

Tanggung Jawab Konstitusional Negara terhadap Perlindungan Data Pribadi Warga dalam Penyelenggaraan Pemerintahan Digital

Wiredarne

wiredarne@ipdn.ac.id

Institut Pemerintahan Dalam Negeri

Abstrak - Penelitian ini bertujuan untuk menganalisis kedudukan data pribadi sebagai bagian dari hak konstitusional warga negara dalam penyelenggaraan pemerintahan digital serta merumuskan tanggung jawab konstitusional negara dalam menjamin perlindungan data pribadi. Penelitian ini menggunakan metode kualitatif dengan jenis penelitian yuridis normatif. Pendekatan yang digunakan meliputi pendekatan perundang-undangan, pendekatan konseptual, dan pendekatan kasus normatif-kontekstual. Sumber data penelitian terdiri atas bahan hukum primer, sekunder, dan tersier yang dikumpulkan melalui studi kepustakaan. Analisis dilakukan secara kualitatif-preskriptif melalui interpretasi hukum dan penalaran hukum. Hasil penelitian menunjukkan bahwa data pribadi warga negara tidak dapat dipahami hanya sebagai informasi administratif, melainkan sebagai bagian dari hak konstitusional yang berkaitan dengan hak atas privasi, hak atas rasa aman, martabat, dan perlindungan diri pribadi. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah memberikan dasar normatif untuk menghubungkan perlindungan data pribadi dengan jaminan hak konstitusional subjek data. Akan tetapi, dalam pemerintahan digital, negara tidak cukup hanya berperan sebagai regulator, tetapi juga sebagai pengendali data, penyelenggara layanan digital, pengawas, dan penjamin pemulihan hak warga negara. Penelitian ini menawarkan lima parameter tanggung jawab konstitusional negara, yaitu legalitas pemrosesan data, pembatasan tujuan, keamanan sistem, transparansi akses subjek data, dan pemulihan hak. Temuan ini menegaskan perlunya penguatan akuntabilitas konstitusional dalam tata kelola data pribadi pada pemerintahan digital.

Kata kunci: data pribadi; hak konstitusional; pemerintahan digital; tanggung jawab negara; UU Pelindungan Data Pribadi.

Abstract - This study aims to analyze the position of personal data as part of citizens' constitutional rights in the implementation of digital government and to formulate the constitutional responsibility of the state in ensuring personal data protection. This research uses a qualitative method with a normative juridical approach. The study applies statutory, conceptual, and normative-contextual case approaches. The data sources consist of primary, secondary, and tertiary legal materials collected through library research. The analysis is conducted qualitatively and prescriptively through legal interpretation and legal reasoning. The findings show that citizens' personal data cannot be understood merely as administrative information, but must be positioned as part of constitutional rights related to privacy, security, dignity, and personal protection. Law Number 27 of 2022 on Personal Data Protection provides a normative basis for linking personal data protection with the guarantee of the constitutional rights of data subjects. In the context of digital government, the state does not only act as a regulator, but also as a data controller, digital service provider, supervisory actor, and guarantor of citizens' rights recovery. This study proposes five parameters of the state's constitutional responsibility: legality of data processing, purpose limitation, system security, transparency and access for data subjects, and rights recovery. The findings imply that personal data governance in digital government must move beyond administrative compliance toward stronger constitutional accountability in protecting citizens' rights.

Keywords: personal data; constitutional rights; digital government; state responsibility; Personal Data Protection Law.

1. Pendahuluan

Transformasi pemerintahan digital telah mengubah cara negara menyelenggarakan pelayanan publik, mengambil keputusan administratif, dan membangun relasi dengan warga negara. Layanan kependudukan, kesehatan, pendidikan, perpajakan, bantuan sosial, perizinan, pengaduan masyarakat, serta sistem identitas digital kini menempatkan data pribadi sebagai prasyarat utama dalam akses pelayanan publik. Dalam konteks tersebut, data pribadi tidak lagi dapat dipahami semata-mata sebagai informasi administratif yang dikumpulkan oleh negara, melainkan sebagai bagian dari hak konstitusional warga negara yang melekat pada martabat, keamanan, dan perlindungan diri pribadi. Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 menjamin hak setiap orang atas

perlindungan diri pribadi, keluarga, kehormatan, martabat, harta benda, serta hak atas rasa aman dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu. Jaminan tersebut memperoleh relevansi baru dalam penyelenggaraan pemerintahan digital karena setiap proses pengumpulan, perekaman, penyimpanan, pemadanan, pengolahan, dan pembagian data warga negara dapat berdampak langsung terhadap privasi, keamanan, dan akses warga terhadap hak-hak publik. Perlindungan data pribadi pada akhirnya harus ditempatkan sebagai bagian dari kewajiban konstitusional negara, bukan sekadar isu teknis dalam tata kelola sistem elektronik pemerintahan (Beduschi, 2021; Santana & Ansari, 2023; Republik Indonesia, 1945; Republik Indonesia, 2022).

Permasalahan utama dalam pemerintahan digital terletak pada menguatnya ketergantungan negara terhadap data warga negara, sementara posisi warga sering kali tidak setara dengan pemerintah sebagai penyedia layanan dan pengendali sistem. Dalam layanan publik, warga negara umumnya tidak memiliki pilihan yang bebas untuk menolak pemberian data karena akses terhadap pelayanan administratif, bantuan sosial, pendidikan, kesehatan, atau dokumen kependudukan sering bergantung pada pemrosesan data pribadi. Relasi yang tidak seimbang tersebut membedakan pemrosesan data oleh negara dari pemrosesan data oleh sektor privat, karena negara memiliki kewenangan publik yang bersifat memaksa dan berdampak langsung terhadap pemenuhan hak warga. Risiko kebocoran data, pemrosesan berlebihan, penggunaan data di luar tujuan awal, lemahnya keamanan sistem, dan minimnya transparansi algoritmik dapat menimbulkan kerugian konstitusional yang tidak selalu mudah dipulihkan. Dalam perspektif tata kelola data sektor publik, persoalan tersebut menuntut kejelasan tanggung jawab negara sebagai pembentuk regulasi, pengendali data, penyelenggara layanan, dan penjamin hak asasi manusia (Anand & Brass, 2021; Buttow & Weerts, 2024; Rahman, 2025; van Donge et al., 2022).

Kehadiran Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi merupakan langkah penting dalam memperkuat kerangka hukum pelindungan data pribadi di Indonesia. Undang-undang ini secara eksplisit mendefinisikan pelindungan data pribadi sebagai keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data guna menjamin hak konstitusional subjek data pribadi. Formulasi tersebut memperlihatkan bahwa pelindungan data pribadi bukan hanya instrumen hukum administratif, melainkan juga mekanisme pemenuhan hak konstitusional. Persoalan yang muncul adalah bagaimana negara harus dimintai pertanggungjawaban ketika sistem pemerintahan digital gagal melindungi data pribadi warga, terutama ketika data tersebut digunakan dalam pelayanan publik yang bersifat wajib, luas, dan berkelanjutan. Negara tidak cukup hanya menyediakan regulasi, karena Pasal 28I ayat (4) UUD 1945 menegaskan bahwa perlindungan, pemajuan, penegakan, dan pemenuhan hak asasi manusia merupakan tanggung jawab negara, terutama pemerintah. Kerangka tersebut menempatkan pemerintah pada posisi konstitusional yang lebih kuat untuk memastikan bahwa setiap pemrosesan data pribadi dalam pemerintahan digital tunduk pada prinsip legalitas, akuntabilitas, keamanan, proporsionalitas, transparansi, dan pemulihan hak warga negara (Badriah et al., 2024; Kurniawan et al., 2024; Syailendra et al., 2024; Widiatedja & Mishra, 2023; Yuspin et al., 2024).

Kajian terdahulu telah membahas perlindungan data pribadi dari berbagai sudut pandang. Fauzy dan Shandy (2022) menempatkan hak atas privasi sebagai dasar politik hukum pembentukan UU PDP, terutama dalam kaitannya dengan jaminan konstitusional Pasal 28G ayat (1) UUD 1945. Rosadi et al. (2023) menilai bahwa pengaturan perlindungan data pribadi di Indonesia perlu menjawab kebutuhan ekonomi digital, termasuk kepastian hukum bagi subjek data dan pelaku pemrosesan data. Widiatedja dan Mishra (2023) menekankan pentingnya pembentukan otoritas perlindungan data yang independen agar pengawasan terhadap pemrosesan data tidak bergantung sepenuhnya pada institusi pemerintah yang juga dapat menjadi pengendali data. Syailendra et al. (2024) menguraikan tantangan dan peluang pelaksanaan UU PDP setelah pengesahannya, terutama berkaitan dengan efektivitas kelembagaan, kesiapan pengendali data, dan penegakan hukum. Wibowo et al. (2024) melihat perlindungan data pribadi sebagai faktor penting dalam pembangunan ekonomi digital, karena kepercayaan publik terhadap ekosistem digital sangat dipengaruhi oleh keamanan dan kepastian hukum data pribadi. Yuspin et al. (2023) membahas perlindungan data pribadi dalam tata kelola perbankan digital, sedangkan Rahman dan Mulyani (2025) mengkaji tantangan transfer data lintas batas setelah pengesahan UU PDP. Kurniawan et al. (2024) menyoroti peran sanksi pidana dalam perlindungan data pribadi, Rahmatullah et al. (2024) mengaitkan UU PDP dengan pengelolaan data dalam tata kelola zakat, dan Yuspin et al. (2024) membahas prinsip akuntabilitas dalam pengawasan perlindungan data pribadi. Kumpulan studi tersebut menunjukkan bahwa perlindungan data pribadi telah menjadi isu lintas sektor, tetapi pembahasannya masih banyak terfokus pada aspek regulasi, kelembagaan, sektor ekonomi, sanksi, dan kepatuhan teknis.

Kajian lain yang berkaitan dengan pemerintahan digital menunjukkan bahwa perlindungan data pribadi berkaitan erat dengan kepercayaan publik, tata kelola data, dan kualitas pelayanan negara. Rahman (2025) secara khusus menunjukkan bahwa pemrosesan data pribadi oleh sektor publik memiliki karakter yang berbeda karena pengumpulan data oleh negara sering bersifat wajib dan melekat pada akses pelayanan publik. Marwenny et al. (2024) menegaskan bahwa perlindungan data dalam pelayanan publik membutuhkan partisipasi masyarakat, kesiapan institusi, dan kepastian tanggung jawab penyelenggara layanan. Badriah et al. (2024) membandingkan akuntabilitas kebijakan perlindungan data pribadi di Indonesia dengan Korea Selatan dan Singapura, lalu menekankan pentingnya pembelajaran kelembagaan bagi Indonesia. Dalam literatur tata kelola digital, van Donge et al. (2022) menjelaskan pentingnya data stewardship dalam ekosistem data pemerintah, sedangkan Schmeling et al. (2025) menempatkan kolaborasi data sebagai agenda penting dalam riset pemerintahan digital. Buttow dan Weerts (2024) serta Buttow (2025) memperlihatkan bahwa pengelolaan data sektor publik memerlukan model tata kelola yang mampu mengendalikan risiko regulasi, kualitas data, dan dampak kebijakan berbasis data. Kanaan et al. (2023), Shayganmehr et al. (2023), dan Li dan Xue (2021) memperkuat argumen bahwa keamanan, privasi, kepercayaan, dan risiko merupakan variabel penting dalam penerimaan layanan e-government. Beduschi (2021) dan Anand dan Brass (2021) menambahkan bahwa sistem identitas digital harus dibangun dengan memperhatikan privasi, hak asasi manusia, dan prinsip inovasi yang bertanggung jawab. Studi-studi tersebut relevan bagi penelitian ini karena memperlihatkan bahwa pemerintahan digital tidak

hanya membutuhkan efisiensi teknologi, tetapi juga fondasi konstitusional yang menjamin perlindungan hak warga negara.

Berangkat dari peta kajian tersebut, penelitian ini mengambil posisi yang berbeda dengan menempatkan perlindungan data pribadi warga sebagai bagian dari tanggung jawab konstitusional negara dalam penyelenggaraan pemerintahan digital. Penelitian terdahulu telah banyak membahas UU PDP dari aspek privasi, ekonomi digital, sanksi, transfer data lintas batas, otoritas pengawas, pelayanan publik, dan tata kelola data, tetapi belum secara spesifik membangun argumentasi mengenai hubungan antara UU PDP dan kewajiban konstitusional negara untuk menjamin hak privasi, hak atas rasa aman, serta perlindungan diri pribadi sebagaimana dijamin dalam UUD 1945. Kebaruan penelitian ini terletak pada upaya merumuskan konstruksi tanggung jawab konstitusional negara ketika pemerintah bertindak sebagai regulator, pengendali data, pemroses data, penyedia layanan digital, sekaligus penjamin hak warga negara. Penelitian ini bertujuan untuk menganalisis kedudukan data pribadi sebagai bagian dari hak konstitusional warga dalam layanan pemerintahan digital, mengkaji implikasi UU PDP terhadap kewajiban negara dalam menjamin privasi dan keamanan data warga, serta merumuskan parameter pertanggungjawaban konstitusional negara atas kegagalan perlindungan data pribadi dalam penyelenggaraan pemerintahan digital.

2. Metode penelitian

Penelitian ini menggunakan **metode kualitatif dengan jenis penelitian yuridis normatif atau doctrinal legal research**. Penelitian ini tidak menggunakan metode kuantitatif, mix method, survei statistik, eksperimen, maupun algoritma komputasional tertentu seperti machine learning atau text mining. Pilihan metode kualitatif yuridis normatif digunakan karena fokus utama penelitian ini adalah menganalisis norma hukum, prinsip konstitusional, kewajiban negara, dan konstruksi pertanggungjawaban pemerintah dalam perlindungan data pribadi warga negara pada penyelenggaraan pemerintahan digital. Objek utama penelitian bukan perilaku responden, melainkan norma hukum positif, prinsip hak konstitusional, serta hubungan antara Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Melalui metode ini, penelitian diarahkan untuk menelaah apakah perlindungan data pribadi dalam pemerintahan digital telah dapat diposisikan sebagai bagian dari tanggung jawab konstitusional negara dalam menjamin hak privasi, hak atas rasa aman, dan perlindungan diri pribadi warga negara.

Pendekatan yang digunakan dalam penelitian ini terdiri atas **pendekatan perundang-undangan, pendekatan konseptual, dan pendekatan kasus normatif-kontekstual**. Pendekatan perundang-undangan digunakan untuk menelaah norma-norma hukum yang mengatur perlindungan data pribadi, hak konstitusional warga negara, pelayanan publik digital, administrasi pemerintahan, dan sistem pemerintahan berbasis elektronik. Pendekatan konseptual digunakan untuk menjelaskan konsep data pribadi sebagai bagian dari hak konstitusional, konsep tanggung jawab negara, konsep privasi, konsep keamanan data, serta konsep pemerintahan digital. Pendekatan kasus normatif-kontekstual digunakan untuk membaca persoalan perlindungan data pribadi dalam praktik penyelenggaraan layanan pemerintahan

digital di Indonesia, terutama ketika pemerintah bertindak sebagai pengendali data, pemroses data, penyedia layanan digital, sekaligus penjamin hak warga negara. Pendekatan ini dipilih agar analisis tidak berhenti pada uraian norma, tetapi juga mampu menjelaskan implikasi hukum ketika data pribadi warga digunakan dalam layanan publik berbasis sistem elektronik.

Studi kasus dalam penelitian ini difokuskan pada **penyelenggaraan pemerintahan digital di Indonesia setelah berlakunya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi**. Studi kasus tersebut bersifat normatif, bukan studi kasus empiris pada satu instansi tertentu. Fokus kasus diarahkan pada situasi ketika data pribadi warga negara dikumpulkan, disimpan, dipadankan, diproses, dan digunakan dalam layanan pemerintahan digital, seperti layanan administrasi kependudukan, bantuan sosial, kesehatan, pendidikan, perizinan, perpajakan, layanan pengaduan, dan sistem identitas digital. Pemilihan studi kasus ini didasarkan pada pertimbangan bahwa layanan pemerintahan digital merupakan ruang paling relevan untuk menguji hubungan antara kewajiban negara dan hak konstitusional warga negara. Dalam layanan tersebut, warga sering berada dalam posisi yang tidak seimbang karena pemberian data pribadi menjadi syarat untuk memperoleh pelayanan publik. Kondisi ini memperkuat kebutuhan untuk menilai tanggung jawab konstitusional negara ketika terjadi kebocoran data, penyalahgunaan data, pemrosesan data yang tidak transparan, atau penggunaan data di luar tujuan pelayanan publik.

Sumber data dalam penelitian ini terdiri atas **bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier**. Bahan hukum primer meliputi Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, terutama Pasal 28G ayat (1), Pasal 28H ayat (4), dan Pasal 28I ayat (4); Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi; Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik; Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan; Undang-Undang Nomor 11 Tahun 2008 beserta perubahannya tentang Informasi dan Transaksi Elektronik; Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik; serta peraturan teknis lain yang relevan dengan penyelenggaraan pemerintahan digital dan pelindungan data pribadi. Bahan hukum sekunder meliputi artikel jurnal ilmiah bereputasi, buku akademik, hasil penelitian, laporan kebijakan, dan publikasi ilmiah yang membahas pelindungan data pribadi, hak privasi, digital government, data governance, cybersecurity, constitutional rights, dan public sector data protection. Bahan hukum tersier digunakan untuk memperjelas istilah hukum dan konsep teknis, seperti kamus hukum, ensiklopedia hukum, glosarium kebijakan digital, serta sumber penunjang akademik lainnya.

Pengumpulan data dilakukan melalui **studi kepustakaan atau library research** dengan teknik dokumentasi. Data dikumpulkan dengan cara menelusuri, memilih, membaca, dan mengklasifikasi bahan hukum serta literatur ilmiah yang relevan dengan fokus penelitian. Literatur ilmiah dipilih secara purposive berdasarkan beberapa kriteria, yaitu terbit dalam lima tahun terakhir, memiliki relevansi langsung dengan pelindungan data pribadi atau pemerintahan digital, diterbitkan oleh jurnal yang dapat ditelusuri secara akademik, memiliki DOI aktif, dan memuat pembahasan yang dapat mendukung analisis

tentang hak konstitusional serta tanggung jawab negara. Kata kunci yang digunakan dalam penelusuran literatur meliputi *personal data protection*, *constitutional right to privacy*, *digital government*, *public sector data governance*, *data protection authority*, *privacy rights*, *e-government trust*, *public service digitalization*, dan *state responsibility*. Literatur yang terkumpul kemudian dipilah berdasarkan tema, yaitu hak konstitusional atas privasi, tanggung jawab negara, tata kelola data sektor publik, keamanan data dalam layanan pemerintahan, dan akuntabilitas pemerintah dalam pemrosesan data pribadi.

Analisis data dilakukan secara **kualitatif-preskriptif** melalui analisis isi hukum, interpretasi norma, dan penalaran hukum. Analisis isi hukum digunakan untuk mengidentifikasi substansi norma dalam UUD 1945, UU PDP, dan regulasi pemerintahan digital. Interpretasi gramatikal digunakan untuk memahami makna tekstual norma perlindungan data pribadi dan hak konstitusional. Interpretasi sistematis digunakan untuk menghubungkan UU PDP dengan UUD 1945, hukum administrasi pemerintahan, pelayanan publik, dan sistem pemerintahan berbasis elektronik. Interpretasi teleologis digunakan untuk membaca tujuan perlindungan data pribadi sebagai instrumen jaminan hak konstitusional warga negara. Penalaran hukum kemudian diarahkan untuk merumuskan parameter tanggung jawab konstitusional negara, terutama ketika pemerintah gagal menjamin keamanan data, transparansi pemrosesan, pembatasan tujuan, akuntabilitas pengendali data, dan pemulihan hak subjek data dalam layanan pemerintahan digital.

Validitas data dalam penelitian ini dijaga melalui **triangulasi sumber hukum dan literatur ilmiah**. Norma dalam UUD 1945 dan UU PDP tidak dibaca secara terpisah, tetapi dibandingkan dengan regulasi pelayanan publik, administrasi pemerintahan, SPBE, dan temuan penelitian terdahulu. Literatur yang digunakan juga diperiksa berdasarkan kesesuaian tema, kejelasan sumber, keterlacakan DOI, dan relevansi substansial terhadap isu perlindungan data pribadi. Validasi dilakukan dengan memastikan bahwa setiap argumentasi hukum memiliki dasar normatif dan dukungan akademik yang memadai. Melalui tahapan tersebut, penelitian ini diharapkan mampu menghasilkan analisis yang tidak hanya deskriptif, tetapi juga preskriptif, yaitu menawarkan rumusan tanggung jawab konstitusional negara dalam melindungi data pribadi warga negara pada penyelenggaraan pemerintahan digital.

3. Hasil dan Pembahasan

a. Data Pribadi sebagai Bagian dari Hak Konstitusional Warga Negara dalam Pemerintahan Digital

Hasil penelitian menunjukkan bahwa data pribadi warga negara dalam penyelenggaraan pemerintahan digital memiliki kedudukan yang lebih tinggi daripada sekadar data administratif. Data pribadi merupakan bagian dari hak konstitusional karena berkaitan langsung dengan perlindungan diri pribadi, martabat, kehormatan, rasa aman, dan kebebasan warga negara dari tindakan sewenang-wenang dalam pemrosesan informasi pribadi. Posisi ini dapat ditarik dari Pasal 28G ayat (1) UUD 1945 yang menjamin hak setiap orang atas perlindungan diri pribadi, keluarga, kehormatan, martabat, harta benda, serta rasa aman. Kedudukan tersebut diperkuat oleh UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi yang secara eksplisit menyatakan bahwa perlindungan data pribadi bertujuan menjamin hak konstitusional subjek data pribadi. UU PDP juga mengatur jenis data pribadi, hak subjek data, kewajiban

pengendali dan prosesor, transfer data, sanksi administratif, kelembagaan, penyelesaian sengketa, larangan penggunaan data pribadi, serta ketentuan pidana.

Temuan tersebut memperlihatkan bahwa hak atas perlindungan data pribadi tidak dapat dilepaskan dari hak atas privasi dan hak atas rasa aman. Dalam pemerintahan digital, warga negara menyerahkan data pribadi karena membutuhkan pelayanan publik, bukan karena berada dalam posisi tawar yang sepenuhnya bebas. Data kependudukan, data biometrik, data kesehatan, data pendidikan, data perpajakan, data bantuan sosial, dan data layanan publik lainnya diproses oleh pemerintah sebagai syarat akses terhadap hak-hak administratif. Kondisi tersebut menempatkan negara dalam relasi yang dominan karena warga negara tidak selalu dapat menolak pemrosesan data tanpa kehilangan akses terhadap pelayanan publik. Temuan ini sejalan dengan Rahman (2025), yang menegaskan bahwa pemrosesan data pribadi oleh sektor publik memiliki karakter khusus karena pengumpulan data oleh negara sering bersifat wajib dan melekat pada layanan publik.

Posisi data pribadi sebagai hak konstitusional juga membedakan tanggung jawab negara dari tanggung jawab korporasi digital. Ketika perusahaan swasta memproses data pribadi, hubungan hukum umumnya berangkat dari relasi kontraktual, persetujuan pengguna, dan kepentingan bisnis. Dalam pemerintahan digital, relasi hukum bersumber dari kewenangan publik dan fungsi negara sebagai penyelenggara pelayanan. Perbedaan ini membuat pelanggaran data pribadi oleh pemerintah tidak hanya berdampak pada kerugian individual, tetapi juga dapat menimbulkan kerugian konstitusional. Kebocoran data, pemadanan data yang keliru, penggunaan data di luar tujuan pelayanan, atau pembukaan akses data tanpa dasar hukum yang jelas dapat merugikan martabat, keamanan, dan kepercayaan warga negara terhadap negara. Beduschi (2021) juga menekankan bahwa sistem identitas digital harus dibaca melalui perspektif hak asasi manusia karena identitas digital dapat menentukan akses seseorang terhadap layanan, mobilitas, dan pengakuan hukum.

Analisis ini memperluas kajian Fauzy dan Shandy (2022) yang menempatkan hak atas privasi sebagai dasar politik hukum UU PDP. Penelitian ini tidak hanya melihat privasi sebagai hak individual, tetapi juga sebagai hak konstitusional yang menimbulkan kewajiban aktif negara dalam penyelenggaraan pemerintahan digital. Kajian Wibowo et al. (2024) menekankan pentingnya perlindungan data pribadi bagi pembangunan ekonomi digital, sedangkan penelitian ini menempatkan perlindungan data pribadi dalam konteks pelayanan publik dan kewajiban konstitusional pemerintah. Perbedaan tersebut penting karena kerugian akibat pelanggaran data pribadi dalam layanan pemerintahan tidak selalu dapat diukur melalui kerugian ekonomi. Kerugian dapat muncul dalam bentuk hilangnya rasa aman, ketidakpastian hukum, diskriminasi administratif, pembatasan akses layanan, dan melemahnya kepercayaan warga terhadap negara.

b. Kewajiban Negara sebagai Regulator, Pengendali Data, dan Penyelenggara Layanan Digital

Hasil penelitian menemukan bahwa negara memiliki tiga posisi utama dalam perlindungan data pribadi warga pada pemerintahan digital, yaitu sebagai regulator, pengendali data, dan penyelenggara

layanan publik berbasis elektronik. Sebagai regulator, negara wajib membentuk norma hukum yang memberikan kepastian, batas kewenangan, mekanisme pengawasan, sanksi, dan pemulihan hak bagi subjek data. Sebagai pengendali data, pemerintah wajib memastikan bahwa setiap pemrosesan data pribadi dilakukan berdasarkan dasar hukum yang sah, tujuan yang jelas, prinsip proporsionalitas, keamanan sistem, dan akuntabilitas kelembagaan. Sebagai penyelenggara layanan digital, pemerintah wajib menjamin bahwa sistem elektronik pemerintahan tidak merugikan hak konstitusional warga negara. Perpres Nomor 95 Tahun 2018 menempatkan SPBE sebagai penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.

Temuan tersebut menunjukkan bahwa tanggung jawab negara dalam UU PDP tidak cukup dipahami sebagai tanggung jawab administratif biasa. Ketika pemerintah mengumpulkan dan memproses data pribadi dalam layanan publik, pemerintah tidak hanya menjalankan fungsi teknis, tetapi juga menjalankan kewajiban konstitusional. Kewajiban tersebut meliputi perlindungan terhadap hak privasi, hak atas rasa aman, dan perlindungan diri pribadi sebagaimana dijamin UUD 1945. Negara wajib memastikan bahwa data pribadi warga tidak digunakan secara berlebihan, tidak disebarluaskan tanpa dasar hukum, tidak diproses untuk tujuan yang menyimpang, dan tidak dikelola oleh sistem yang rentan terhadap kebocoran. Dalam konteks ini, prinsip akuntabilitas dalam UU PDP harus diterjemahkan ke dalam tata kelola pemerintahan digital yang konkret, mulai dari desain sistem, pembatasan akses internal, audit keamanan, penilaian dampak perlindungan data, dokumentasi pemrosesan, sampai mekanisme pengaduan warga.

Temuan ini memiliki keterkaitan dengan studi Syailendra et al. (2024) yang menyatakan bahwa pelaksanaan UU PDP menghadapi tantangan kelembagaan, kesiapan pengendali data, dan efektivitas penegakan hukum. Penelitian ini memperdalam temuan tersebut dengan menegaskan bahwa tantangan kelembagaan dalam pemerintahan digital harus dibaca sebagai persoalan konstitusional. Jika lembaga pemerintah tidak mampu menjaga keamanan data warga, persoalan tersebut bukan hanya kelemahan manajerial, melainkan potensi kegagalan negara dalam memenuhi kewajiban konstitusionalnya. Badriah et al. (2024) juga menunjukkan pentingnya pembelajaran dari Korea Selatan dan Singapura dalam membangun akuntabilitas kebijakan perlindungan data pribadi. Penelitian ini menambahkan bahwa model akuntabilitas Indonesia harus disesuaikan dengan kedudukan pemerintah sebagai pengendali data publik yang memiliki hubungan langsung dengan pemenuhan hak warga negara.

Kewajiban negara juga perlu ditempatkan dalam relasi antara UU PDP, hukum administrasi pemerintahan, dan pelayanan publik. UU Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan menuntut tindakan pemerintahan berjalan berdasarkan asas legalitas, kepastian hukum, kecermatan, keterbukaan, dan akuntabilitas. UU Nomor 25 Tahun 2009 tentang Pelayanan Publik menempatkan pelayanan sebagai kewajiban negara dalam memenuhi kebutuhan warga. Ketika kedua rezim tersebut dibaca bersama UU PDP, pemrosesan data pribadi dalam pemerintahan digital harus memenuhi tiga lapis legitimasi. Pertama, legitimasi konstitusional karena berkaitan dengan hak warga negara. Kedua, legitimasi administratif karena dilakukan oleh organ pemerintahan. Ketiga, legitimasi teknis karena

menggunakan sistem elektronik yang harus aman, andal, dan dapat diaudit. Pembacaan berlapis ini membedakan penelitian ini dari kajian Rosadi et al. (2023), yang lebih menekankan kebutuhan UU PDP dalam ekonomi digital dan kepastian hukum bagi ekosistem digital.

Hasil analisis juga menunjukkan adanya risiko konflik kepentingan ketika pemerintah berperan sebagai pembentuk kebijakan, pengendali data, sekaligus pihak yang diawasi. Risiko ini terutama muncul ketika pengawasan perlindungan data pribadi tidak memiliki independensi yang kuat. Widiatedja dan Mishra (2023) menekankan pentingnya otoritas perlindungan data yang independen agar pengawasan tidak bergantung pada institusi yang juga dapat menjadi objek pengawasan. Dalam pemerintahan digital, kebutuhan terhadap pengawasan independen menjadi semakin penting karena data pribadi warga diproses dalam skala besar dan sering melibatkan interoperabilitas antarlembaga. Tanpa pengawasan yang kuat, perlindungan data pribadi berisiko berhenti sebagai kepatuhan formal, sementara warga tidak memiliki akses yang efektif untuk mengetahui, memperbaiki, membatasi, atau menuntut pemulihan atas pemrosesan data yang merugikan mereka.

c. Parameter Tanggung Jawab Konstitusional Negara atas Kegagalan Pelindungan Data Pribadi

Hasil penelitian merumuskan bahwa tanggung jawab konstitusional negara dalam perlindungan data pribadi warga setidaknya dapat diukur melalui lima parameter. Parameter pertama adalah **legalitas pemrosesan data**, yaitu setiap pengumpulan, penyimpanan, pemadanan, penggunaan, pembukaan, dan penghapusan data pribadi oleh pemerintah harus memiliki dasar hukum yang jelas. Parameter kedua adalah **pembatasan tujuan**, yaitu data pribadi hanya boleh digunakan untuk tujuan pelayanan publik yang sah, spesifik, dan dapat dipertanggungjawabkan. Parameter ketiga adalah **keamanan dan integritas sistem**, yaitu negara wajib memastikan bahwa sistem pemerintahan digital memiliki perlindungan teknis dan organisasi yang memadai. Parameter keempat adalah **transparansi dan akses subjek data**, yaitu warga harus dapat mengetahui bagaimana data mereka diproses, untuk tujuan apa, oleh siapa, dan bagaimana hak mereka dapat digunakan. Parameter kelima adalah **pemulihan hak**, yaitu negara wajib menyediakan mekanisme pengaduan, koreksi, penghentian pemrosesan, ganti rugi, dan penyelesaian sengketa yang efektif.

Kelima parameter tersebut menunjukkan bahwa tanggung jawab negara tidak cukup dipenuhi melalui keberadaan regulasi semata. Negara juga harus memastikan pelaksanaan regulasi dalam desain kelembagaan dan praktik layanan digital. UU PDP telah memberikan dasar normatif mengenai hak subjek data, kewajiban pengendali dan prosesor, sanksi administratif, penyelesaian sengketa, serta ketentuan pidana. Akan tetapi, efektivitas tanggung jawab negara sangat bergantung pada kemampuan pemerintah menerjemahkan norma tersebut ke dalam standar operasional pelayanan, tata kelola sistem elektronik, pengawasan internal, audit eksternal, dan mekanisme pemulihan bagi warga. Pada titik ini, perlindungan data pribadi harus dipahami sebagai bagian dari kualitas pelayanan publik, bukan sekadar kewajiban kepatuhan teknologi informasi.

Temuan ini sejalan dengan van Donge et al. (2022), yang menyatakan bahwa pemerintahan berbasis data membutuhkan data stewardship dalam ekosistem data publik. Data stewardship penting karena pemrosesan data pemerintah tidak hanya membutuhkan penguasaan teknologi, tetapi juga tata kelola, tanggung jawab, dan pembagian peran antarlembaga. Schmeling et al. (2025) juga menekankan bahwa kolaborasi data dalam pemerintahan digital memerlukan agenda riset dan tata kelola yang lebih kuat karena kolaborasi data dapat meningkatkan kualitas kebijakan sekaligus menimbulkan risiko baru terhadap privasi. Penelitian ini memperluas pandangan tersebut dengan menempatkan data stewardship dan kolaborasi data sebagai bagian dari kewajiban konstitusional negara. Artinya, integrasi data antarlembaga hanya dapat dibenarkan apabila dilakukan dalam batas hukum, tujuan yang sah, standar keamanan yang kuat, dan perlindungan hak warga negara.

Parameter tanggung jawab konstitusional juga relevan untuk membaca potensi penyalahgunaan data dalam layanan pemerintahan digital. Dalam praktiknya, penggunaan data pribadi oleh pemerintah dapat menimbulkan risiko pemantauan berlebihan, pengambilan keputusan otomatis yang tidak transparan, diskriminasi berbasis profil data, dan pembatasan akses pelayanan karena kesalahan data. Kanaan et al. (2023), Li dan Xue (2021), serta Shayganmehr et al. (2023) menunjukkan bahwa kepercayaan, keamanan, privasi, dan persepsi risiko berpengaruh terhadap penerimaan layanan e-government. Penelitian ini menegaskan bahwa kepercayaan publik bukan hanya persoalan kepuasan pengguna, tetapi juga akibat langsung dari kemampuan negara menjamin hak konstitusional warga dalam sistem digital. Ketika warga merasa data pribadinya tidak aman, kepercayaan terhadap pemerintahan digital akan melemah, sekalipun layanan tersebut dirancang untuk meningkatkan efisiensi.

Pembahasan ini juga memperlihatkan bahwa kegagalan perlindungan data pribadi oleh negara harus dipahami sebagai kegagalan berlapis. Pada lapis pertama, kegagalan dapat terjadi karena norma hukum belum diterjemahkan secara jelas ke dalam prosedur teknis dan standar layanan. Pada lapis kedua, kegagalan dapat terjadi karena pengendali data di sektor publik tidak memiliki kapasitas kelembagaan, sumber daya manusia, dan infrastruktur keamanan yang memadai. Pada lapis ketiga, kegagalan dapat muncul karena warga tidak memiliki mekanisme yang efektif untuk mengajukan keberatan, meminta koreksi, memperoleh informasi, atau menuntut pemulihan. Pada lapis keempat, kegagalan dapat timbul karena pengawasan terhadap pemerintah tidak berjalan independen dan transparan. Kurniawan et al. (2024) menyoroti peran sanksi pidana dalam perlindungan data pribadi, sedangkan penelitian ini menegaskan bahwa sanksi pidana hanya satu bagian dari tanggung jawab negara. Tanggung jawab konstitusional memerlukan pencegahan, pengawasan, akuntabilitas, dan pemulihan hak secara terpadu.

Berdasarkan keseluruhan analisis, penelitian ini menemukan bahwa UU PDP memberikan dasar penting untuk menghubungkan perlindungan data pribadi dengan hak konstitusional warga negara, tetapi tanggung jawab negara dalam pemerintahan digital membutuhkan konstruksi yang lebih operasional. Konstruksi tersebut harus memosisikan pemerintah sebagai pihak yang wajib mencegah pelanggaran, menjamin keamanan sistem, membatasi tujuan pemrosesan, membuka ruang transparansi, memastikan pengawasan independen, dan menyediakan pemulihan hak yang efektif. Kebaruan hasil penelitian ini

terletak pada perumusan tanggung jawab konstitusional negara sebagai kerangka analisis terhadap perlindungan data pribadi dalam pemerintahan digital. Kerangka ini menggeser pembahasan dari kepatuhan administratif menuju kewajiban konstitusional yang melekat pada negara ketika data pribadi warga menjadi fondasi pelayanan publik digital.

4. Kesimpulan

Penelitian ini menemukan bahwa data pribadi warga negara dalam penyelenggaraan pemerintahan digital tidak dapat diposisikan hanya sebagai informasi administratif yang dikelola oleh negara. Data pribadi memiliki kedudukan sebagai bagian dari hak konstitusional warga negara karena berhubungan langsung dengan hak atas privasi, hak atas rasa aman, perlindungan diri pribadi, martabat, dan kepastian akses terhadap pelayanan publik. Dalam konteks layanan pemerintahan digital, warga negara sering tidak berada dalam posisi yang sepenuhnya bebas untuk menolak pemrosesan data pribadi karena data tersebut menjadi syarat untuk memperoleh layanan kependudukan, kesehatan, pendidikan, bantuan sosial, perpajakan, perizinan, dan layanan publik lainnya. Posisi tersebut menimbulkan kewajiban konstitusional bagi negara untuk memastikan bahwa setiap pemrosesan data pribadi dilakukan secara sah, aman, transparan, terbatas pada tujuan pelayanan, dan dapat dipertanggungjawabkan.

Temuan utama penelitian ini menunjukkan bahwa Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah memberikan dasar normatif penting dalam menghubungkan perlindungan data pribadi dengan hak konstitusional subjek data. Akan tetapi, dalam penyelenggaraan pemerintahan digital, norma tersebut perlu dibaca secara lebih luas melalui kerangka UUD 1945, hukum administrasi pemerintahan, pelayanan publik, dan sistem pemerintahan berbasis elektronik. Negara tidak cukup hanya berperan sebagai pembentuk regulasi, tetapi juga harus bertanggung jawab sebagai pengendali data, pemroses data, penyelenggara layanan digital, pengawas, dan penjamin pemulihan hak warga negara. Kegagalan negara dalam melindungi data pribadi warga tidak hanya dapat dipahami sebagai kelalaian teknis atau kelemahan administratif, tetapi juga sebagai potensi kegagalan pemenuhan kewajiban konstitusional.

Kontribusi atau kebaruan penelitian ini terletak pada perumusan konsep **tanggung jawab konstitusional negara** dalam perlindungan data pribadi pada pemerintahan digital. Penelitian ini menawarkan lima parameter pertanggungjawaban, yaitu legalitas pemrosesan data, pembatasan tujuan, keamanan dan integritas sistem, transparansi serta akses subjek data, dan pemulihan hak warga negara. Parameter tersebut memperluas pembahasan sebelumnya yang cenderung menempatkan perlindungan data pribadi dalam kerangka privasi, kepatuhan regulasi, ekonomi digital, sanksi, transfer data lintas batas, atau kelembagaan otoritas pengawas. Penelitian ini menegaskan bahwa perlindungan data pribadi dalam layanan pemerintahan digital harus dibaca sebagai bagian dari kewajiban negara untuk melindungi hak konstitusional warga negara, terutama ketika negara memiliki kewenangan dominan dalam pengumpulan dan pemrosesan data.

Implikasi penelitian ini terhadap kajian sejenis sebelumnya adalah perlunya pergeseran orientasi analisis dari sekadar kepatuhan terhadap UU PDP menuju penguatan akuntabilitas konstitusional dalam tata kelola pemerintahan digital. Studi-studi terdahulu telah memberikan dasar penting mengenai hak privasi, urgensi otoritas pengawas independen, tantangan implementasi UU PDP, dan pentingnya kepercayaan publik dalam layanan digital. Penelitian ini melengkapi kajian tersebut dengan menegaskan bahwa persoalan data pribadi dalam sektor publik memiliki karakter khusus karena negara bukan hanya pengguna data, melainkan pemegang kewenangan publik yang tindakan digitalnya dapat berdampak langsung pada pemenuhan hak warga negara. Kekosongan kajian atau *lack of study* yang diisi oleh penelitian ini terletak pada belum kuatnya pembahasan yang secara khusus mengaitkan UU PDP dengan kewajiban konstitusional negara dalam menjamin hak privasi, hak atas rasa aman, dan perlindungan diri pribadi sebagaimana dijamin dalam UUD 1945.

Penelitian ini merekomendasikan agar pemerintah memperkuat tata kelola perlindungan data pribadi dalam pemerintahan digital melalui standar operasional yang jelas, audit keamanan data secara berkala, pembatasan akses internal, penilaian dampak perlindungan data, mekanisme pengaduan yang mudah diakses, serta penguatan lembaga pengawas yang independen. Pemerintah juga perlu memastikan bahwa setiap integrasi data antarlembaga tidak hanya berorientasi pada efisiensi layanan, tetapi juga tunduk pada prinsip legalitas, proporsionalitas, keamanan, transparansi, dan akuntabilitas. Untuk penelitian selanjutnya, kajian dapat dikembangkan melalui pendekatan empiris terhadap praktik perlindungan data pribadi pada instansi pemerintah tertentu, misalnya layanan kependudukan, bantuan sosial, kesehatan, pendidikan, atau perizinan digital. Penelitian lanjutan juga dapat menggunakan pendekatan perbandingan dengan negara lain untuk menilai model kelembagaan pengawasan, mekanisme pemulihan hak, dan standar pertanggungjawaban negara atas pelanggaran data pribadi dalam pemerintahan digital.

Daftar Pustaka

- Anand, N., & Brass, I. (2021). Responsible innovation for digital identity systems. *Data & Policy*, 3, e35. <https://doi.org/10.1017/dap.2021.35>
- Badriah, L., Indiahono, D., & Sukarso. (2024). Accountability in personal data protection policy in Indonesia: Learning from South Korea and Singapore. *Matra Pembaruan: Jurnal Inovasi Kebijakan*, 8(2), 89–102. <https://doi.org/10.21787/mp.8.2.2024.89-102>
- Beduschi, A. (2021). Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations. *Data & Policy*, 3, e15. <https://doi.org/10.1017/dap.2021.15>
- Buttow, C. V. (2025). Data-driven policy making and its impacts on regulation: A study of the OECD vision in the light of data critical studies. *European Journal of Risk Regulation*, 16(1), 114–132. <https://doi.org/10.1017/err.2024.73>
- Buttow, C. V., & Weerts, S. (2024). Managing public sector data: National challenges in the context of the European Union's new data governance models. *Information Polity*, 29(3). <https://doi.org/10.3233/IP-230003>

- Fauzy, E., & Shandy, N. A. R. (2022). Hak atas privasi dan politik hukum Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. *Lex Renaissance*, 7(3), 445–461. <https://doi.org/10.20885/JLR.vol7.iss3.art1>
- Hammerschmid, G., Palaric, E., Rackwitz, M., & Wegrich, K. (2024). A shift in paradigm? Collaborative public administration in the context of national digitalization strategies. *Governance*, 37(2), 411–430. <https://doi.org/10.1111/gove.12778>
- Kanaan, A., Al-Hawamleh, A., Abulfaraj, A., Al-Kaseasbeh, H. M., & Alorfi, A. (2023). The effect of quality, security and privacy factors on trust and intention to use e-government services. *International Journal of Data and Network Science*, 7(1), 185–198. <https://doi.org/10.5267/j.ijdns.2022.11.004>
- Kurniawan, K. D., Hehanussa, D. J. A., Setiawan, R., Susilowati, I., Sopian, & Helfisar, D. (2024). Criminal sanctions and personal data protection in Indonesia. *Lex Publica*, 11(2), 221–247. <https://doi.org/10.58829/lp.11.2.2024.255>
- Li, W., & Xue, L. (2021). The role of trust and risk in citizens' e-government services adoption: A perspective of the extended UTAUT model. *Sustainability*, 13(14), 7671. <https://doi.org/10.3390/su13147671>
- Marwenny, E., Syafwar, R., & Yani, P. (2024). Personal data protection in public services. *Jurnal Ilmiah Ekotrans & Erudisi*, 4(2), 74–85. <https://doi.org/10.69989/yjew5p90>
- Rahman, F. (2025). Safeguarding personal data in the public sector: Unveiling the impact of the new Personal Data Protection Act in Indonesia. *UUM Journal of Legal Studies*, 16(1), 1–18. <https://doi.org/10.32890/uumjls2025.16.1.1>
- Rahman, F., & Mulyani, C. K. (2025). Minimising unnecessary restrictions on cross-border data flows? Indonesia's position and challenges post personal data protection act enactment. *International Review of Law, Computers & Technology*, 39(2), 281–300. <https://doi.org/10.1080/13600869.2024.2359901>
- Rahmatullah, I., Suwadi, P., & Purwadi, H. (2024). Legal reform of zakat management based on personal data protection law in Indonesia. *Mazahib*, 23(1), 199–236. <https://doi.org/10.21093/mj.v23i1.5917>
- Razi, F., Tuasikal, H., & Markus, D. P. (2024). Implementation and challenges of the Personal Data Protection Law in Indonesia. *Jurnal Indonesia Sosial Teknologi*, 5(12), 6559–6565. <https://doi.org/10.59141/jist.v5i12.1285>
- Rosadi, S. D., Noviandika, A., Walters, R., & Aisy, F. R. (2023). Indonesia's personal data protection bill, 2020: Does it meet the needs of the new digital economy? *International Review of Law, Computers & Technology*, 37(1), 78–90. <https://doi.org/10.1080/13600869.2022.2114660>
- Santana, P. C., & Ansari, F. A. (2023). Data protection and privacy as a fundamental right: A comparative study of Brazil and India. *Journal of Liberty and International Affairs*, 9(3), 456–470. <https://doi.org/10.47305/JLIA2393555cs>

- Schmeling, J., Al Dakruni, S., & Mergel, I. (2025). Data collaboration in digital government research: A literature review and research agenda. *Government Information Quarterly*, 42(3), 102063. <https://doi.org/10.1016/j.giq.2025.102063>
- Shayganmehr, M., Kumar, A., Garza-Reyes, J. A., & Zavadskas, E. K. (2023). A framework for assessing trust in e-government services under uncertain environment. *Information Technology & People*, 36(7), 2718–2755. <https://doi.org/10.1108/ITP-01-2021-0096>
- Syailendra, M. R., Lie, G., & Sudiro, A. (2024). Personal data protection law in Indonesia: Challenges and opportunities. *Indonesia Law Review*, 14(2), Article 4. <https://doi.org/10.15742/ilrev.v14n2.4>
- Tan, E., Mahula, S., & Cromptvoets, J. (2022). Blockchain governance in the public sector: A conceptual framework for public management. *Government Information Quarterly*, 39(1), 101625. <https://doi.org/10.1016/j.giq.2021.101625>
- van Donge, W., Bharosa, N., & Janssen, M. (2022). Data-driven government: Cross-case comparison of data stewardship in data ecosystems. *Government Information Quarterly*, 39(2), 101642. <https://doi.org/10.1016/j.giq.2021.101642>
- Wibowo, A., Alawiyah, W., & Azriadi. (2024). The importance of personal data protection in Indonesia's economic development. *Cogent Social Sciences*, 10(1), 2306751. <https://doi.org/10.1080/23311886.2024.2306751>
- Widiatedja, I. G. N. P., & Mishra, N. (2023). Establishing an independent data protection authority in Indonesia: A future-forward perspective. *International Review of Law, Computers & Technology*, 37(3), 252–273. <https://doi.org/10.1080/13600869.2022.2155793>
- Yusliwidaka, A., Abqa, M. A. R., & Wardana, K. A. (2024). A discourse of personal data protection: How Indonesia responsible under domestic and international law? *Pandecta Research Law Journal*, 19(2), 453–482. <https://doi.org/10.15294/pandecta.v19i2.13279>
- Yuspin, W., Rajput, T., Bal, A. B., Wardiono, K., & Absori. (2024). The regulations of the supervisory officer personal data protection-based accountability principle. *BESTUUR*, 12(1), 49–68. <https://doi.org/10.20961/bestuur.v12i1.89742>
- Yuspin, W., Wardiono, K., Nurrahman, A., & Budiono, A. (2023). Personal data protection law in digital banking governance in Indonesia. *Studia Iuridica Lublinensia*, 32(1), 99–130. <https://doi.org/10.17951/sil.2023.32.1.99-130>

Bahan Hukum Primer

Republik Indonesia. (1945). *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*.

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*.