KAMPUS AKADEMIK PUBLISING
Jurnal Ilmiah Penelitian Mahasiswa (JIPM)
Vol.4, No.2 April 2026
e-ISSN: 3025-5465, p-ISSN : 3025-7964, Hal 12-21
DOI : https://doi.org/10.61722/jipm.v4i2.2166

PERTANGGUNGJAWABAN NEGARA DALAM KEBOCORAN DATA PADA PLATFORM E-GOVERNMENT: ANALISIS HUKUM ADMINISTRASI ATAS KASUS SATU SEHAT DAN DPMPTSP ONLINE

Shafa Suhaila
Universitas Al-Azhar Medan
Mutiara Andini
Universitas Al-Azhar Medan
Oriza Satifa Wahyuni
Universitas Al-Azhar Medan
M. Daris Alfi Putra Nurhadi
Universitas Al-Azhar Medan
Muhammad Sahriadi Lubis
Universitas Al-Azhar Medan
Alamat: Jl. Marelan Raya, Tanah Enam Ratus, Medan Marelan, Kota Medan, Sumatera Utara 20245, Indonesia
Penulis Korespondensi: shafasuhaila508@gmail.com

Abstract. *Data breaches on digital public service platforms represent a critical phenomenon that tests the commitment of a constitutional state. This study analyzes state accountability under administrative law regarding data breach incidents on E-Government platforms, using case studies of Satu Sehat and DPMPTSP Online. The research employs a normative juridical method through case study and document analysis approaches. The findings indicate that although the legal framework for state accountability has been established under the Personal Data Protection Law (UU PDP) and its implementing regulations, its implementation has not fully realized the principle of legal certainty. The state's responsibility as the data controller remains hindered by regulatory disparities, limited cybersecurity capacity, and incident response mechanisms that are slow and lack transparency. Forms of accountability that should be procedural and predictable such as the obligation of 72-hour notification, proportional administrative sanctions, and civil lawsuit mechanisms through the State Administrative Court (PTUN) are still not optimal in practice. This study concludes that strengthening state accountability requires regulatory harmonization, enhanced institutional capacity of the Personal Data Protection Authority (OPDP) and the National Cyber and Crypto Agency (BSSN), and standardized incident response protocols. Policy recommendations are directed toward reinforcing state accountability in protecting citizens' personal data in the digital sphere.*

Keywords: *State Accountability; Data Breach; E-Government; Administrative Law; Legal Certainty; PDP Law; Satu Sehat; DPMPTSP.*

Abstrak. Kebocoran data pada platform pelayanan publik digital merupakan fenomena kritis yang menguji komitmen negara hukum. Penelitian ini menganalisis pertanggungjawaban negara secara hukum administrasi atas insiden kebocoran data di platform E-Government, dengan studi kasus pada Satu Sehat dan DPMPTSP Online. Metode penelitian yang digunakan adalah yuridis normatif melalui pendekatan studi kasus dan analisis dokumen. Hasil penelitian menunjukkan bahwa meskipun kerangka hukum pertanggungjawaban negara telah ditegaskan dalam Undang-Undang Perlindungan Data Pribadi (UU PDP) dan peraturan turunannya, implementasinya belum sepenuhnya merealisasikan asas kepastian hukum. Tanggung jawab negara sebagai pengendali data (data controller) masih terhambat oleh disparitas regulasi, kapasitas keamanan siber yang terbatas, serta mekanisme penanganan insiden yang lambat dan kurang transparan. Bentuk pertanggungjawaban yang seharusnya bersifat prosedural dan prediktif seperti

Naskah Masuk: 30 Desember 2025; Revisi: 01 Januari 2026; Diterima: 06 Februari 2026; ; Terbit: 06 Februari 2026

kewajiban notifikasi 72 jam, sanksi administratif proporsional, dan mekanisme gugatan perdata melalui Pengadilan Tata Usaha Negara (PTUN) masih belum optimal dalam praktik. Penelitian ini menyimpulkan bahwa penguatan pertanggungjawaban negara memerlukan harmonisasi regulasi, peningkatan kapasitas institusional Otoritas Pelindungan Data Pribadi (OPDP) dan Badan Siber dan Sandi Negara (BSSN), serta protokol respons insiden yang terstandardisasi. Rekomendasi kebijakan diarahkan untuk memperkuat akuntabilitas negara dalam melindungi data pribadi warga di ruang digital.

Kata kunci: Pertanggungjawaban Negara; Kebocoran Data; *E-Government*; Hukum Administrasi; Kepastian Hukum; UU PDP; Satu Sehat; DPMPTSP.

LATAR BELAKANG

Transformasi digital dalam tata kelola pemerintahan melalui implementasi *E-Government* telah menjadi suatu keniscayaan bagi negara modern untuk menjawab tuntutan pelayanan publik yang efisien, transparan, dan akuntabel (Undang-Undang Nomor 25 Tahun 2009, 2009, Pasal 1 ayat 1). Di Indonesia, perkembangan ini dimanifestasikan melalui platform digital publik sepertiSatu Sehat yang mengintegrasikan data kesehatan nasional, serta layanan DPMPTSP (Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu) Online yang menyediakan perizinan berusaha terpadu. Platform-platform ini merepresentasikan upaya pemerintah menuju *smart government* yang berorientasi pada kemudahan dan kecepatan layanan (Peraturan Presiden Nomor 95 Tahun 2018, 2018, Pasal 2). Namun, kemajuan teknologi ini tidak terlepas dari risiko fundamental berupa kerentanan keamanan data pribadi jutaan warga negara yang dikelola oleh negara.

Insiden kebocoran data masif yang menimpa platform Satu Sehat pada akhir 2023, di mana data sensitif kesehatan masyarakat diduga terekspos, serta kasus serupa pada beberapa layanan DPMPTSP *Online* di daerah, telah menjadi *wake-up call* yang keras (Liputan6, 2023). Peristiwa ini tidak lagi dapat dipandang semata sebagai persoalan teknis, melainkan telah menyentuh ranah hukum administrasi dan prinsip dasar penyelenggaraan pemerintahan yang baik (*good governance*), khususnya asas kepastian hukum. Asas ini menjamin bahwa setiap tindakan negara harus menciptakan rasa aman dan dapat diprediksi oleh warga negaranya (Hadjon et al., 2020). Penyerahan data pribadi kepada negara dalam konteks *E-Government* seharusnya dilandasi oleh kepastian bahwa negara memiliki kewajiban hukum *(rechtsplicht)* untuk melindunginya. Kebocoran data justru secara paradoksal menciptakan ketidakpastian hukum baru, di mana warga yang mematuhi kewajiban memberikan datanya dirugikan oleh kelalaian aparatur negara (Utrecht, 1986).

Dari perspektif hukum administrasi, fenomena ini mengindikasikan tiga masalah mendasar. Pertama, terdapat potensi kegagalan negara dalam menjalankan fungsi pengurusan *(beheer)* dan pengawasan *(toezicht)* yang layak atas aset digital publik. Kedua, kerangka regulasi yang ada, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Presiden SPBE, dinilai belum komprehensif dan kuat dalam mengatur standar keamanan, akuntabilitas, serta sanksi administratif khusus bagi penyelenggara negara yang lalai (Undang-Undang Nomor 11 Tahun 2008). Ketiga, mekanisme pertanggungjawaban hukum administrasi negara pascakebocoran data masih samar apakah terbatas pada pertanggungjawaban internal, atau meluas hingga pada kewajiban memberikan pemulihan (*rechtsherstel*) yang nyata kepada korban (Ridwan HR, 2022).

Kehadiran Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) seharusnya menjadi landasan kuat bagi pertanggungjawaban negara (Undang-Undang Nomor 27 Tahun 2022, 2022, Pasal 4 & Pasal 47). UU ini menetapkan negara sebagai pengendali data (data controller) yang bertanggung jawab atas pemrosesan data pribadi, dengan kewajiban menjamin keamanannya. Namun, efektivitas UU PDP dalam konteks *E-Government* masih dipertanyakan, terutama menyangkut penegakan, transparansi, dan respons cepat terhadap insiden kebocoran data pada platform publik. Penelitian sebelumnya oleh Makarim (2024) menyoroti bahwa meski norma telah ada, tantangan implementasi berupa kelemahan kapasitas keamanan siber dan koordinasi antar-lembaga masih menjadi penghambat utama akuntabilitas negara (Makarim, 2024).

Oleh karena itu, analisis mendalam yang mengaitkan konsep *E-Government* dengan asas kepastian hukum dalam bingkai hukum administrasi menjadi sangat mendesak. Penelitian ini berupaya mengkritisi dan menganalisis kesenjangan antara janji kepastian hukum dalam pelayanan digital dengan realitas kerentanan yang terjadi. Dengan mengambil studi kasus aktual kebocoran data di Satu Sehat dan DPMPTSP Online, penelitian ini diharapkan dapat memberikan kontribusi pemikiran bagi penguatan konsep negara hukum yang responsif dan akuntabel di era digital.

Berdasarkan latar belakang di atas, rumusan masalah dalam penelitian ini adalah:

1. Bagaimana implementasi asas kepastian hukum dalam penyelenggaraan *E-Government*, khususnya pada platform digital publik seperti Satu Sehat dan layanan DPMPTSP Online?
2. Apakah kerangka hukum administrasi saat ini, terutama pasca pengesahan UU PDP, telah memadai dalam mengatur pertanggungjawaban negara dan memberikan perlindungan hukum kepada masyarakat terkait kebocoran data pada platform digital publik?
3. Bagaimana bentuk pertanggung jawaban hukum administrasi negara dalam kasus kebocoran data di platform Satu Sehat dan DPMPTSP Online ditinjau dari asas kepastian hukum?

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif atau yang sering disebut sebagai penelitian hukum doktrinal (*doctrinal legal research*). Pendekatan ini dipilih karena fokus penelitian adalah pada analisis terhadap prinsip-prinsip hukum, asas-asas hukum administrasi, dan norma-norma hukum positif yang berlaku terkait dengan pertanggungjawaban negara atas kebocoran data pada platform *E-Government.*

HASIL DAN PEMBAHASAN

Konsep dan Landasan Asas Kepastian Hukum dalam Konteks Digital

Asas kepastian hukum merupakan prinsip fundamental dalam negara hukum yang menjamin adanya norma hukum yang jelas, konsisten, dan dapat diprediksi bagi semua pihak (Manan, 2004). Dalam konteks *E-Government*, asas ini mendapatkan dimensi baru karena melibatkan hubungan administratif yang dimediasi oleh teknologi digital. Implementasi asas kepastian hukum pada platform digital publik seperti Satu Sehat dan DPMPTSP Online tidak hanya mencakup kepastian prosedural administratif tradisional, tetapi juga meluas kepada kepastian mengenai keamanan, integritas, dan kerahasiaan data pribadi warga negara yang diserahkan kepada negara (Asshiddiqie, 2010).

Dari analisis dokumen kebijakan, platform Satu Sehat secara eksplisit menyatakan komitmennya terhadap prinsip perlindungan data dalam "Ketentuan Umum dan Kebijakan Privasi

Satu Sehat" yang diterbitkan Kementerian Kesehatan (Kementerian Kesehatan RI, 2023). Demikian pula, sistem OSS (Online Single Submission) yang menjadi tulang punggung DPMPTSP Online mengatur secara detail prosedur, waktu, dan biaya perizinan yang terstandardisasi (CNN Indonesia, 2023). Secara normatif, kedua platform telah memenuhi aspek formal asas kepastian hukum melalui adanya regulasi yang mengatur operasional mereka.

Realitas Implementasi: Antara Janji dan Kerentanan

Meski memiliki landasan regulasi yang memadai, realitas implementasi menunjukkan kesenjangan yang signifikan antara janji kepastian hukum dan kerentanan sistem. Insiden kebocoran data yang menimpa Satu Sehat pada akhir 2023 membuktikan bahwa keberadaan regulasi saja tidak cukup untuk menciptakan kepastian hukum yang sesungguhnya (irto.id, 2023). Data menunjukkan bahwa dalam insiden tersebut, data sensitif kesehatan masyarakat termasuk riwayat vaksinasi dan informasi medis diduga terekspos akibat kerentanan sistem keamanan (Maulana et al., 2024).

Pada DPMPTSP Online, meskipun tidak terekspos secara masif seperti Satu Sehat, studi lapangan menunjukkan adanya kerentanan sistemik. Penelitian oleh Maulana et al. (2024) menemukan bahwa beberapa pemerintah daerah belum memiliki infrastruktur teknologi informasi yang memadai untuk menjamin keamanan data dalam sistem OSS, sementara mereka tetap diwajibkan untuk terintegrasi dengan sistem nasional (Maulana et al., 2024). Hal ini menciptakan "ketidakpastian bertingkat" di satu sisi, pemerintah pusat menjamin kepastian prosedur melalui OSS, namun di sisi lain, kapasitas teknis daerah menciptakan ketidakpastian mengenai keamanan data.

Analisis Faktor Penghambat Kepastian Hukum

Berdasarkan analisis komparatif terhadap kedua kasus, terdapat tiga faktor utama yang menghambat realisasi asas kepastian hukum:

Pertama, disparitas kapasitas dan regulasi. Meski UU PDP telah berlaku, implementasinya memerlukan peraturan teknis dan standar operasional di tingkat sektoral. Kementerian Kesehatan telah menerbitkan Peraturan Menteri Kesehatan tentang Rekam Medis Elektronik (Permenkes No. 24/2022), namun koordinasi dengan BSSN dalam menetapkan standar keamanan spesifik untuk data kesehatan masih perlu diperkuat. Demikian pula, integrasi OSS dengan sistem daerah memerlukan harmonisasi regulasi antara pemerintah pusat dan daerah.

Kedua, literasi digital dan transparansi. Asas kepastian hukum mensyaratkan bahwa norma harus dapat diketahui dan dipahami oleh masyarakat. Dalam konteks digital, hal ini mencakup pemahaman mengenai hak dan risiko dalam berinteraksi dengan platform pemerintah. Survei yang dilakukan oleh SAFEnet (2024) menunjukkan bahwa 68% pengguna layanan digital pemerintah tidak membaca syarat dan ketentuan privasi, dan hanya 12% yang memahami mekanisme pengaduan jika terjadi kebocoran data (Southeast Asia Freedom of Expression Network,2024). Minimnya transparansi pascainsiden seperti dalam kasus Satu Sehatmemperparah ketidakpastian ini.

Ketiga, mekanisme pengawasan yang belum optimal. Fungsi pengawasan administrasi (*bestuurstoezicht*) yang menjadi instrumen penting dalam menjamin kepastian hukum belum sepenuhnya efektif dalam konteks digital. Meski BSSN memiliki kewenangan melakukan audit keamanan siber, kapasitas dan jangkauannya terhadap seluruh platform *E-Government* masih

terbatas. Studi oleh Pusat Studi Hukum dan Teknologi Universitas Indonesia (2024) menemukan bahwa hanya 30% instansi pemerintah pusat yang secara rutin melakukan audit keamanan data mandiri (Pusat Studi Hukum dan Teknologi Fakultas Hukum Universitas Indonesia, 2024).

Analisis Regulasi Terkait Pertanggung jawaban Negara

Kerangka hukum pertanggungjawaban negara atas kebocoran data pada platform *E-Government* dapat ditelusuri melalui tiga lapisan regulasi:

Lapisan pertama: Regulasi umum administrasi pemerintahan. UU Administrasi Pemerintahan (UU AP) mengatur pertanggungjawaban pejabat pemerintahan atas keputusan dan tindakan administratif (Undang-Undang Nomor 30 Tahun 2014). 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. Namun, UU AP belum secara spesifik mengatur pertanggungjawaban atas kelalaian pengamanan data dalam sistem elektronik.

Lapisan kedua: Regulasi sektoral *E-Government* dan keamanan siber. Perpres SPBE (Sistem Pemerintahan Berbasis Elektronik) menetapkan kewajiban setiap instansi pemerintah untuk menjamin keamanan sistem elektronik. Demikian pula, Peraturan BSSN menetapkan standar keamanan informasi bagi penyelenggara sistem elektronik pemerintah (Peraturan BSSN Nomor 4 Tahun 2023). Namun, regulasi ini lebih berfokus pada aspek teknis pencegahan, bukan pada mekanisme pertanggungjawaban pascakejadian.

Lapisan ketiga: Regulasi spesifik perlindungan data pribadi. UU PDP menjadi lompatan signifikan dengan secara eksplisit mengatur pertanggungjawaban pengendali data, termasuk negara (Undang-Undang Nomor 27 Tahun 2022, 2022, Pasal 47 & Pasal 65). Pasal 47 UU PDP menetapkan bahwa pengendali data bertanggung jawab atas pemrosesan data pribadi dan wajib menjamin keamanannya. Pasal 65 lebih lanjut mengatur sanksi administratif berupa denda hingga Rp 5 miliar bagi pengendali data yang lalai melindungi data pribadi.

Kelemahan dan Kesenjangan Regulasi

Meski terlihat komprehensif secara normatif, analisis mendalam menunjukkan beberapa kelemahan struktural:

Pertama, fragmentasi kewenangan. Kewenangan pengawasan dan penegakan hukum atas kebocoran data tersebar di beberapa instansi: OPDP (Otoritas Pelindungan Data Pribadi) sebagai regulator utama, BSSN sebagai otoritas keamanan siber, Ombudsman untuk maladministrasi, dan inspektorat internal masing-masing kementerian/lembaga (Makarim, 2024). Fragmentasi ini berpotensi menciptakan tumpang-tindih wewenang atau justru vakum penanganan, sebagaimana terjadi dalam kasus awal kebocoran data PeduliLindungi dimana tidak jelas lembaga mana yang berwenang melakukan investigasi komprehensif (PBHI, 2023).

Kedua, ketidakjelasan mekanisme pertanggungjawaban keuangan negara. Jika negara harus memberikan ganti rugi kepada korban kebocoran data, mekanisme pembayarannya belum diatur secara jelas. UU Pertanggungjawaban Keuangan Negara mengatur pertanggungjawaban bendahara, namun tidak spesifik mengatur kompensasi akibat kelalaian administratif dalam pengelolaan data (Undang-Undang Nomor 1 Tahun 2004). Hal ini menciptakan ketidakpastian prosedural yang justru bertentangan dengan asas kepastian hukum yang hendak dilindungi.

Ketiga, tantangan penerapan asas strict liability. Pasal 47 ayat (2) UU PDP menerapkan asas strict liability (pertanggungjawaban mutlak) bagi pengendali data. Dalam konteks negara sebagai pengendali data, penerapan asas ini memiliki kompleksitas tersendiri. Bagaimana

membedakan antara kelalaian yang dapat dipertanggungjawabkan dan kerentanan sistem yang mungkin timbul meski telah dilakukan upaya standar? Penelitian hukum komparatif oleh Sembiring (2024) menunjukkan bahwa negara-negara seperti Jerman menerapkan standar "due diligence" yang lebih proporsional untuk pertanggungjawaban instansi publik (Sembiring, 2024).

Kerangka Teoritis Pertanggungjawaban Administrasi

Dalam teori hukum administrasi, pertanggungjawaban negara dapat dibedakan menjadi tiga bentuk: (1) pertanggungjawaban politik kepada rakyat melalui mekanisme demokrasi; (2) pertanggungjawaban hukum melalui proses peradilan; dan (3) pertanggungjawaban administratif melalui mekanisme internal pemerintahan (Ridwan, 2022). Dalam konteks kebocoran data, ketiga bentuk ini saling beririsan, namun fokus penelitian ini adalah pada pertanggungjawaban hukum dan administratif.

Asas kepastian hukum mensyaratkan bahwa mekanisme pertanggungjawaban harus memenuhi empat kriteria: (a) kejelasan subjek yang bertanggung jawab; (b) kejelasan jenis dan besaran tanggung jawab; (c) kejelasan prosedur penuntutan pertanggungjawaban; dan (d) prediktabilitas outcome dari proses pertanggungjawaban (Attamimi, 1990).

Bentuk Pertanggungjawaban dalam Kasus Satu Sehat

Berdasarkan analisis dokumen hukum dan pemberitaan, dapat diidentifikasi beberapa bentuk pertanggungjawaban yang muncul atau seharusnya muncul dalam kasus Satu Sehat:

Pertama, pertanggung jawaban administratif internal. Kementerian Kesehatan memiliki kewajiban internal untuk melakukan investigasi, menindak pejabat/pegawai yang lalai, dan memperbaiki sistem. Meski Kemenkes mengklaim telah melakukan investigasi internal, publik tidak mendapatkan akses terhadap hasil investigasi secara lengkap, sehingga mempertanyakan akuntabilitas proses ini (Kompas, 2023).

Kedua, pertanggungjawaban kepada otoritas pengawas. Berdasarkan UU PDP, Kemenkes wajib melaporkan kebocoran data kepada OPDP dalam waktu 3x24 jam. OPDP kemudian berwenang melakukan pemeriksaan dan mengenakan sanksi administratif. Hingga saat penelitian ini ditulis, belum ada informasi publik mengenai proses sanksi administratif oleh OPDP terhadap Kemenkes terkait kasus ini.

Ketiga, pertanggungjawaban perdata kepada korban. Masyarakat yang dirugikan berhak mengajukan gugatan perdata berdasarkan Pasal 26 UU PDP jo. ketentuan tentang perbuatan melawan hukum dalam KUHPerdata. Mekanisme ini mensyaratkan pembuktian kerugian yang konkret, yang dalam kasus kebocoran data kesehatan seringkali sulit dibuktikan secara langsung dan segera (Ganarsih, 2023).

Keempat, pertanggungjawaban melalui PTUN. Gugatan ke PTUN dapat diajukan berdasarkan UU AP jika dapat dibuktikan bahwa kebocoran data terjadi akibat kelalaian atau kesalahan prosedural pejabat pemerintah. Gugatan semacam ini pernah diajukan PBHI terhadap Kemenkes terkait kebocoran data PeduliLindungi, namun prosesnya masih berlangsung (Hukumonline, 2024).

Bentuk Pertanggungjawaban dalam Kasus DPMPTSP Online

Untuk DPMPTSP Online, bentuk pertanggungjawaban memiliki karakteristik yang sedikit berbeda karena melibatkan hubungan tiga pihak: pemerintah pusat (BKPM), pemerintah daerah, dan pelaku usaha.

Pertama, pertanggung jawaban administratif terbagi. Berdasarkan UU Cipta Kerja dan peraturan turunannya, BKPM bertanggung jawab atas sistem OSS nasional, sementara pemerintah daerah bertanggung jawab atas integrasi sistem daerah dengan OSS (Undang-Undang Nomor 11 Tahun 2020). Jika kebocoran data terjadi pada data yang dikelola daerah, maka pertanggungjawaban utama berada pada pemerintah daerah. Namun, jika kerentanan ada pada sistem pusat, BKPM yang bertanggung jawab.

Kedua, mekanisme kompensasi administratif khusus. Peraturan Menteri Investasi/BKPM mengatur bahwa jika terjadi kesalahan sistem yang merugikan pelaku usaha, pemerintah wajib mengeluarkan perbaikan administratif berupa penerbitan ulang dokumen perizinan tanpa biaya (BKPM, 2021). Namun, peraturan ini belum mengatur kompensasi untuk kerugian immaterial akibat kebocoran data usaha yang bersifat rahasia.

Ketiga, tantangan pembuktian dan locus standi. Berbeda dengan data kesehatan yang secara intrinsik bersifat pribadi, data usaha dalam DPMPTSP Online sebagian bersifat publik (seperti nama perusahaan, alamat). Namun, data seperti rencana bisnis, laporan keuangan, atau dokumen rahasia lainnya juga dikelola dalam sistem. Jika terjadi kebocoran data rahasia ini, pelaku usaha menghadapi tantangan pembuktian bahwa data tersebut benar-benar bersifat rahasia dan bahwa kebocoran menyebabkan kerugian kompetitif (Wijaya, 2024).

Evaluasi Terhadap Pemenuhan Asas Kepastian Hukum

Berdasarkan analisis terhadap kedua kasus, dapat dievaluasi bahwa mekanisme pertanggungjawaban yang ada belum sepenuhnya memenuhi prinsip kepastian hukum:

Pertama, belum adanya kejelasan hierarki pertanggungjawaban. Ketika terjadi kebocoran data pada platform seperti Satu Sehat yang melibatkan kerjasama dengan pihak ketiga (vendor teknologi), tidak jelas apakah pertanggungjawaban utama tetap pada negara atau dapat dialihkan kepada vendor berdasarkan kontrak. UU PDP menyatakan bahwa pengendali data (dalam hal ini negara) tetap bertanggung jawab meski pemrosesan data dilimpahkan kepada pihak lain (Undang-Undang Nomor 27 Tahun 2022), namun implementasi prinsip ini dalam praktik administrasi belum memiliki pedoman operasional yang jelas.

Kedua, ketidakpastian mengenai besaran kompensasi. Tidak adanya standar nasional mengenai besaran ganti rugi untuk kebocoran data menciptakan ketidakpastian. Bandingkan dengan beberapa negara yang telah mengatur standar kompensasi, seperti di Inggris di mana *Information Commissioner's Office* (ICO) memiliki pedoman penghitungan ganti rugi berdasarkan jenis dan sensitivitas data yang bocor (ICO, 2023).

Ketiga, prosedur yang rumit dan berbiaya tinggi. Mekanisme gugatan melalui PTUN atau pengadilan perdata memerlukan biaya dan waktu yang tidak sedikit, sehingga seringkali tidak terjangkau bagi korban individual. Hal ini bertentangan dengan prinsip akses terhadap keadilan *(access to justice)* yang merupakan elemen penting dari kepastian hukum.

KESIMPULAN DAN SARAN

Penelitian ini menunjukkan bahwa penyelenggaraan E-Government di Indonesia, khususnya pada platform Satu Sehat dan DPMPTSP Online, secara normatif telah memiliki landasan hukum yang memadai untuk menjamin asas kepastian hukum dan perlindungan data pribadi. Berbagai regulasi, termasuk standar operasional dan komitmen perlindungan data, telah tersedia dan diperkuat dengan hadirnya Undang-Undang Perlindungan Data Pribadi (UU PDP) yang menetapkan prinsip pertanggungjawaban ketat (strict liability) bagi pengendali data,

termasuk negara. Namun demikian, keberadaan regulasi tersebut belum sepenuhnya berbanding lurus dengan implementasi substantif di lapangan, sebagaimana tercermin dari terjadinya insiden kebocoran data, keterbatasan kapasitas keamanan siber, kesenjangan digital antarwilayah, rendahnya literasi digital masyarakat, serta minimnya transparansi dalam penanganan insiden.

Bentuk pertanggungjawaban hukum administrasi negara atas kebocoran data pada platform E-Government secara teoritis telah mencakup mekanisme administratif internal, pengawasan otoritas pelindungan data, gugatan perdata, hingga upaya hukum melalui Pengadilan Tata Usaha Negara. Akan tetapi, dalam praktiknya mekanisme tersebut belum sepenuhnya memenuhi asas kepastian hukum karena masih terdapat fragmentasi kewenangan antar-lembaga, prosedur yang kompleks dan berbiaya tinggi, ketidakjelasan standar kompensasi, serta lemahnya koordinasi antara pemerintah pusat dan daerah. Kondisi ini menyebabkan pertanggungjawaban negara cenderung bersifat reaktif dan tidak memberikan jaminan perlindungan hukum yang prediktabel dan mudah diakses bagi masyarakat yang dirugikan.

Untuk memperkuat realisasi asas kepastian hukum, pemerintah perlu melakukan harmonisasi dan penyederhanaan regulasi melalui pembentukan kerangka tata kelola keamanan data E-Government yang terintegrasi, disertai penguatan peran Otoritas Pelindungan Data Pribadi sebagai koordinator utama dengan dukungan teknis BSSN. Selain itu, diperlukan pengembangan mekanisme kompensasi administratif yang cepat dan terstandardisasi, peningkatan transparansi penanganan insiden melalui keterbukaan informasi publik, serta pelaksanaan program literasi digital yang masif bagi masyarakat dan aparatur negara. Langkah-langkah tersebut diharapkan mampu memastikan bahwa pertanggungjawaban negara atas kebocoran data tidak hanya bersifat normatif, tetapi benar-benar efektif dalam melindungi hak-hak warga negara di era pemerintahan digital.

DAFTAR REFERENSI

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 1 Tahun 2004 tentang Perbendaharaan Negara.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 1 Tahun 2024.

Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik.

Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan.

Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja.

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 Menteri Investasi/Kepala BKPM Nomor 6 Tahun 2021 tentang Pedoman dan Tata Cara Pelayanan Perizinan Berusaha melalui Sistem OSS.

Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2023 tentang Standar Keamanan Informasi untuk Penyelenggara Sistem Elektronik Pemerintah.

Asshiddiqie, Jimly. (2010). Perihal Undang-Undang. Jakarta: Rajawali Pers.

Attamimi, A. Hamid S. (1990). Peranan Keputusan Presiden Republik Indonesia dalam Penyelenggaraan Pemerintahan Negara. Disertasi. Depok: Universitas Indonesia.

Ganarsih, Yenti. (2023). Aspek Hukum Perlindungan Data Pribadi di Indonesia (Cetakan Kedua). Jakarta: Kencana.

Hadjon, Philipus M., dkk. (2020). Pengantar Hukum Administrasi Indonesia (Edisi Revisi). Yogyakarta: Gadjah Mada University Press.

Manan, Bagir. (2004). Teori dan Politik Konstitusi. Yogyakarta: FH UII Press.

Makarim, Edmon. (2024). Perlindungan Data Pribadi: Teori & Praktik Implementasi UU PDP. Jakarta: Prenadamedia Group.

Ridwan HR. (2022). Hukum Administrasi Negara (Edisi Revisi). Jakarta: Rajawali Pers.

Utrecht, E. (1986). Rangkaian Sari Kuliah Hukum Administrasi Negara. Surabaya: Pustaka Tinta Mas.

Maulana, Rizky, dkk. (2024). Analisis Kerentanan Keamanan Sistem OSS pada Pemerintah Daerah. *Jurnal Administrasi Publik,* 15(2), 45-60.

Pusat Studi Hukum dan Teknologi FHUI. (2024). Audit Keamanan Data pada Instansi Pemerintah: Temuan dan Rekomendasi (*Policy Brief* No. 03/2024). Depok: Universitas Indonesia.

Sembiring, Selma. (2024). *Comparative Analysis of State Liability for Data Breaches: Lessons from the EU GDPR. Indonesian Journal of International Law*, 21(1), 89-112.

Wijaya, Chandra. (2024). Perlindungan Hukum Data Usaha dalam Sistem Perizinan Online. Jurnal Hukum Bisnis, 42(3), 78-85.

Badan Siber dan Sandi Negara (BSSN). (2023). Pedoman Manajemen Insiden Keamanan Siber untuk Penyelenggara Sistem Elektronik Publik. Jakarta: BSSN.

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/

Kementerian Kesehatan Republik Indonesia. (2023, 18 September). Ketentuan Umum dan Kebijakan Privasi Satu Sehat. Diakses dari https://satusehat.kemkes.go.id/kebijakan-privasi

Perhimpunan Bantuan Hukum Indonesia (PBHI). (2023). Laporan Investigasi Kebocoran Data PeduliLindungi. Jakarta: PBHI.

Southeast Asia Freedom of Expression Network (SAFEnet). (2024). Laporan Kesadaran Keamanan Digital Masyarakat Indonesia 2024. Jakarta: SAFEnet.

CNN Indonesia. (2023, 20 November). Kebocoran Data Satu Sehat, Kemenkes Diminta Transparan. Diakses dari https://www.cnnindonesia.com/teknologi/20231120154531-192-1032457/kebocoran-data-satu-sehat-kemenkes-diminta-transparan

Hukumonline. (2024, 15 Februari). PBHI Gugat Kemenkes ke PTUN Jakarta Soal Kebocoran Data PeduliLindungi. Diakses dari https://www.hukumonline.com/berita/a/pbhi-gugat-kemenkes-ke-ptun-jakarta-soal-kebocoran-data-pedulilindungi-lt65cda5b7e3a59

Kompas. (2023, 28 November). Kemenkes Klaim Investigasi Kebocoran Data Satu Sehat, Publik Minta Transparansi. Diakses dari https://tekno.kompas.com/read/2023/11/28/15000047/kemenkes-klaim-investigasi-kebocoran-data-satu-sehat-publik-minta-transparansi

Liputan6. (2023, 15 November). Kasus Kebocoran Data Satu Sehat, Kemenkes Klaim Sudah Lakukan Investigasi. Diakses dari https://www.liputan6.com/tekno/read/5404341/kasus-kebocoran-data-satu-sehat-kemenkes-klaim-sudah-lakukan-investigasi

Tirto.id. (2023, 25 November). Potret Kebocoran Data Kesehatan di Indonesia: dari PeduliLindungi hingga Satu Sehat. Diakses dari https://tirto.id/potret-kebocoran-data-kesehatan-di-indonesia-dari-pedulilindungi-hingga-satu-sehat-gt1H