

TANGGUNG JAWAB PERDATA INSTANSI PEMERINTAH SEBAGAI PENGENDALI DATA DALAM KASUS KEBOCORAN DATA PRIBADI WARGA NEGARA

Yossy Mulyani¹, Muhammad Adrian Perdana²

Politeknik Pengadaan Nasional, Pekanbaru

e-mail: ¹ yossymulyani20@gmail.com

Abstract: *The rapid advancement of digital technology has placed the government in the position of a large-scale personal data controller through various E-Government platforms and public service applications. However, the government's capacity to protect this data has proven inadequate, as demonstrated by several major data breach incidents involving national platforms such as the Temporary National Data Center (PDNS) in 2024, Satu Sehat, and DPMPTSP Online. This research aims to analyze the civil liability of government agencies as personal data controllers in cases of personal data breaches, viewed through the framework of Law Number 27 of 2022 on Personal Data Protection (UU PDP) and Law Number 30 of 2014 on Government Administration (UU AP). The research method employed is normative juridical (doctrinal legal research) through a statutory approach and a conceptual approach, with primary legal materials drawn from the aforementioned laws and secondary materials from scientific articles and relevant legal textbooks. The findings indicate that the government, as a public body and personal data controller under UU PDP, can be held civilly liable when a data breach occurs due to negligence or unlawful acts in data management. Civil liability may arise through two mechanisms: the unlawful act (onrechtmatige overheidsdaad) mechanism under Article 1365 of the Civil Code, and the administrative court (PTUN) mechanism under UU AP. However, implementation faces significant obstacles, including the absence of government implementing regulations for UU PDP, fragmentation of supervisory authority, the absence of standardized compensation mechanisms, and limited institutional capacity. This research concludes that comprehensive regulatory harmonization, the establishment of a strong Personal Data Protection Authority, and the development of fast, accessible compensation procedures are urgently needed to realize effective legal protection for citizens' personal data.*

Keywords: *Civil Liability; Government; Personal Data Controller; Data Breach; UU PDP; Government Administration Law.*

Abstrak: Kemajuan teknologi digital yang pesat menempatkan pemerintah pada posisi sebagai pengendali data pribadi dalam skala besar melalui berbagai platform E-Government dan aplikasi pelayanan publik. Namun, kapasitas pemerintah dalam menjaga keamanan data tersebut terbukti belum memadai, sebagaimana tercermin dari berbagai insiden kebocoran data besar yang melibatkan platform nasional seperti Pusat Data Nasional Sementara (PDNS) tahun 2024, Satu Sehat, dan DPMPTSP Online. Penelitian ini bertujuan untuk menganalisis tanggung jawab perdata instansi pemerintah sebagai pengendali data pribadi dalam kasus kebocoran data pribadi warga negara, ditinjau dari kerangka Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan (UU AP). Metode penelitian yang digunakan adalah yuridis normatif (doctrinal legal research) melalui pendekatan perundang-undangan dan pendekatan konseptual, dengan bahan hukum primer berupa undang-undang terkait dan bahan hukum sekunder berupa artikel ilmiah dan buku hukum yang relevan. Hasil penelitian menunjukkan bahwa pemerintah sebagai badan publik dan pengendali data pribadi berdasarkan UU PDP dapat dimintai pertanggungjawaban perdata apabila terjadi kebocoran data akibat kelalaian atau

perbuatan melanggar hukum dalam pengelolaan data. Pertanggungjawaban perdata dapat ditempuh melalui dua mekanisme, yakni mekanisme perbuatan melanggar hukum (onrechtmatige overheidsdaad) berdasarkan Pasal 1365 KUHPerdata, maupun mekanisme peradilan administrasi melalui PTUN berdasarkan UU AP. Namun implementasinya menghadapi hambatan signifikan, di antaranya belum terbitnya peraturan pemerintah pelaksana UU PDP, fragmentasi kewenangan pengawasan, ketiadaan mekanisme kompensasi yang terstandarisasi, dan keterbatasan kapasitas kelembagaan. Penelitian ini menyimpulkan bahwa harmonisasi regulasi yang komprehensif, pembentukan Otoritas Pelindungan Data Pribadi yang kuat, dan pengembangan prosedur ganti rugi yang cepat dan mudah diakses sangat mendesak untuk diwujudkan demi perlindungan hukum yang efektif atas data pribadi warga negara.

Kata kunci: Tanggung Jawab Perdata; Pemerintah; Pengendali Data Pribadi; Kebocoran Data; UU PDP; Hukum Administrasi Pemerintahan.

PENDAHULUAN

Era transformasi digital telah mendorong pemerintah Indonesia untuk mengadopsi berbagai platform E-Government sebagai instrumen utama pelayanan publik. Platform-platform seperti Satu Sehat yang mengintegrasikan data rekam medis nasional, DPMPTSP Online yang mengelola data perizinan berusaha, hingga Pusat Data Nasional Sementara (PDNS) yang menampung data dari ratusan instansi pemerintah, merepresentasikan babak baru dalam tata kelola pemerintahan yang berbasis digital.

Dalam konteks ini, pemerintah tidak lagi sekadar penyedia layanan konvensional, melainkan telah bertransformasi menjadi pengendali data pribadi (data controller) dalam skala masif yang menyimpan jutaan rekam data sensitif warga negara. Urgensi penelitian ini diperkuat oleh fakta empiris yang mencengangkan.

Databoks mencatat bahwa pada kuartal III tahun 2022, Indonesia menduduki peringkat ketiga dunia sebagai negara dengan akumulasi kasus kebocoran data terbanyak, dengan total 12.742.031 data akun yang bocor. Puncak krisis terjadi pada 20 Juni 2024, ketika PDNS yang dikelola Kementerian Komunikasi dan Informatika (Kominfo) lumpuh akibat serangan ransomware varian LockBit 3.0 yang dikenal sebagai Brain Cipher. Serangan ini berdampak

pada 282 instansi pemerintah pusat dan daerah, dengan 239 instansi mengalami gangguan layanan publik tanpa cadangan data. Direktur Jenderal Aplikasi Informatika Kominfo, Samuel Abrijani Pangerapan, mengonfirmasi bahwa data dari 210 instansi pemerintahan pusat dan daerah ikut terdampak, termasuk layanan keimigrasian di seluruh bandara internasional Indonesia. Pelaku meminta tebusan sebesar USD 8 juta, sementara data Inafis POLRI ditawarkan di forum gelap dengan harga USD 1.000 hingga 7.000.

Sebelumnya, insiden kebocoran data pada platform Satu Sehat pada akhir 2023 juga membuka luka yang sama. Data sensitif kesehatan masyarakat, termasuk riwayat vaksinasi dan informasi medis, diduga terekspos akibat kerentanan sistem keamanan. Demikian pula, DPMPTSP Online di berbagai daerah menghadapi kerentanan sistemik, di mana banyak pemerintah daerah belum memiliki infrastruktur teknologi informasi yang memadai untuk menjamin keamanan data dalam sistem OSS. Rangkaian insiden ini tidak hanya menimbulkan kerugian finansial yang diperkirakan menyentuh miliaran rupiah, tetapi juga mengikis kepercayaan publik terhadap kapabilitas negara dalam melindungi data warganya.

Kehadiran Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) semestinya menjadi

fondasi kokoh bagi pertanggungjawaban negara. Undang-undang ini secara eksplisit menempatkan badan publik sebagai pengendali data pribadi yang bertanggung jawab penuh atas pemrosesan dan keamanan data yang dikelolanya. Namun, realitas di lapangan menunjukkan bahwa implementasi UU PDP masih jauh dari ideal. Peraturan pemerintah pelaksana yang diamanatkan oleh setidaknya 10 pasal dalam UU PDP belum kunjung terbit, lembaga pengawas independen (Otoritas Pelindungan Data Pribadi/OPDP) masih belum beroperasi optimal, dan mekanisme ganti rugi bagi korban kebocoran data masih kabur secara prosedural.

Pertanyaan mendasar yang muncul adalah: sejauh mana instansi pemerintah dapat dimintai pertanggungjawaban perdata atas insiden kebocoran data yang menimpa warga negara? Apakah kerangka hukum yang tersedia, yakni UU PDP dan Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan (UU AP), telah memadai untuk merealisasikan pertanggungjawaban tersebut secara efektif? Penelitian ini berupaya menjawab pertanyaan-pertanyaan tersebut melalui analisis yuridis normatif yang komprehensif, dengan harapan dapat memberikan kontribusi pemikiran bagi penguatan perlindungan hukum data pribadi di Indonesia.

METODE

Penelitian ini menggunakan metode penelitian hukum normatif atau yang lazim disebut *doctrinal legal research*. Pilihan metode ini didasarkan pada fokus kajian yang tertuju pada analisis norma-norma hukum positif, asas-asas hukum, dan prinsip-prinsip hukum administrasi yang berkaitan dengan pertanggungjawaban perdata pemerintah dalam kasus kebocoran data pribadi.

Sumber bahan hukum dalam penelitian ini diklasifikasikan menjadi dua kategori. Bahan hukum primer meliputi: Undang-

Undang Dasar Negara Republik Indonesia Tahun 1945, Kitab Undang-Undang Hukum Perdata (KUHPerdata) khususnya Pasal 1365 tentang perbuatan melawan hukum, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan (UU AP), Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (UU KIP), Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE), serta Undang-Undang Nomor 23 Tahun 2006 jo.

Undang-Undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan (UU Admuduk). Adapun bahan hukum sekunder terdiri dari artikel-artikel ilmiah yang dipublikasikan di jurnal hukum bereputasi, buku-buku teks hukum administrasi dan hukum perdata, Naskah Akademik RUU PDP, serta laporan-laporan investigasi dari lembaga terkait. Pendekatan yang digunakan dalam penelitian ini meliputi dua pendekatan utama. Pertama, pendekatan perundang-undangan (*statute approach*), yakni menelaah secara menyeluruh berbagai peraturan hukum yang relevan untuk memperoleh pemahaman komprehensif mengenai kerangka pertanggungjawaban perdata pemerintah sebagai pengendali data.

Kedua, pendekatan konseptual (*conceptual approach*), yang digunakan untuk mengeksplorasi dan mengembangkan konsep-konsep teoritis seperti konsep tanggung gugat pemerintah (*governmental liability*), doktrin perbuatan melanggar hukum oleh penguasa (*onrechtmatige overheidsdaad*), dan teori perlindungan hukum preventif-represif.

Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*), yaitu dengan mengumpulkan, membaca, mengklasifikasikan, dan menganalisis

bahan-bahan hukum yang relevan secara sistematis.

HASIL DAN PEMBAHASAN

Kedudukan Instansi Pemerintah sebagai Pengendali Data Pribadi

Kedudukan hukum instansi pemerintah sebagai pengendali data pribadi. Pasal 1 ayat (4) UU PDP mendefinisikan Pengendali Data Pribadi sebagai "setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri atau bersama-sama dalam menentukan tujuan dan melakukan pengendalian terhadap pemrosesan Data Pribadi." Definisi ini secara eksplisit memasukkan badan publik, termasuk instansi pemerintah, sebagai salah satu kategori pengendali data pribadi.

Lebih lanjut, Pasal 1 ayat (4) UU PDP juga menegaskan bahwa badan publik, sebagaimana diatur dalam UU Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, mencakup lembaga eksekutif, legislatif, yudikatif, dan lembaga lainnya yang dananya bersumber dari APBN/APBD. Dalam konteks ini, Kominfo sebagai pengelola PDNS, Kementerian Kesehatan sebagai pengelola Satu Sehat, serta Badan Koordinasi Penanaman Modal (BKPM) sebagai pengelola sistem OSS yang menjadi tulang punggung DPMPTSP Online, semuanya secara tidak terbantahkan berkedudukan sebagai pengendali data pribadi dalam pengertian UU PDP.

Sebagai pengendali data pribadi, instansi pemerintah mengemban serangkaian kewajiban hukum yang bersifat imperatif. Berdasarkan UU PDP, setidaknya terdapat tiga kelompok kewajiban utama. Pertama, kewajiban menjaga keamanan data (Pasal 35 UU PDP), yang mengharuskan instansi pemerintah untuk menerapkan langkah-langkah teknis (seperti enkripsi, autentikasi berlapis, firewall, dan sistem deteksi intrusi) maupun administratif (seperti SOP pengelolaan data, audit berkala, dan pelatihan aparatur) guna

mencegah akses tidak sah. Ironi muncul dalam kasus PDNS 2024, di mana server yang menyimpan data jutaan warga negara diketahui menggunakan kata sandi lemah berupa "Admin#1234", dan sistem tersebut tidak memenuhi persyaratan sertifikasi ISO 22301 untuk kelangsungan bisnis. Kedua, kewajiban transparansi dan notifikasi insiden (Pasal 46 UU PDP), yang mewajibkan pengendali data untuk memberitahukan kepada subjek data pribadi dan lembaga pengawas paling lambat 3x24 jam setelah mengetahui terjadinya kegagalan perlindungan data. Ketiga, kewajiban memastikan akurasi dan legalitas pemrosesan data (Pasal 20 dan Pasal 27-29 UU PDP), yang mewajibkan instansi pemerintah untuk memiliki dasar hukum yang sah dalam setiap pemrosesan data yang dilakukannya.

Kurangnya Kominfo dalam memenuhi kewajiban-kewajiban tersebut dalam kasus PDNS 2024, khususnya lemahnya sistem keamanan, kurangnya transparansi publik, dan lambatnya penanganan insiden, secara normatif merupakan bentuk wanprestasi terhadap kewajiban hukum yang dibebankan UU PDP. Kondisi serupa juga terjadi dalam kasus Satu Sehat, di mana meskipun Kementerian Kesehatan mengklaim telah melakukan investigasi internal, publik tidak mendapatkan akses terhadap hasil investigasi tersebut secara transparan, sehingga bertentangan dengan kewajiban transparansi yang diamanatkan undang-undang.

Tanggung Jawab Perdata Pemerintah dalam Kebocoran Data Pribadi

Pertanggungjawaban perdata pemerintah atas kebocoran data pribadi dapat dianalisis melalui dua pilar hukum utama yang saling melengkapi. Pilar pertama adalah doktrin Perbuatan Melanggar Hukum oleh Penguasa (*onrechtmatige overheidshandeling/OOD*). Doktrin ini berakar pada Pasal 1365 KUHPerdata yang mengatur bahwa setiap perbuatan melanggar hukum yang menimbulkan kerugian bagi orang lain

mewajibkan pelakunya untuk mengganti kerugian tersebut. Dalam konteks hukum publik, pemerintah dapat dinyatakan melakukan OOD apabila: (1) tindakan atau kelalaiannya melanggar peraturan perundang-undangan yang berlaku; (2) melanggar hak-hak subjektif warga negara; (3) tidak melakukan sesuatu yang menjadi kewajiban hukumnya; atau (4) tidak bertindak cermat dan hati-hati dalam menjalankan fungsinya, sebagaimana dikembangkan melalui yurisprudensi arrest Hoge Raad tahun 1919. Dikemukakan oleh Philipus M. Hadjon bahwa tanggung gugat pemerintah di Indonesia dibedakan menjadi dua bentuk: tanggung gugat akibat keputusan pemerintah yang tidak sesuai hukum, dan tanggung gugat akibat perbuatan melanggar hukum oleh pemerintah.

Penerapan doktrin OOD dalam kasus kebocoran PDNS 2024 dapat diargumentasikan sebagai berikut. Kominfo, sebagai pengendali data, terbukti melanggar ketentuan Pasal 35 UU PDP dengan membiarkan sistem keamanan PDNS beroperasi jauh di bawah standar yang dipersyaratkan. Penggunaan kata sandi "Admin#1234" dan ketiadaan sertifikasi ISO 22301 merupakan bukti nyata dari kelalaian administratif yang melampaui batas toleransi standar pengelolaan data nasional. Kelalaian ini secara kausal mengakibatkan kerugian nyata bagi 282 instansi pemerintah dan jutaan warga negara yang datanya terekspos. Untuk berhasilnya gugatan ganti rugi berdasarkan OOD, pemohon perlu membuktikan lima unsur: (a) adanya perbuatan/kelalaian pemerintah; (b) sifat melawan hukum dari perbuatan tersebut; (c) adanya kesalahan pejabat atau sistem; (d) adanya kerugian yang diderita korban; dan (e) hubungan kausal (causaal verband) antara kelalaian dan kerugian. Dalam kasus kebocoran PDNS, kelima unsur ini secara substansial dapat dipenuhi.

Pilar kedua adalah mekanisme pertanggungjawaban melalui Peradilan Tata Usaha Negara (PTUN) berdasarkan

UU AP. Pasal 69 UU AP mengatur bahwa setiap keputusan dan/atau tindakan administrasi pemerintahan yang melanggar hukum dan/atau melampaui wewenang dapat dibatalkan atau dinyatakan tidak sah. Lebih lanjut, warga negara yang merasa dirugikan oleh tindakan atau kelalaian pemerintah dapat mengajukan gugatan ke PTUN dengan menyertakan tuntutan agar pemerintah melaksanakan kegiatan tertentu, menghentikan perbuatan tertentu, dan/atau membayar ganti rugi. Mekanisme ini telah dipraktikkan oleh Perhimpunan Bantuan Hukum Indonesia (PBHI) yang mengajukan gugatan ke PTUN Jakarta terkait kebocoran data PeduliLindungi yang merupakan pendahulu Satu Sehat, meskipun prosesnya masih berlangsung.

Selain kedua pilar utama tersebut, UU PDP sendiri dalam Pasal 12 secara eksplisit mengakui hak subjek data pribadi untuk melakukan penggugatan dan mendapatkan ganti rugi atas pelanggaran dalam pemrosesan data pribadi yang mereka miliki. Hak ini diperkuat oleh ketentuan sanksi administratif dalam Pasal 57 UU PDP dan sanksi pidana dalam Pasal 67, yang memberikan efek deterren bagi pengendali data yang lalai. Dalam UU Adminduk, Pasal 2 juga secara tegas memberikan hak kepada setiap penduduk untuk memperoleh perlindungan dari instansi pelaksana yang menyalahgunakan data pribadi, termasuk hak untuk memperoleh ganti kerugian.

Konsep tanggung gugat pemerintah juga dapat dipilah melalui ajaran kesalahan dalam hukum administrasi, yakni antara *faute de personelles* (kesalahan pribadi pejabat) dan *faute de services* (kesalahan jabatan). Dalam kasus kebocoran PDNS, di mana kelemahan keamanan bersifat sistemik dan merupakan hasil dari kebijakan pengelolaan yang buruk secara institusional, maka tanggung gugat lebih tepat dikualifikasikan sebagai *faute de services*. Konsekuensinya, ganti rugi yang diperintahkan pengadilan dibebankan

kepada negara, bukan kepada pejabat secara pribadi.

Hambatan Implementasi dan Rekomendasi Penguatan Pertanggungjawaban Perdata

Meskipun kerangka hukum pertanggungjawaban perdata pemerintah atas kebocoran data pribadi telah tersedia secara normatif, implementasinya di lapangan masih menghadapi hambatan struktural yang serius. Berdasarkan analisis terhadap kasus PDNS 2024, Satu Sehat, dan DPMPTSP Online, setidaknya terdapat empat hambatan utama yang perlu diidentifikasi.

Hambatan pertama adalah kekosongan peraturan pelaksana. UU PDP mengamankan pembentukan peraturan pemerintah untuk mengatur lebih lanjut setidaknya 10 aspek teknis, mulai dari standar keamanan data, mekanisme notifikasi insiden, hingga tata cara pengajuan ganti rugi. Namun, hingga penelitian ini ditulis, peraturan-peraturan pemerintah tersebut belum seluruhnya terbit. Akibatnya, ketentuan-ketentuan dalam UU PDP yang bersifat umum dan belum dapat diterapkan secara teknis menciptakan ketidakpastian hukum bagi para penegak hukum, lembaga pengawas, dan masyarakat yang ingin menuntut hak-haknya. Kondisi ini sejalan dengan temuan dalam penelitian Nabiha Khansa Rusyda yang menegaskan pentingnya pembentukan peraturan pelaksana guna menjamin efektivitas perlindungan data pribadi di Indonesia.

Hambatan kedua adalah fragmentasi kewenangan pengawasan. Kewenangan pengawasan dan penegakan hukum atas kebocoran data tersebar di beberapa instansi sekaligus: OPDP sebagai regulator utama, BSSN sebagai otoritas keamanan siber, Ombudsman untuk aspek maladministrasi, inspektorat internal masing-masing kementerian, dan PTUN untuk penyelesaian sengketa administrasi. Fragmentasi ini secara potensial menciptakan tumpang-tindih kewenangan atau bahkan vakum penanganan, sebagaimana terlihat dalam

insiden awal kebocoran data PeduliLindungi di mana tidak jelas lembaga mana yang berwenang melakukan investigasi komprehensif. Hasil survei SAFEnet (2024) menunjukkan bahwa 68% pengguna layanan digital pemerintah tidak memahami hak privasi mereka, dan hanya 12% yang memahami mekanisme pengaduan apabila terjadi kebocoran data, yang mengindikasikan rendahnya aksesibilitas mekanisme pertanggungjawaban bagi masyarakat umum.

Hambatan ketiga adalah ketiadaan standar kompensasi yang terukur. Tidak adanya standar nasional mengenai besaran ganti rugi untuk kebocoran data menciptakan ketidakpastian yang serius bagi korban. Dalam konteks perdata, korban kebocoran data seringkali kesulitan membuktikan kerugian yang bersifat imaterial, seperti risiko penyalahgunaan identitas di masa depan, trauma psikologis akibat tereksposnya data sensitif, atau kerugian kompetitif akibat bocornya rahasia bisnis dalam sistem DPMPTSP Online.

Berbeda dengan negara-negara yang telah maju dalam regulasi perlindungan data, seperti Jerman yang menerapkan standar *due diligence* yang proporsional untuk pertanggungjawaban instansi publik, atau Inggris yang memiliki pedoman perhitungan ganti rugi dari Information Commissioner's Office (ICO) berdasarkan jenis dan sensitivitas data yang bocor, Indonesia belum memiliki panduan serupa. Studi komparatif oleh Sembiring (2024) menunjukkan bahwa Indonesia perlu mengadopsi pendekatan yang lebih terstruktur dalam menentukan besaran kompensasi untuk korban kebocoran data.

Hambatan keempat adalah kompleksitas prosedural yang tidak ramah korban. Mekanisme gugatan melalui PTUN maupun pengadilan perdata memerlukan biaya, waktu, dan pemahaman hukum yang tidak sedikit. Hal ini mengakibatkan ketidakseimbangan posisi antara warga negara

individual sebagai korban dan negara sebagai tergugat yang memiliki sumber daya hukum tak terbatas. Kondisi ini bertentangan dengan prinsip access to justice sebagai elemen krusial dari asas kepastian hukum dalam negara hukum.

Menghadapi rangkaian hambatan tersebut, penelitian ini merumuskan beberapa rekomendasi kebijakan. Pertama, pemerintah perlu segera menerbitkan seluruh peraturan pemerintah pelaksana UU PDP, khususnya yang mengatur mekanisme ganti rugi, standar keamanan teknis wajib, dan prosedur notifikasi insiden yang terperinci. Kedua, perlu dilakukan harmonisasi regulasi untuk mengatasi fragmentasi kewenangan, dengan menempatkan OPDP sebagai koordinator tunggal yang memiliki otoritas mengikat atas seluruh instansi terkait.

Ketiga, perlu dikembangkan mekanisme kompensasi administratif yang cepat dan terstandarisasi, yang memungkinkan korban kebocoran data mengakses pemulihan hak tanpa harus menempuh jalur litigasi yang panjang dan mahal. Keempat, kapasitas keamanan siber seluruh instansi pemerintah perlu ditingkatkan secara sistematis melalui audit keamanan data yang rutin dan mengikat, mengingat hasil studi Pusat Studi Hukum dan Teknologi Universitas Indonesia (2024) menemukan bahwa hanya 30% instansi pemerintah pusat yang secara rutin melakukan audit keamanan data mandiri. Kelima, program literasi digital dan hukum perlu digalakkan agar warga negara memahami hak-hak mereka sebagai subjek data dan mekanisme hukum yang tersedia apabila hak-hak tersebut dilanggar.

Secara keseluruhan, penelitian ini menegaskan bahwa pertanggungjawaban perdata pemerintah dalam kasus kebocoran data pribadi bukanlah sekadar kemungkinan teoritis, melainkan telah memiliki landasan hukum yang konkret dalam hukum positif Indonesia. Tantangan terbesar kini terletak bukan pada aspek normatif, melainkan pada aspek implementasi yang membutuhkan

political will pemerintah, kapasitas kelembagaan yang memadai, dan aksesibilitas mekanisme hukum bagi seluruh lapisan masyarakat.

SIMPULAN

Penelitian ini menyimpulkan bahwa instansi pemerintah, dalam kedudukannya sebagai pengendali data pribadi berdasarkan UU PDP, dapat dimintai pertanggungjawaban perdata apabila terjadi kebocoran data pribadi warga negara akibat kelalaian atau perbuatan melanggar hukum dalam pengelolaan data. Pertanggungjawaban tersebut dapat ditempuh melalui dua mekanisme hukum: mekanisme OOD berdasarkan Pasal 1365 KUHPerdata dan mekanisme peradilan administrasi melalui PTUN berdasarkan UU AP. Meskipun kerangka hukum normatifnya telah tersedia, implementasi pertanggungjawaban perdata tersebut masih menghadapi empat hambatan struktural utama, yaitu kekosongan peraturan pelaksana UU PDP, fragmentasi kewenangan pengawasan antar-lembaga, ketiadaan standar kompensasi yang terukur, dan kompleksitas prosedural yang tidak ramah korban. Oleh karena itu, penerbitan peraturan pemerintah pelaksana UU PDP, penguatan OPDP sebagai koordinator pengawasan tunggal, pengembangan mekanisme kompensasi yang cepat dan terstandarisasi, peningkatan kapasitas keamanan siber instansi pemerintah, serta pemasyarakatan literasi digital-hukum merupakan langkah-langkah mendesak yang tidak dapat ditunda.

DAFTAR PUSTAKA

- Al Farichi, V. (2025). Analisis Tanggung Gugat Pemerintah Dalam Perlindungan Data Pribadi Pada Aplikasi Kesehatan Berbasis Digital. *Future Academia: The Journal of Multidisciplinary Research on Scientific and Advanced*, 3(1), 388-

396. DOI: <https://doi.org/10.61579/future.v3i1.430>
- Asshiddiqie, J. (2010). *Perihal Undang-Undang*. Jakarta: Rajawali Pers.
- Attamimi, A. H. S. (1990). *Peranan Keputusan Presiden Republik Indonesia dalam Penyelenggaraan Pemerintahan Negara*. Disertasi. Depok: Universitas Indonesia.
- Bayu Satrio, M., & Widiatno, M. W. (2020). Perlindungan hukum terhadap data pribadi dalam media elektronik (analisis kasus kebocoran data pengguna Facebook di Indonesia). *Journal Civitas Academica of Law Esa Unggul University*, 1(1).
- Djafar, W. (2019). *Hukum perlindungan data pribadi di Indonesia: Lanskap, urgensi dan kebutuhan pembaruan*. Dalam *Seminar Hukum dalam Era Analisis Big Data*, Program Pascasarjana Fakultas Hukum UGM, Vol. 26.
- Ganarsih, Y. (2023). *Aspek Hukum Perlindungan Data Pribadi di Indonesia (Cetakan Kedua)*. Jakarta: Kencana.
- Hadjon, P. M., dkk. (2020). *Pengantar Hukum Administrasi Indonesia (Edisi Revisi)*. Yogyakarta: Gadjah Mada University Press.
- Information Commissioner's Office (ICO) United Kingdom. (2023). *Guide to Data Protection: Compensation and Liability (2023 Edition)*. Diakses dari <https://ico.org.uk/for-organisations/guide-to-data-protection/>
- Kusnadi, S. A., & Wijaya, A. U. (2021). Perlindungan hukum data pribadi sebagai hak privasi. *Jurnal Al Wasath*, 2(1). DOI: <https://doi.org/10.47776/alwasath.v2i1.127>
- Makarim, E. (2024). *Perlindungan Data Pribadi: Teori & Praktik Implementasi UU PDP*. Jakarta: Prenadamedia Group.
- Mamonto, D. F. (2022). *Analisis perlindungan hukum terhadap penyalahgunaan data pribadi berdasarkan Undang-Undang Nomor 27 Tahun 2022*. E-Journal UNSTRAT.
- Maulana, R., dkk. (2024). Analisis Kerentanan Keamanan Sistem OSS pada Pemerintah Daerah. *Jurnal Administrasi Publik*, 15(2), 45-60.
- Naskah Akademik Rancangan Undang-Undang Pelindungan Data Pribadi (RUU PDP).
- Philipus, M. H. (2007). *Perlindungan Hukum Bagi Rakyat di Indonesia (Edisi Khusus, Cetakan Pertama)*. Peradaban.
- Pusat Studi Hukum dan Teknologi FHUI. (2024). *Audit Keamanan Data pada Instansi Pemerintah: Temuan dan Rekomendasi (Policy Brief No. 03/2024)*. Depok: Universitas Indonesia.
- Ridwan HR. (2022). *Hukum Administrasi Negara (Edisi Revisi)*. Jakarta: Rajawali Pers.
- Rosadi, S. D. (2022). *Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional*. Refika Aditama.
- Rusyda, N. K. (2025). Perlindungan Hukum terhadap Subjek Data Kebocoran Data oleh Badan Publik Menurut UU Nomor 27 Tahun 2022. *Desentralisasi: Jurnal Hukum, Kebijakan Publik, dan Pemerintahan*, 2(3), 247-262. DOI: <https://doi.org/10.62383/desentralisasi.v2i3.940>
- Sembiring, S. (2024). Comparative Analysis of State Liability for Data Breaches: Lessons from the EU GDPR. *Indonesian Journal of International Law*, 21(1), 89-112.
- Southeast Asia Freedom of Expression Network (SAFEnet). (2024). *Laporan Kesadaran Keamanan Digital Masyarakat Indonesia 2024*. Jakarta: SAFEnet.
- Suhaila, S., dkk. (2026). *Pertanggungjawaban Negara dalam Kebocoran Data pada Platform E-Government: Analisis Hukum Administrasi atas Kasus Satu Sehat*

-
- dan DPMPTSP Online. Jurnal Ilmiah Research Student (JIRS), 3(1), 578-587. DOI: <https://doi.org/10.61722/jirs.v3i1.878>
- Utrecht, E. (1986). Rangkaian Sari Kuliah Hukum Administrasi Negara. Surabaya: Pustaka Tinta Mas.
- Wijaya, C. (2024). Perlindungan Hukum Data Usaha dalam Sistem Perizinan Online. Jurnal Hukum Bisnis, 42(3), 78-85.
- Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
- Kitab Undang-Undang Hukum Perdata (KUHPerdata), khususnya Pasal 1365 tentang Perbuatan Melawan Hukum.
- Undang-Undang Nomor 23 Tahun 2006 jo. Undang-Undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan.
- Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.
- Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik.
- Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan.
- Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
- Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.
- Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis Elektronik.
- Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2023 tentang Standar Keamanan Informasi untuk Penyelenggara Sistem Elektronik Pemerintah.