dari hubungan kontraktual dan dari ketentuan UU PDP. Apabila terjadi kebocoran data yang disebabkan oleh kegagalan pengendali data dalam menerapkan standar keamanan yang layak, maka pelanggaran tersebut tidak hanya merupakan pelanggaran terhadap ketentuan UU PDP, tetapi juga dapat dikualifikasikan sebagai bentuk wanprestasi karena pengendali data tidak memenuhi prestasi yang telah diperjanjikan secara eksplisit maupun implisit.

Menurut doktrin hukum perjanjian, wanprestasi tidak hanya terjadi ketika debitur sama sekali tidak melaksanakan prestasi, tetapi juga apabila prestasi dilaksanakan tidak sebagaimana mestinya, terlambat dipenuhi, atau dilakukan dengan cara yang bertentangan dengan isi perjanjian.¹⁹ Dalam konteks pelindungan data pribadi, kegagalan pengendali data menerapkan sistem keamanan yang

¹⁸ Bagir Manan, *Asas-Asas Perundang-undangan Indonesia* (Jakarta: FH UII Press, 2006), hlm. 48–52

¹⁹ R. Subekti, *Hukum Perjanjian* (Jakarta: Intermasa, 2014), hlm. 45–47.

memadai, tidak melakukan pembaruan sistem (*security update*), atau lalai melakukan pengawasan terhadap akses data dapat dikategorikan sebagai bentuk pelaksanaan prestasi yang tidak sempurna (*improper performance*). Maka dari itu, sekalipun layanan digital tetap dapat digunakan oleh konsumen, kebocoran data pribadi akibat lemahnya sistem keamanan tetap dapat menjadi dasar gugatan wanprestasi karena pengendali data gagal memenuhi kewajiban kontraktualnya untuk menjaga keamanan data.

Analisis tersebut menunjukkan bahwa objek prestasi dalam hubungan hukum digital tidak lagi terbatas pada penyediaan barang atau jasa, tetapi telah berkembang mencakup kewajiban melindungi data pribadi sebagai bagian dari kualitas layanan (*quality of service*). Dengan kata lain, keamanan data bukan lagi merupakan kewajiban tambahan (*ancillary obligation*), melainkan telah menjadi unsur utama (*essential obligation*) dalam hubungan kontraktual antara penyelenggara sistem elektronik dan pengguna. Kegagalan menjaga keamanan data semestinya dipandang sebagai pelanggaran terhadap inti prestasi yang diperjanjikan.

Meskipun demikian, konstruksi wanprestasi dalam sengketa kebocoran data pribadi masih menghadapi sejumlah kendala. Salah satu persoalan utama adalah banyaknya klausula baku dalam syarat dan ketentuan layanan digital yang membatasi bahkan mengesampingkan tanggung jawab penyelenggara atas kerugian yang timbul akibat gangguan sistem atau serangan siber. Klausula semacam ini berpotensi menimbulkan ketidakseimbangan posisi tawar (*inequality of bargaining power*) antara pelaku usaha dan konsumen. Dalam praktik, pengguna hampir tidak memiliki kesempatan untuk merundingkan isi kontrak karena perjanjian disusun secara sepihak oleh penyelenggara layanan digital. Kondisi tersebut mengakibatkan persetujuan yang diberikan pengguna lebih bersifat formal daripada substantif.

Dari perspektif hukum perlindungan konsumen dan hukum perjanjian modern, keberadaan klausula yang membebaskan pengendali data dari seluruh tanggung jawab atas kebocoran data patut dipandang secara kritis. Klausula tersebut tidak sejalan dengan prinsip itikad baik (*good faith*) dan asas keseimbangan dalam hukum kontrak. Terlebih lagi, UU PDP menghendaki setiap pengendali data untuk menerapkan prinsip akuntabilitas (*accountability principle*) dalam seluruh tahapan pemrosesan data pribadi. Keberadaan klausula eksonerasi (*exoneration clause*) tidak semestinya menghapus tanggung jawab pengendali data apabila kebocoran terjadi akibat kelalaian dalam memenuhi standar keamanan yang diwajibkan oleh peraturan perundang-undangan.

Selain persoalan klausula baku, tantangan lain terletak pada pembuktian hubungan kausal (*causal relationship*) antara kebocoran data dan kerugian yang dialami oleh subjek data. Dalam gugatan wanprestasi, penggugat harus membuktikan bahwa kerugian yang dialaminya merupakan akibat langsung dari tidak dipenuhinya prestasi oleh tergugat. Persoalan ini menjadi semakin kompleks dalam perkara kebocoran data karena kerugian yang muncul sering kali tidak bersifat langsung (*direct loss*), melainkan berupa kerugian yang berkembang secara bertahap (*progressive damage*), seperti pencurian identitas, penyalahgunaan rekening, penipuan berbasis data, atau kerusakan reputasi yang baru diketahui beberapa waktu setelah insiden kebocoran terjadi. Atas dasar hal itu, penerapan standar pembuktian konvensional dalam perkara wanprestasi berpotensi mengurangi efektivitas perlindungan hukum bagi korban.

Dalam kacamata penulis, kondisi tersebut menunjukkan perlunya reinterpretasi terhadap konsep wanprestasi dalam transaksi digital. Pengendali data sebagai pihak yang menguasai sistem informasi, menentukan tujuan pemrosesan data, dan memperoleh manfaat ekonomi dari penggunaan data pribadi seharusnya memikul tanggung jawab kontraktual yang lebih besar dibandingkan konsumen. Prinsip ini sejalan dengan pendekatan *risk allocation* dalam kontrak modern yang menempatkan risiko pada pihak yang paling mampu mengendalikan dan mencegah terjadinya kerugian. Sehingga apabila terjadi kebocoran data yang berasal dari sistem pengendali data, maka seharusnya berlaku praduga tanggung jawab (*presumption of contractual liability*), dan pengendali data wajib membuktikan bahwa seluruh standar keamanan telah dipenuhi dan kebocoran terjadi karena keadaan di luar kendalinya.

Pendekatan tersebut tidak hanya memberikan perlindungan yang lebih efektif bagi subjek data, tetapi juga mendorong terciptanya budaya kepatuhan (*compliance culture*) dalam pengelolaan data pribadi. Pengendali data akan terdorong untuk meningkatkan investasi pada sistem keamanan informasi, audit kepatuhan, serta mitigasi risiko siber karena mengetahui bahwa kegagalan memenuhi kewajiban tersebut berpotensi menimbulkan konsekuensi hukum berupa tanggung jawab kontraktual. Pada konteks ini, hubungan antara UU PDP dan KUHPerdata tidak lagi dipahami sebagai hubungan

antara dua rezim hukum yang terpisah, melainkan sebagai sistem hukum yang saling melengkapi dalam memberikan perlindungan yang efektif terhadap hak-hak subjek data pada era ekonomi digital.

Gugatan Perbuatan Melawan Hukum Terhadap Pengendali Data Dalam Perspektif Rekonstruksi Pertanggungjawaban Perdata Berbasis Risiko Pada Era Transformasi Digital

Selain dapat diajukan melalui mekanisme wanprestasi, pertanggungjawaban perdata terhadap pengendali data juga dapat didasarkan pada rezim perbuatan melawan hukum (PMH) sebagaimana diatur dalam Pasal 1365 Kitab Undang-Undang Hukum Perdata (KUHPerdata). Konstruksi ini memiliki arti penting karena tidak seluruh hubungan hukum antara subjek data dengan pengendali data lahir dari suatu hubungan kontraktual. Dalam praktik transaksi digital, sering dijumpai pemrosesan data pribadi yang dilakukan oleh pihak ketiga, perusahaan afiliasi, penyedia *cloud service*, *data analytics provider*, hingga perusahaan periklanan digital (*ad-tech*) yang tidak memiliki hubungan perjanjian secara langsung dengan subjek data. Pembatasan penyelesaian sengketa hanya melalui gugatan wanprestasi akan mempersempit ruang perlindungan hukum yang seharusnya dapat dinikmati oleh korban kebocoran data pribadi.

Secara doktrinal, Pasal 1365 KUHPerdata menentukan bahwa setiap perbuatan yang melawan hukum dan menimbulkan kerugian kepada orang lain mewajibkan pelaku mengganti kerugian tersebut. Perkembangan doktrin hukum Indonesia pasca *Arrest Lindenbaum v. Cohen* (1919) telah memperluas makna perbuatan melawan hukum, sehingga tidak lagi terbatas pada pelanggaran terhadap undang-undang, tetapi juga mencakup pelanggaran terhadap hak subjektif orang lain, pelanggaran terhadap kewajiban hukum, tindakan yang bertentangan dengan kesusilaan, serta tindakan yang bertentangan dengan kepatutan, ketelitian, dan kehati-hatian dalam pergaulan masyarakat.²⁰ Perluasan makna tersebut memberikan ruang yang cukup bagi hakim untuk mengkualifikasikan kebocoran data pribadi sebagai bentuk perbuatan melawan hukum apabila pengendali data gagal memenuhi standar perlindungan yang diwajibkan oleh peraturan perundang-undangan maupun standar kepatutan dalam penyelenggaraan sistem elektronik.

Dalam konteks perlindungan data pribadi, unsur melawan hukum tidak hanya dapat didasarkan pada pelanggaran terhadap ketentuan UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), tetapi juga pada kelalaian pengendali data dalam menerapkan prinsip kehati-hatian (*duty of care*) yang semestinya menjadi standar minimum dalam pengelolaan sistem elektronik. Pengendali data pada dasarnya memegang posisi yang sangat dominan karena menguasai keseluruhan siklus pemrosesan data, mulai dari pengumpulan, penyimpanan, penggunaan, pengungkapan, hingga penghapusan data pribadi. Posisi tersebut menimbulkan kewajiban hukum untuk menjamin keamanan, kerahasiaan, integritas, dan ketersediaan data pribadi yang berada dalam penguasaannya. Setiap kegagalan dalam memenuhi kewajiban tersebut tidak hanya merupakan pelanggaran administratif sebagaimana diatur dalam UU PDP, tetapi juga dapat menimbulkan tanggung jawab keperdataan berdasarkan Pasal 1365 KUHPerdata.

Persoalan yang kemudian muncul adalah mengenai pembuktian unsur kesalahan (*fault*) dalam sengketa kebocoran data pribadi. Dalam konstruksi PMH klasik, korban harus membuktikan adanya perbuatan melawan hukum, kesalahan pelaku, kerugian, serta hubungan kausal antara perbuatan dan kerugian. Pendekatan demikian relatif mudah diterapkan dalam sengketa konvensional, namun menjadi problematis ketika diterapkan pada sengketa perlindungan data pribadi. Hal ini disebabkan sebagian besar informasi mengenai sistem keamanan, prosedur pemrosesan data, arsitektur jaringan, serta mekanisme mitigasi risiko sepenuhnya berada dalam penguasaan pengendali data. Korban umumnya hanya mengetahui bahwa data pribadinya telah bocor tanpa memiliki kemampuan teknis maupun akses terhadap alat bukti digital untuk membuktikan penyebab kebocoran tersebut. Kondisi demikian menciptakan asimetri informasi (*information asymmetry*) yang sangat tajam antara pengendali data dan subjek data, sehingga penerapan asas umum pembuktian dalam hukum acara perdata berpotensi menghambat akses korban terhadap keadilan.

Dalam sudut pandang penulis, pendekatan pertanggungjawaban yang semata-mata didasarkan pada kesalahan (*fault-based liability*) sudah tidak lagi memadai untuk menjawab karakteristik risiko dalam ekosistem digital. Berbeda dengan hubungan hukum konvensional, kebocoran data pribadi merupakan risiko sistemik yang lahir dari kompleksitas teknologi informasi, penggunaan komputasi

²⁰ Rosa Agustina, *Op.Cit.*, hlm. 43-47

awan (*cloud computing*), integrasi aplikasi, pemanfaatan *Application Programming Interface* (API), hingga pemrosesan data lintas yurisdiksi. Dalam situasi demikian, pembuktian kesalahan individual menjadi semakin sulit karena kerugian dapat timbul akibat kombinasi berbagai faktor teknis yang tidak sepenuhnya dapat diakses oleh korban. Oleh sebab itu, perlindungan hukum yang efektif tidak lagi cukup mengandalkan paradigma pertanggungjawaban klasik, tetapi memerlukan pendekatan yang lebih adaptif terhadap perkembangan teknologi.

Berdasarkan analisis tersebut, penelitian ini menawarkan rekonstruksi model pertanggungjawaban perdata pengendali data berbasis risiko (*risk-based civil liability*) sebagai nilai kebaruan (*novelty*) penelitian. Model ini dibangun atas tiga lapisan pertanggungjawaban yang saling melengkapi. Lapisan pertama adalah pertanggungjawaban kontraktual, yang berlaku apabila hubungan antara subjek data dan pengendali data lahir dari suatu perjanjian elektronik sehingga pelanggaran terhadap kewajiban menjaga keamanan data dapat dikualifikasikan sebagai wanprestasi. Lapisan kedua adalah pertanggungjawaban berdasarkan perbuatan melawan hukum, yang berlaku terhadap setiap pelanggaran hak subjek data, baik terdapat hubungan kontraktual maupun tidak. Lapisan ketiga merupakan pengembangan dari dua model tersebut, yaitu pertanggungjawaban berbasis risiko dengan penerapan praduga tanggung jawab (*presumption of liability*) terhadap pengendali data.

Model pertanggungjawaban berbasis risiko didasarkan pada argumentasi bahwa pengendali data merupakan pihak yang memiliki kendali penuh terhadap sistem pemrosesan data sekaligus memperoleh manfaat ekonomi dari pemanfaatan data pribadi. Secara prinsipil pengendali data merupakan pihak yang paling mampu mengidentifikasi, mengendalikan, dan memitigasi risiko kebocoran data. Pendekatan ini sejalan dengan prinsip akuntabilitas (*accountability*) yang menjadi salah satu prinsip fundamental dalam UU PDP maupun *General Data Protection Regulation* (GDPR) Uni Eropa berdasarkan Regulation (EU) 2016/679 (General Data Protection Regulation), khususnya Pasal 5 ayat (2), Pasal 24, dan Pasal 82. Model ini menunjukkan apabila terjadi kebocoran data yang berasal dari sistem pengendali data, maka timbul praduga hukum bahwa pengendali data bertanggung jawab, kecuali apabila ia mampu membuktikan bahwa seluruh standar keamanan telah diterapkan secara optimal dan kebocoran terjadi karena keadaan memaksa (*force majeure*) atau tindakan pihak ketiga yang sama sekali berada di luar kendalinya.

Rekonstruksi tersebut menurut penulis lebih sesuai dengan perkembangan teori pertanggungjawaban dalam hukum modern yang tidak lagi semata-mata bertumpu pada kesalahan, tetapi juga memperhatikan distribusi risiko (*risk allocation*). Pengendali data yang memperoleh manfaat ekonomi dari pemanfaatan data pribadi seharusnya juga memikul konsekuensi hukum yang proporsional terhadap risiko yang timbul dari kegiatan tersebut. Beban tanggung jawab kepada pengendali data bukan hanya dimaksudkan untuk memberikan kompensasi kepada korban, tetapi juga mendorong terciptanya budaya kepatuhan (*compliance culture*) melalui peningkatan investasi pada sistem keamanan siber, tata kelola data, audit kepatuhan, serta penguatan mekanisme manajemen risiko.

Urgensi rekonstruksi tersebut semakin mengemuka apabila dikaitkan dengan perkembangan teknologi digital yang berlangsung sangat cepat. Salah satu isu yang berkembang saat ini adalah pemanfaatan kecerdasan buatan (*artificial intelligence*), khususnya model *generative AI*, yang memerlukan data dalam jumlah sangat besar untuk proses pelatihan algoritma (*machine learning*). Dalam praktiknya, tidak seluruh data yang digunakan dalam pelatihan model AI berasal dari sumber yang secara eksplisit memberikan persetujuan. Persoalan ini menimbulkan pertanyaan mengenai batas tanggung jawab pengendali data apabila data pribadi digunakan untuk pengembangan sistem AI tanpa dasar hukum yang jelas atau mengalami kebocoran akibat proses integrasi dengan sistem kecerdasan buatan. UU PDP belum mengatur secara spesifik mengenai tanggung jawab perdata dalam konteks tersebut sehingga potensi sengketa diperkirakan akan meningkat seiring berkembangnya penggunaan AI dalam berbagai sektor.²¹

Di samping itu, praktik perdagangan data pribadi oleh data broker juga menjadi tantangan serius. Perusahaan data broker mengumpulkan, mengolah, menggabungkan, dan memperjualbelikan data pribadi kepada berbagai pihak untuk kepentingan pemasaran maupun analisis perilaku

²¹ Tri Vebri Yance, et.al, “Perlindungan Data Pribadi dalam Teknologi AI: Analisis Peran Hukum dan Kepatuhan Regulasi Bisnis Digital”, *Jurnal Ilmu Hukum: Vol. 14, No. 2*, (Agustus 2025) : 191-207

konsumen. Hubungan hukum dalam praktik tersebut sering kali berlangsung secara tidak transparan sehingga subjek data tidak mengetahui pihak-pihak yang memperoleh akses terhadap datanya. Kondisi demikian memperbesar risiko penyalahgunaan data serta menyulitkan korban dalam menentukan pihak yang harus dimintai pertanggungjawaban apabila terjadi kebocoran data. Oleh karena itu, penguatan konsep tanggung jawab bersama (*joint liability*) antara pengendali data utama dengan pihak-pihak yang memperoleh akses terhadap data menjadi salah satu kebutuhan pembaruan hukum di masa mendatang.

Isu lain yang tidak kalah penting adalah transfer data lintas negara (*cross-border data transfer*). Digitalisasi ekonomi menyebabkan sebagian besar data masyarakat Indonesia disimpan pada pusat data (*data center*) yang berada di luar wilayah hukum Indonesia. Kondisi ini menimbulkan persoalan mengenai yurisdiksi, pilihan hukum (*choice of law*), serta pelaksanaan putusan pengadilan apabila terjadi kebocoran data yang melibatkan perusahaan multinasional. Meskipun UU PDP telah mengatur mekanisme transfer data ke luar negeri, pengaturan mengenai pertanggungjawaban perdata dalam sengketa lintas batas masih memerlukan harmonisasi lebih lanjut dengan prinsip-prinsip hukum perdata internasional.

Selanjutnya, dari perspektif hukum acara perdata, penyelesaian sengketa kebocoran data yang melibatkan jutaan korban akan lebih efektif apabila difasilitasi melalui mekanisme gugatan kelompok (*class action*). Kebocoran data berskala besar umumnya menimbulkan kerugian individual yang relatif kecil tetapi berdampak terhadap jumlah korban yang sangat besar. Dalam kondisi ini, gugatan perorangan tidak efisien baik dari segi biaya maupun waktu. Pengembangan mekanisme *class action* dalam sengketa perlindungan data pribadi akan memperluas akses terhadap keadilan sekaligus meningkatkan efek jera bagi pengendali data yang lalai memenuhi kewajiban hukumnya.

Terakhir, perkembangan sengketa perlindungan data pribadi juga menuntut pembaruan dalam aspek pembuktian. Alat bukti digital (*digital evidence*) dan hasil pemeriksaan forensik digital (*digital forensic examination*) akan memegang peranan yang semakin penting dalam menentukan penyebab kebocoran data serta tingkat kesalahan pengendali data. Sehingga penguatan kapasitas lembaga penegak hukum, hakim, maupun ahli forensik digital merupakan prasyarat penting agar mekanisme pertanggungjawaban perdata yang diatur dalam UU PDP dapat diterapkan secara efektif.

Berdasarkan keseluruhan uraian tersebut, dapat ditegaskan bahwa keberhasilan implementasi UU PDP tidak hanya ditentukan oleh keberadaan norma yang mengatur hak dan kewajiban para pihak, tetapi juga oleh kemampuan sistem hukum perdata Indonesia dalam mengembangkan *role model* pertanggungjawaban yang adaptif terhadap karakteristik risiko teknologi digital. Rekonstruksi pertanggungjawaban perdata berbasis risiko yang ditawarkan dalam penelitian ini diharapkan mampu mengisi kekosongan pengaturan mengenai mekanisme ganti kerugian, memperkuat perlindungan terhadap hak-hak subjek data, serta memberikan kepastian hukum bagi penyelenggara sistem elektronik dalam menghadapi tantangan transformasi digital yang semakin kompleks.

SIMPULAN

Pertama, hak subjek data untuk memperoleh ganti kerugian telah memperoleh dasar hukum melalui Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), tetapi pengaturannya belum sepenuhnya memberikan kepastian mengenai bentuk kerugian, standar pembuktian, serta mekanisme penentuan besaran ganti kerugian. Kondisi tersebut menyebabkan pemulihan hak korban masih memerlukan integrasi dengan ketentuan hukum perdata umum dalam Kitab Undang-Undang Hukum Perdata (KUHPperdata). Dengan demikian, hak atas ganti kerugian dalam UU PDP harus dipahami sebagai hak keperdataan yang dapat ditegakkan melalui mekanisme hukum perdata, baik berdasarkan hubungan kontraktual maupun berdasarkan pelanggaran terhadap hak subjektif subjek data.

Kedua, hubungan antara UU PDP dan KUHPperdata bersifat komplementer, dengan UU PDP sebagai *lex specialis* yang memberikan dasar dan substansi perlindungan data pribadi, sedangkan KUHPperdata menyediakan konstruksi pertanggungjawaban dan pemulihan melalui gugatan wanprestasi serta perbuatan melawan hukum. Gugatan wanprestasi dapat digunakan ketika kewajiban perlindungan data merupakan bagian dari hubungan kontraktual antara subjek data dan pengendali data, termasuk kewajiban menjaga keamanan dan kerahasiaan data dalam perjanjian elektronik. Sementara itu, perbuatan melawan hukum dapat menjadi dasar pertanggungjawaban ketika kebocoran data melanggar hak subjek data atau kewajiban hukum pengendali data, termasuk dalam keadaan

tidak terdapat hubungan kontraktual secara langsung. Namun, penerapan model pertanggungjawaban yang bertumpu pada pembuktian kesalahan masih menghadapi kendala akibat adanya asimetri informasi dan kompleksitas teknologi dalam pembuktian kebocoran data.

Ketiga, perkembangan transaksi digital, kecerdasan buatan, *data broker*, transfer data lintas negara, serta meningkatnya kebocoran data berskala besar menunjukkan perlunya pengembangan model pertanggungjawaban perdata yang lebih adaptif. Sebagai nilai kebaruan penelitian, ditawarkan model pertanggungjawaban perdata berbasis risiko (*risk-based civil liability*) yang mengintegrasikan pertanggungjawaban kontraktual, perbuatan melawan hukum, dan penerapan praduga tanggung jawab (*presumption of liability*) terhadap pengendali data sebagai pihak yang memiliki kendali atas pemrosesan dan keamanan data. Model tersebut menempatkan pengendali data pada posisi untuk membuktikan bahwa kewajiban perlindungan dan keamanan data telah dilaksanakan secara patut, sehingga tidak seluruh beban pembuktian dibebankan kepada korban. Rekonstruksi ini diharapkan dapat memperkuat kepastian hukum, efektivitas pemulihan kerugian, dan perlindungan hak subjek data sekaligus mendorong akuntabilitas pengendali data dalam menghadapi perkembangan ekosistem digital.

DAFTAR PUSTAKA

Buku

- Agustina, Rosa. *Perbuatan Melawan Hukum*. Jakarta: Pascasarjana Fakultas Hukum Universitas Indonesia, 2003.
- Ibrahim, Johnny. *Teori dan Metodologi Penelitian Hukum Normatif*. Malang: Bayumedia Publishing, 2006.
- Lynskey, Orla. *The Foundations of EU Data Protection Law*. Oxford: Oxford University Press, 2015.
- Manan, Bagir. *Asas-Asas Perundang-undangan Indonesia*. Jakarta: FH UII Press, 2006.
- Marzuki, Peter Mahmud. *Penelitian Hukum*. Edisi Revisi. Jakarta: Kencana Prenada Media Group, 2021.
- OECD. *The OECD Privacy Framework*. Paris: OECD Publishing, 2013.
- Soekanto, Soerjono, dan Sri Mamudji. *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: RajaGrafindo Persada, 2015.
- Solove, Daniel J. *Understanding Privacy*. Cambridge: Harvard University Press, 2008.
- Subekti, R. *Hukum Perjanjian*. Jakarta: Intermasa, 2014.

Jurnal

- Goenawan, Daniel Johnson, et al. "PMH di Era Digital: Pertanggungjawaban Perdata atas Penyalahgunaan Data Pribadi". *Al-Zayn: Jurnal Ilmu Sosial & Hukum Vol. 4, No. 1* (Januari 2026): 205–213.
- Hotima, Desi Patul, dan Diki Zukriadi. "Tanggung Jawab Hukum Perdata atas Penggunaan Citra Publik Figur dalam Foto Buatan AI". *Al-Muamalat: Jurnal Ilmu Hukum & Ekonomi Syariah, Vol. 11, No. 1* (Januari–Juni 2026): 93–105.
- Hukom, Suratman, et al. "The Urgency of Legal Regulation for Personal Data Protection in Indonesia in the Big Data Era". *Hakim: Jurnal Ilmu Hukum Dan Sosial, Vol. 3, No. 1* (Februari 2025): 974–992.
- Khansa, Farah Naurah. "Penguatan Hukum Dan Urgensi Otoritas Pengawas Independen Perlindungan Data Pribadi". *Rewang Rencang: Jurnal Hukum Lex Generalis, Vol. 2, No. 8* (Agustus 2021): 18–22.
- Lutfi, Melinda Putri, et al. "Urgensi Perlindungan Hukum Terhadap Data Privasi Nasabah Bank Di Era Perkembangan Digital". *Jurnal Multidisiplin Ilmu Akademik, Vol. 1, No. 5* (Oktober 2024): 210–218.
- Yance, Tri Vebri, et al. "Perlindungan Data Pribadi dalam Teknologi AI: Analisis Peran Hukum dan Kepatuhan Regulasi Bisnis Digital". *Jurnal Ilmu Hukum, Vol. 14, No. 2* (Agustus 2025): 191–207.