

Pengawasan Negara dan Tanggung Jawab atas Dugaan Kebocoran Data MyPertamina dalam Perspektif UU Pelindungan Data Pribadi

Aryadika Syaban^{1*}, Sidi Ahyar Wiraguna²

Fakultas Ilmu Hukum, Hukum, Universitas Esa Unggul, Indonesia

Email Korespondensi*: aryadika.syaban@student.esaunggul.ac.id^{1*}; sidi.ahyar@esaunggul.ac.id²

ARTICLE INFO

Article History

Submission : 08-07-2026

Received : 09-07-2026

Revised : 01-09-2026

Accepted : 02-09-2026

Keywords

Accountability Gap;

BUMN;

MyPertamina;

Pelindungan Data Pribadi;

Pengawasan Negara

DOI:

10.59066/ijoms.v5i2.2699

ABSTRACT

Dugaan penawaran 44.237.264 rekaman yang diklaim berasal dari MyPertamina pada November 2022 menimbulkan pertanyaan mengenai pengawasan negara terhadap pengendali data dan penyelenggara sistem elektronik. Karena sumber kebocoran belum dibuktikan melalui putusan atau laporan forensik publik yang final, penelitian ini tidak menetapkan PT Pertamina sebagai pelaku pelanggaran, melainkan menggunakan insiden tersebut sebagai kasus uji normatif. Penelitian hukum normatif ini menggunakan pendekatan perundang-undangan, konseptual, kasus, dan perbandingan terbatas. Bahan hukum dianalisis dengan interpretasi gramatikal, sistematis, dan teleologis serta pemetaan kewenangan. Hasil penelitian menunjukkan bahwa UU Nomor 27 Tahun 2022 telah menetapkan dasar pemrosesan, penilaian dampak, keamanan, pencegahan akses tidak sah, notifikasi kegagalan, pejabat pelindungan data, sanksi, dan hak ganti rugi. Namun, efektivitas pengawasan masih dibatasi oleh belum operasionalnya lembaga PDP yang independen, irisan mandat Komdigi dan BSSN, serta minimnya transparansi hasil investigasi. Status BUMN tidak otomatis mengatribusikan tindakan korporasi kepada negara menurut Articles on State Responsibility; pertanggungjawaban korporasi harus dibedakan dari kewajiban konstitusional negara untuk mengatur, mengawasi, menegakkan, dan menyediakan pemulihan. Kebaruan penelitian adalah model akuntabilitas berlapis yang memisahkan tanggung jawab pengendali data dari kewajiban negara sebagai regulator, supervisor, dan penjamin pemulihan.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.
Copyright© 2026 by Author. Published by CV. Era Digital Nusantara



Pendahuluan

Transformasi layanan publik berbasis aplikasi memperluas pemrosesan data pribadi oleh badan publik dan badan usaha milik negara. Pada saat yang sama, serangan siber dan kegagalan pengamanan dapat menimbulkan kerugian material maupun immaterial bagi subjek data. Konstitusi menempatkan pelindungan diri pribadi sebagai hak yang dijamin Pasal 28G ayat (1) UUD 1945. UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) kemudian membentuk kerangka hak subjek data, kewajiban pengendali dan prosesor, pengawasan, sanksi, serta pemulihan.

Pada 10 November 2022 beredar penawaran basis data yang diklaim pelaku bernama “Bjorka” sebagai data MyPertamina dengan jumlah 44.237.264 rekaman. Pemberitaan pada

saat itu merekam pernyataan Pertamina dan Telkom bahwa keduanya melakukan pemeriksaan bersama. Informasi tersebut membuktikan adanya klaim dan proses verifikasi, bukan dengan sendirinya membuktikan bahwa sumber data adalah sistem MyPertamina atau bahwa PT Pertamina telah melanggar kewajiban hukum. Hingga batas penelusuran penelitian ini, tidak ditemukan putusan pengadilan atau laporan forensik otoritas yang dipublikasikan secara lengkap dan menetapkan sumber, sebab, serta pihak yang bertanggung jawab. Oleh sebab itu, seluruh penyebutan insiden dalam artikel ini menggunakan istilah “dugaan kebocoran data MyPertamina”.

Pembatasan status fakta tersebut penting secara metodologis. Penyangkalan atau belum adanya konfirmasi tidak membuktikan keamanan sistem, tetapi juga tidak boleh dipakai sebagai bukti terjadinya kelalaian. Insiden digunakan sebagai kasus uji untuk menilai apakah hukum positif menyediakan: (1) standar pencegahan; (2) pembagian kewenangan pengawasan; (3) prosedur investigasi dan notifikasi; dan (4) pemulihan bagi subjek data apabila pelanggaran terbukti.

Kajian terdahulu umumnya bergerak pada empat kelompok. Pertama, kajian keamanan data menekankan kewajiban teknis pengendali dan penyelenggara sistem elektronik. Kedua, kajian kelembagaan menyoroti urgensi otoritas PDP yang independen. Ketiga, kajian BUMN lebih sering membahas pertanggungjawaban korporasi atau pelayanan publik tanpa menguji syarat atribusi tindakan kepada negara. Keempat, kajian remediasi membahas sanksi, tetapi belum menghubungkan pengawasan preventif, penegakan, dan pemulihan korban dalam satu model. Artikel ini mengisi celah tersebut dengan membedakan tanggung jawab PT Pertamina sebagai badan hukum/pengendali data dari kewajiban negara sebagai regulator, supervisor, dan penjamin akses pemulihan.

Dalam artikel ini, *accountability gap* didefinisikan sebagai jarak antara kewajiban hukum yang telah ditetapkan dengan kemampuan institusional untuk mendeteksi ketidakpatuhan, menetapkan tanggung jawab secara independen, membuka hasil pengawasan secara proporsional, dan menyediakan pemulihan efektif. Unsurnya meliputi kesenjangan norma pelaksana, kesenjangan kewenangan, kesenjangan informasi, kesenjangan penegakan, dan kesenjangan remediasi. Definisi ini mencegah istilah tersebut menjadi sekadar penilaian retorik.

Kerangka teoritis penelitian memadukan perlindungan hukum preventif dan represif dengan kewajiban positif negara atas hak privasi. *Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA)* dipakai hanya sebagai lensa pembanding mengenai atribusi, bukan sebagai dasar langsung pertanggungjawaban domestik. Article 4 berkenaan dengan organ negara; Article 5 dengan entitas yang diberi kewenangan pemerintahan dan bertindak dalam kapasitas tersebut; sedangkan Article 8 mensyaratkan instruksi, arahan, atau kontrol negara atas tindakan tertentu. Kepemilikan saham negara pada persero tidak memenuhi syarat-syarat itu secara otomatis.

Berdasarkan latar tersebut, penelitian menjawab dua pertanyaan: (1) bagaimana desain dan kesenjangan pengawasan preventif terhadap pemrosesan data MyPertamina menurut

UU PDP dan rezim keamanan sistem elektronik; dan (2) bagaimana model pertanggungjawaban yang membedakan tanggung jawab korporasi dari kewajiban konstitusional negara untuk menutup accountability gap?

Tujuan penelitian adalah memetakan kewajiban lembaga, dan instrumen pengawasan yang berlaku; menguji batas atribusi tindakan BUMN kepada negara; serta merumuskan model akuntabilitas berlapis yang menghubungkan pencegahan, penegakan, dan pemulihan. Kebaruannya terletak pada pemisahan dua jalur tanggung jawab—corporate/data-controller liability dan public supervisory responsibility yang dioperasikan melalui indikator yang dapat diuji.

Metode Penelitian

Penelitian ini merupakan penelitian hukum normatif dengan pendekatan perundang-undangan, konseptual, kasus, dan perbandingan terbatas. Pendekatan perundang-undangan digunakan untuk menyinkronkan UU PDP, UU ITE sebagaimana terakhir diubah dengan UU Nomor 1 Tahun 2024, PP Nomor 71 Tahun 2019, Perpres Nomor 82 Tahun 2022, Peraturan BSSN Nomor 8 Tahun 2020, Peraturan BSSN Nomor 7 Tahun 2023, dan Peraturan BSSN Nomor 1 Tahun 2024. Pendekatan konseptual digunakan untuk membedakan kewajiban positif negara, tanggung jawab pengendali data, dan atribusi menurut ARSIWA. Pendekatan kasus digunakan secara terbatas terhadap dokumen publik mengenai dugaan insiden MyPertamina. GDPR dipakai sebagai pembanding fungsional, bukan sebagai hukum yang berlaku di Indonesia.

Bahan hukum primer meliputi UUD 1945, undang-undang dan peraturan pelaksana tersebut, Putusan Mahkamah Konstitusi Nomor 151/PUU-XXII/2024 terkait Pasal 53 ayat (1) UU PDP, serta teks dan komentar resmi ARSIWA. Bahan sekunder meliputi buku metodologi hukum, artikel jurnal 2015–2025, dan laporan resmi lembaga. Pemberitaan media hanya dipakai untuk merekonstruksi kronologi klaim dan respons awal; kredibilitasnya dinilai berdasarkan identitas narasumber, konsistensi antar-sumber, tanggal, dan pemisahan fakta dari dugaan. Google Scholar, JDIH, dan repositori diperlakukan sebagai sarana penelusuran, bukan sebagai jenis bahan hukum.

Penelusuran dilakukan terhadap bahan yang terbit sampai 31 Desember 2025 dengan kata kunci Indonesia dan Inggris yang mencakup MyPertamina, kebocoran data, pengendali data, BUMN, pengawasan PDP, data protection authority, state-owned enterprise, attribution, dan remedy. Status peraturan diverifikasi melalui JDIH pemerintah/BPK dan laman lembaga penerbit. Sumber dikeluarkan apabila metadata tidak dapat diverifikasi, hanya tersedia sebagai cuplikan, atau tidak berhubungan langsung dengan pertanyaan penelitian.

Analisis dilakukan dalam empat tahap. Pertama, inventarisasi kewajiban dan hak menurut hierarki peraturan. Kedua, interpretasi gramatikal untuk menentukan isi pasal, interpretasi sistematis untuk memetakan hubungan UU PDP dengan rezim PSE dan keamanan siber, serta interpretasi teleologis untuk menilai kesesuaiannya dengan

pelindungan hak. Ketiga, pemetaan kewenangan Komdigi, BSSN, dan lembaga PDP untuk mendeteksi irisan maupun kekosongan. Keempat, evaluasi preskriptif melalui matriks norma–institusi–bukti implementasi–remedi. Analogi dengan ARSIWA dibatasi pada tes atribusi dan tidak dipakai untuk menyatakan adanya pelanggaran internasional.

Batas penelitian adalah tidak tersedianya laporan forensik final yang dapat diverifikasi, data kepatuhan internal Pertamina, dan putusan yang menetapkan tanggung jawab dalam insiden ini. Karena itu, penelitian tidak menyimpulkan telah terjadi kebocoran dari sistem MyPertamina atau kelalaian pihak tertentu. Kesimpulan tentang efektivitas diarahkan pada kecukupan desain hukum dan keterlihatan mekanisme pengawasan berdasarkan dokumen publik.

Hasil dan Pembahasan

1. Desain Pengawasan Preventif dan Kewajiban Pengendali Data

UU PDP tidak menempatkan seluruh kewajiban keamanan pada Pasal 20. Pasal 20 mengatur dasar pemrosesan. Prinsip pemrosesan terdapat dalam Pasal 16 ayat (2). Penilaian dampak pelindungan data pribadi untuk pemrosesan berisiko tinggi diatur Pasal 34. Kewajiban menyusun dan menerapkan langkah teknis operasional terdapat dalam Pasal 35, sedangkan penentuan tingkat keamanan dengan memperhatikan sifat dan risiko pemrosesan diatur Pasal 36. Pencegahan akses tidak sah diatur Pasal 39. Apabila terjadi kegagalan pelindungan data, Pasal 46 mewajibkan pemberitahuan tertulis paling lambat 3 x 24 jam kepada subjek data dan lembaga.

Pasal 53 mengharuskan penunjukan pejabat atau petugas yang melaksanakan fungsi pelindungan data pribadi apabila pemrosesan dilakukan untuk kepentingan pelayanan publik, terdapat pemantauan teratur dan sistematis dalam skala besar, atau pemrosesan data spesifik/skala besar. Putusan MK Nomor 151/PUU-XXII/2024 memaknai penghubung pada Pasal 53 ayat (1) huruf b sebagai “dan/atau”, sehingga kondisi pemantauan teratur atau pemrosesan skala besar tidak harus selalu kumulatif. Relevansinya bagi MyPertamina harus ditentukan dari aktivitas pemrosesan aktual, bukan semata-mata status BUMN.

Sebagai penyelenggara sistem elektronik, entitas pengelola MyPertamina juga tunduk pada kewajiban keandalan, keamanan, tata kelola, dan penanganan kegagalan menurut UU ITE dan PP Nomor 71 Tahun 2019. Peraturan BSSN Nomor 8 Tahun 2020 menyediakan kerangka sistem pengamanan PSE. Perpres Nomor 82 Tahun 2022 beserta Peraturan BSSN Nomor 7 Tahun 2023 dan Nomor 1 Tahun 2024 relevan apabila suatu sistem telah diidentifikasi sebagai Infrastruktur Informasi Vital atau masuk tata kelola insiden yang ditentukan. Namun, artikel ini tidak mengasumsikan MyPertamina berstatus IIV tanpa penetapan berwenang.

Matriks berikut memperlihatkan bahwa pengawasan preventif harus mengikuti jenis kewajiban, bukan disederhanakan sebagai “audit BSSN”. Audit keamanan SPBE berdasarkan Peraturan BSSN Nomor 8 Tahun 2024 ditujukan pada objek SPBE dan tidak otomatis berlaku terhadap aplikasi BUMN. Untuk PSE non-SPBE, dasar pengamanan dan

audit harus ditelusuri melalui rezim PSE, klasifikasi sistem, kontrak, serta kemungkinan status IIV.

Tabel 1. Matriks Kewajiban dan Pengawasan

Kewajiban	Dasar Hukum	Pemegang Kewajiban	Pengawasan Utama	Kesenjangan yang diuji
Dasar dan prinsip pemrosesan	UU PDP Pasal 16 (2), 20	Pengendali data	Lembaga PDP	Dokumentasi legalitas dan tujuan
DPIA pemrosesan berisiko tinggi	UU PDP Pasal 34	Pengendali data	Lembaga PDP	Kriteria, dokumentasi, tindak lanjut
Langkah dan tingkat keamanan	UU PDP Pasal 35–36; PP 71/2019	Pengendali/prosesor dan PSE	Lembaga PDP; Komdigi; BSSN sesuai mandat	Standar teknis, asesmen berbasis risiko
Pencegahan akses tidak sah	UU PDP Pasal 39	Pengendali data	Lembaga PDP; dukungan teknis BSSN	Kontrol akses dan bukti pengujian
Notifikasi kegagalan	UU PDP Pasal 46	Pengendali data	Lembaga PDP	Ambang kegagalan, isi dan ketepatan waktu
Petugas fungsi PDP	UU PDP Pasal 53 jo. Putusan MK 151/PUU-XXII/2024	Pengendali/prosesor yang memenuhi kriteria	Lembaga PDP	Independensi dan akses kepada pimpinan

Dari matriks tersebut, UU PDP telah menyediakan norma inti, tetapi efektivitas tidak dapat dinyatakan “memadai” hanya dari kelengkapan pasal. Efektivitas menuntut lembaga yang operasional, prosedur pemeriksaan, akses pada bukti teknis, koordinasi insiden, dan keputusan yang transparan. Ketiadaan informasi publik mengenai hasil forensik MyPertamina tidak membuktikan tidak ada pemeriksaan; namun, minimnya keterlihatan proses dan hasil menimbulkan kesenjangan informasi yang menghambat akuntabilitas publik dan pemulihan subjek data.

2. Pembagian Kewenangan Komdigi, BSSN, dan Lembaga PDP

UU PDP menempatkan penyelenggaraan perlindungan data oleh lembaga yang ditetapkan Presiden (Pasal 58–60). Fungsinya meliputi perumusan kebijakan, pengawasan, penegakan administratif, fasilitasi penyelesaian sengketa di luar pengadilan, dan pelaksanaan kewenangan lain menurut undang-undang. Komdigi menjalankan fungsi pemerintahan di bidang komunikasi dan digital serta rezim PSE. BSSN berfokus pada keamanan siber, standar teknis, koordinasi insiden, dan perlindungan IIV. Perbedaan objek tersebut harus dipertahankan: otoritas PDP menilai legalitas dan kepatuhan pemrosesan serta hak subjek data, sedangkan BSSN menilai aspek teknis keamanan dan respons insiden.

Sampai akhir 2025, lembaga PDP yang dirancang UU belum beroperasi sebagai otoritas independen tersendiri. Keadaan ini menghasilkan transisi kelembagaan: fungsi PSE dan sebagian perlindungan data masih terkait Komdigi, sementara BSSN memegang mandat

teknis keamanan siber. Solusi bukan memindahkan seluruh fungsi PDP kepada BSSN, melainkan membentuk protokol koordinasi. Otoritas PDP harus memimpin pemeriksaan kepatuhan dan remediasi; BSSN memberikan asesmen teknis/forensik sesuai kewenangan; Komdigi menangani tata kelola PSE; dan penegak hukum bertindak apabila unsur pidana terpenuhi.

Konflik kepentingan tidak boleh disimpulkan hanya karena negara memiliki saham BUMN. Risiko struktural muncul apabila unit pemerintah yang berkepentingan terhadap kinerja BUMN juga dapat memengaruhi pengawasan atau keterbukaan hasil pemeriksaan. Mitigasinya adalah independensi fungsional, standar pembuktian yang sama bagi pengendali publik dan privat, publikasi ringkasan keputusan, mekanisme keberatan, serta pengawasan yudisial.

3. Tanggung Jawab Korporasi dan Batas Atribusi kepada Negara

PT Pertamina (Persero) adalah perseroan yang memiliki kepribadian hukum tersendiri. Apabila terbukti bertindak sebagai pengendali atau prosesor dan melanggar UU PDP, tanggung jawab pertama melekat pada entitas sesuai peran pemrosesannya. Hak subjek data mencakup hak memperoleh informasi, akses, koreksi, penghapusan dalam kondisi tertentu, penghentian pemrosesan, dan menggugat serta menerima ganti rugi berdasarkan Pasal 12. Sanksi administratif diatur Pasal 57, sedangkan ketentuan pidana berlaku terhadap perbuatan yang memenuhi unsur larangan pidana; kebocoran tidak otomatis sama dengan tindak pidana oleh pengendali.

ARSIWA tidak mengubah setiap tindakan BUMN menjadi tindakan negara. Pertamina bukan organ negara dalam pengertian Article 4 hanya karena dimiliki negara. Article 5 baru relevan apabila badan tersebut diberi kewenangan pemerintahan dan tindakan yang dipersoalkan dilakukan dalam kapasitas itu. Article 8 menuntut bukti bahwa tindakan spesifik dilakukan atas instruksi, arahan, atau kontrol negara. Dalam perkara dugaan kegagalan keamanan aplikasi komersial/pelayanan, ketiga tes harus dibuktikan secara terpisah. Tanpa bukti tersebut, jalur yang tepat adalah tanggung jawab korporasi domestik, bukan atribusi internasional.

Namun, tidak teratribusi secara langsung bukan berarti negara bebas dari kewajiban. Negara tetap memiliki kewajiban positif yang mandiri untuk membuat aturan, mengawasi kepatuhan tanpa diskriminasi, menyelidiki dugaan pelanggaran secara efektif, menegakkan sanksi, dan menjamin akses pemulihan. Kegagalan pada fungsi-fungsi ini dapat dinilai melalui hukum konstitusi dan administrasi domestik tanpa harus menyatakan perbuatan BUMN sebagai perbuatan negara.

4. Model Akuntabilitas Berlapis

Model yang diusulkan terdiri atas dua jalur tanggung jawab dan tiga fase intervensi. Jalur pertama adalah tanggung jawab pengendali/prosesor yang ditentukan oleh kontrol faktual atas tujuan dan cara pemrosesan. Jalur kedua adalah tanggung jawab pengawasan publik yang ditentukan oleh kualitas regulasi, independensi pemeriksaan, penegakan,

transparansi, dan akses remediasi. Pada fase preventif dilakukan inventarisasi data, penilaian dampak, pengamanan berbasis risiko, pengujian berkala, tata kelola vendor, dan latihan respons insiden. Pada fase represif dilakukan preservasi bukti, investigasi independen, pemberitahuan, perintah korektif, dan sanksi proporsional. Pada fase restoratif disediakan informasi yang dapat dipahami, koreksi/penghapusan, pemantauan penyalahgunaan identitas jika relevan, kanal pengaduan, serta kompensasi melalui mekanisme yang dapat diakses.

Tabel 2. Model Akuntabilitas Berlapis

Lapisan	Aktor utama	Bukti yang harus tersedia	Hasil
Preventif	Pengendali/prosesor; Komdigi; BSSN; lembaga PDP	Inventaris data, DPIA, kontrol keamanan, audit/asesmen yang tepat, latihan insiden	Risiko diturunkan dan kepatuhan dapat diaudit
Represif	Lembaga PDP; BSSN; Komdigi; penegak hukum	Preservasi bukti, laporan forensik, notifikasi, keputusan korektif dan sanksi	Tanggung jawab ditetapkan berdasarkan bukti
Restoratif	Pengendali; lembaga PDP; pengadilan	Informasi korban, koreksi/penghapusan, kanal pengaduan, putusan/ganti rugi	Hak subjek data dipulihkan

Model ini menutup accountability gap karena setiap indikator memiliki penanggung jawab dan bukti kepatuhan. Ia juga menghindari dua ekstrem: menimpakan seluruh tanggung jawab kepada negara semata-mata karena kepemilikan BUMN, atau menyerahkan seluruh risiko kepada korporasi tanpa menguji kualitas pengawasan negara.

Kesimpulan

UU PDP bersama rezim PSE dan keamanan siber menyediakan fondasi pengawasan preventif, tetapi kewajiban harus dibaca menurut pasal yang tepat. Pasal 20 mengatur dasar pemrosesan; Pasal 34 penilaian dampak; Pasal 35–36 langkah dan tingkat keamanan; Pasal 39 pencegahan akses tidak sah; Pasal 46 notifikasi; Pasal 53 pejabat perlindungan data; Pasal 57 sanksi administratif; dan Pasal 58–60 kelembagaan. Fondasi tersebut belum otomatis menghasilkan pengawasan efektif apabila otoritas PDP belum operasional, kewenangan antarlembaga tidak dikoordinasikan, dan hasil pemeriksaan tidak cukup transparan.

Dugaan insiden MyPertamina tidak dapat diperlakukan sebagai kebocoran yang telah terbukti dari sistem Pertamina tanpa laporan forensik atau putusan berwenang. Status BUMN juga tidak otomatis mengatribusikan tindakan korporasi kepada negara menurut Article 4, 5, atau 8 ARSIWA. Tanggung jawab pengendali/prosesor harus diuji berdasarkan peran dan bukti pemrosesan, sementara kewajiban negara dinilai secara mandiri melalui fungsi regulasi, pengawasan, penegakan, dan pemulihan.

Kontribusi penelitian adalah model akuntabilitas berlapis yang memisahkan corporate/data-controller liability dari public supervisory responsibility dan menghubungkannya dengan fase preventif, represif, serta restoratif. Model ini

memungkinkan pemeriksaan yang lebih presisi, dapat diaudit, dan tidak bergantung pada asumsi bahwa kepemilikan negara identik dengan atribusi hukum.

Berdasarkan hasil penelitian, Penulis memberikan saran bahwa dalam jangka pendek, pemerintah perlu menetapkan aturan pelaksana dan mengoperasionalkan lembaga PDP dengan independensi fungsional, anggaran memadai, kewenangan pemeriksaan, serta publikasi ringkasan keputusan. Otoritas transisi perlu menerbitkan protokol bersama Komdigi–BSSN mengenai penerimaan laporan, preservasi bukti, pembagian pemeriksaan legal dan teknis, serta komunikasi kepada subjek data.

Pengendali data berskala besar, termasuk BUMN apabila memenuhi kriteria, perlu mendokumentasikan dasar pemrosesan, penilaian dampak, keputusan retensi, kontrol vendor, penunjukan pejabat perlindungan data, uji keamanan, dan latihan respons insiden. Audit atau asesmen harus mengikuti rezim yang tepat dan tidak menyamakan audit SPBE dengan audit aplikasi BUMN. Apabila kegagalan terbukti, pemulihan harus disesuaikan dengan risiko konkret: pemberitahuan yang jelas, dukungan koreksi data, pemantauan penyalahgunaan identitas bila relevan, kanal pengaduan, dan ganti rugi yang efektif.

Penelitian lanjutan perlu menggunakan pendekatan socio-legal setelah tersedia keputusan otoritas, laporan forensik, atau data pengaduan. Perbandingan kelembagaan dengan otoritas PDP negara lain juga perlu menilai independensi, kewenangan, prosedur banding, dan efektivitas pemulihan, bukan hanya menyalin struktur organisasi.

Referensi

- Aisya, Alyaziza. (2023), Tanggung Jawab Pemerintah Atas Kebocoran Data Pribadi Masyarakat dalam Perspektif Undang-undang Perlindungan Data Pribadi. <https://digilib.uin-palangkaraya.ac.id/6963/1/8>. HTN_ALYAZIZA AISYA_1902140066.pdf.
- Ananta, Wanda Vebya Ayu. (2026), Keamanan Siber Pemerintah Dan Aspek Hukum Administrasi Negara: Tanggung Jawab Administratif Dalam Perlindungan Sistem Informasi Publik di Era Digital. pp. 1–15, <https://lenterapublikasi.com/index.php/jah/article/view/133>.
- Ayiliani, Fanisa Mayda, and Elfia Farida. (2025), “Urgensi Pembentukan Lembaga Pengawas Data Pribadi Sebagai Upaya Perlindungan Hukum Terhadap Transfer Data Pribadi Lintas Negara.” *Jurnal Pembangunan Hukum Indonesia*, vol. 6, pp. 431–55, <https://ejournal2.undip.ac.id/index.php/jphi/article/view/23307>.
- Badan Siber dan Sandi Negara. (2020). Peraturan BSSN Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik.
- Badan Siber dan Sandi Negara. (2023). Peraturan BSSN Nomor 7 Tahun 2023 tentang Identifikasi Infrastruktur Informasi Vital.
- Badan Siber dan Sandi Negara. (2024a). Peraturan BSSN Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber.
- Badan Siber dan Sandi Negara. (2024b). Peraturan BSSN Nomor 8 Tahun 2024 tentang Standar dan Tata Cara Pelaksanaan Audit Keamanan Sistem Pemerintahan Berbasis Elektronik.
- Bahram, Muhammad. (2025), “Tanggung Jawab Konstitusional Pemerintah Dalam

- Menjamin Hak Konstitusional Atas Informasi di Era Digital.” *Jurnal Riset Ilmiah*, vol. 1, no. 01, pp. 15–18, <https://doi.org/10.62335%0AJurnal>.
- Berliant, Pratiwi, and Nikhlis Neilin. *Implementasi Prinsip Due Diligence Dalam Kewajiban Negara Mencegah Cyber Attacks: Tinjauan Hukum Internasional Kontemporer*. vol. 3, no. 2, 2025, pp. 72–92, <https://doi.org/10.51903/06adzb71>.
- Dr. Tedi Sudrajat, S.H., M , and M. Endra Wijaya, S.H. (2020), “Perlindungan Hukum Terhadap Tindakan Pemerintah.” *LIBEROSIS: Jurnal Psikologi Dan Bimbingan Konseling*, vol. 8, no. 2, pp. 96–161, <https://www.google.com/books?hl=id&lr=&id=zbAfEAAQBAJ&oi=fnd&pg=PR1&dq=sudrajat+tindakan+pemerintah&ots=qQHPMWLNWW&sig=nbeetTZlGcOeZULYcop654E6i6Y>.
- European Parliament and Council. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union, L 119.
- Fazila, Raysha Aulia. *Penguatan Perlindungan Data Pribadi Sebagai Upaya*. 2022, pp. 1–12, https://www.researchgate.net/profile/Raysha-Fazila/publication/398410417_PENGUATAN_PERLINDUNGAN_DATA_PRIIBADI_SEBAGAI_UPAYA_PENCEGAHAN_SOCIAL_ENGINEERING_DI_INDONESIA/links/69343fbd06a9ab54f844a399/PENGUATAN-PERLINDUNGAN-DATA-PRIIBADI-SEBAGAI-UPAYA-PENCEGAH.
- Huda, nurul uu, et al. “Data Pribadi, Hak Warga, Dan Negara Hukum: Menjaga Privasi Di Tengah Ancaman Digital.” *Widina Media Utama*, 2024, p. 143, <https://repository.penerbitwidina.com/publications/588510/data-pribadi-hak-wargadan-negara-hukum-menjaga-privasi-di-tengah-ancaman-digita>.
- I Nengah Sudiarta. “Pengaturan Hak Asasi Manusia Dalam Sistem Hukum Nasional.” *IJOLARES: Indonesian Journal of Law Research*, vol. 2, no. 1, 2024, pp. 25–31, <https://doi.org/10.60153/ijolares.v2i1.44>.
- International Law Commision. Draft Articles on Responsibility of States for Internationally Wrongful Acts (2001). Report of the International Law Commission on the work of its fifty-third session, UN GAOR, 56th Sess, Supp No 10, UN Doc A/56/10, 2001, p. 43, https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf.
- International Law Commission. (2001). Draft articles on responsibility of states for internationally wrongful acts, with commentaries. Yearbook of the International Law Commission, 2001(II, Part Two). United Nations.
- Kaharuddin, Kaharuddin, et al. “Urgensi Penerapan UU PDP Nomor 27 Tahun 2022 Dalam Pertanggungjawaban Hukum Atas Kasus Kebocoran Data NPWP.” *Takuana: Jurnal Pendidikan, Sains, Dan Humaniora*, vol. 4, nos. 3 SE-Articles, Dec. 2025, pp. 876–87, <https://doi.org/10.56113/takuana.v4i3.249>.
- Kartika, Shanti Dwi, and Noverdi Puja Saputra. “Tanggung Jawab Negara Dalam Penanganan Aset Tindak Pidana.” 2021, pp. 1–5, <https://www.google.com/books?hl=id&lr=&id=3BIQEAAAQBAJ&oi=fnd&pg=PA1&dq=kartika+tanggung+jawab&ots=4FHkqISRdb&sig=ZVF22rwPyF2q2uVEsaCqX9DnmXy>.
- Locke, John. *Two Treatises of Government*. Awnsham Churchill, 1689, <https://www.yorku.ca/comninel/courses/3025pdf/Locke.pdf>.
- Mahkamah Konstitusi Republik Indonesia. (2025). Putusan Nomor 151/PUU-XXII/2024.
- Makkuaseng, A. Syamrullah. *Kewenangan Badan Siber Dan Sandi Negara Dalam*

- Mengawasi Keamanan Kegiatan Ekonomi Berbasis Elektronik*. 2023, pp. 1–42, <https://repository.unhas.ac.id/id/eprint/30379/>.
- Marzuki, P. M. (2017). *Penelitian hukum* (edisi revisi). Kencana.
- Marzuki, Peter Mahmud. (2017), *Penelitian Hukum Normatif: Edisi Revisi*. Jakarta: Kencana, Prenada Media, <https://books.google.co.id/books?id=CKZADwAAQBAJ&printsec=copyright>.
- Mudrajat, Kuncoro, et al. *Transformasi Pertamina: Dilema Antara Orientasi Bisnis & Pelayanan Publik*. Galangpress Group, 2009, [https://www.google.com/books?hl=id&lr=&id=VS7M1QisNv0C&oi=fnd&pg=PA127&dq=Dalam+konteks+kasus+MyPertamina,+konstruksi+tanggung+jawab+negara+menghadapi+tantangan+normatif+karena+PT+Pertamina+\(Persero\)+berstatus+sebagai+BUMN+yang+secara+yuridis+merupakan+ba](https://www.google.com/books?hl=id&lr=&id=VS7M1QisNv0C&oi=fnd&pg=PA127&dq=Dalam+konteks+kasus+MyPertamina,+konstruksi+tanggung+jawab+negara+menghadapi+tantangan+normatif+karena+PT+Pertamina+(Persero)+berstatus+sebagai+BUMN+yang+secara+yuridis+merupakan+ba).
- Nasruddin, Nadya Annisa, et al. (2023), *The Role of Technology in Detecting Cyber Risk and Improving Internal Audit: A Systematic Review*. vol. 18, no. 2, pp. 173–83, <https://doi.org/10.37058/jak.v18i2.7675>.
- Pemerintah Pusat. “Undang-Undang (UU) Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.” *Pemerintah Pusat*, no. 016999, 2022, p. 1, [https://peraturan.bpk.go.id/Download/224884/UU Nomor 27 Tahun 2022.pdf](https://peraturan.bpk.go.id/Download/224884/UU%20Nomor%2027%20Tahun%2022.pdf).
- Pemerintah Republik Indonesia. (1945). *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*.
- Pemerintah Republik Indonesia. (2019). *Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik*.
- Pemerintah Republik Indonesia. (2022a). *Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital*.
- Pemerintah Republik Indonesia. (2022b). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*.
- Pemerintah Republik Indonesia. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.
- Radika Hanny Syah, and Muhammad Irwan Padli Nasution. “Analisis Keamanan Siber Dan Hukum: Studi Kasus Bjorka.” *Jurnal Ilmiah Ekonomi, Manajemen, Bisnis Dan Akuntansi*, vol. 2, no. 3, 2025, pp. 329–38, <https://doi.org/10.61722/jemba.v2i3.948>.
- Rahayu Lestari, Chery, et al. “Analisis Tingkat Kepatuhan Pengelolaan Data Pribadi Pengguna Terhadap Undang-Undang Perlindungan Data Pribadi (UU PDP) Pada Platform Digital.” *Adagium: Jurnal Ilmiah Hukum*, vol. 4, no. 1, 2026, pp. 146–68, <https://doi.org/10.70308/adagium.v4i1.279>.
- Rahman, Faiz. *KERANGKA HUKUM PERLINDUNGAN DATA PRIBADI DALAM PENERAPAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI INDONESIA*. 2021, https://www.researchgate.net/profile/Faiz-Rahman-6/publication/350648863_Kerangka_Hukum_Perlindungan_Data_Pribadi_dalam_Penerapan_Sistem_Pemerintahan_Berbasis_Elektronik_di_Indonesia/links/606bfb492851c91b1a6db22/Kerangka-Hukum-Perlindungan-Data-Pribadi-dalam-Penerapan-Sistem-Pemerintahan-Berbasis-Elektronik-di-Indonesia.pdf.
- Sane, Mardiman, et al. *REGULATIONS IN DIGITAL SERVICES IN INDONESIA: ASYSTEMATIC*. vol. 6, no. 12, 2026, pp. 1–25, <https://www.ojs.rewangrencang.com/index.php/JHLG/article/view/3170>.

- Silaen, Mangaraja Gideon, and Men Wih Widiatno. *Jurnal Impresi Indonesia (JII) Tanggung Jawab Mutlak Pengendali Data Akibat Kebocoran Data Pribadi Di Aplikasi Mypertamina*. vol. 5, no. 3, 2026, pp. 1259–74, <https://jii.rivierapublishing.id/index.php/jii/article/download/7569/1360>.
- Silawati, D., et al. (2025). Urgensi pembentukan lembaga pengawas dalam pembaharuan hukum perlindungan data pribadi menurut Undang-Undang PDP. *Locus Journal of Academic Literature Review*, 4(2), 106–113.
- Silawati, Dayang, et al. “Urgensi Pembentukan Lembaga Pengawas Dalam Pembaharuan Hukum Perlindungan Data Pribadi Menurut Undang-Undang PDP.” *Locus Journal of Academic Literature Review*, vol. 4, no. 2, 2025, pp. 106–13, <https://jurnal.locusmedia.id/index.php/jalr/article/download/433/259>.
- Siti Maesaroh, Risma. “Tantangan Keamanan Siber Dan Implikasinya Terhadap Hukum Kenegaraan: Tinjauan Atas Peran Negara Dalam Menjamin Ketahanan Digital.” *Staatsrecht: Jurnal Hukum Kenegaraan Dan Politik Islam*, vol. 4, no. 2, 2025, pp. 255–74, <https://doi.org/10.14421/3n8bxw79>.
- Vania, C., Markoni, M., & Disemadi, H. S. (2023). Tinjauan yuridis terhadap perlindungan data pribadi dari aspek pengamanan data dan keamanan siber. *Jurnal Multidisiplin Indonesia*, 2(3), 654–666. <https://doi.org/10.58344/jmi.v2i3.157>
- Vania, Cindy, et al. (2023), “Tinjauan Yuridis Terhadap Perlindungan Data Pribadi Dari Aspek Pengamanan Data Dan Keamanan Siber.” *Jurnal Multidisiplin Indonesia*, vol. 2, no. 3, pp. 654–66, <https://doi.org/10.58344/jmi.v2i3.157>.
- Veliz, Carissa. (2021), “Privacy Is Power, Why and How You Should Take Back Control of Your Data.” <https://cdn.penguin.co.uk/dam-assets/books/9780552177719/9780552177719-%0Asample.pdf>.
- Zelafiara, Ega. (2022). *KEBIJAKAN FORMULASI TERHADAP KEBOCORAN DATA PRIBADI BERDASARKAN RANCANGAN UNDANG-UNDANG PERLINDUNGAN DATA PRIBADI*. <https://digilib.unila.ac.id/64406/>.