CAUSA
ISSN 3031-0369

Jurnal Hukum dan Kewarganegaraan
Vol 14 No 9 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

URGENSI UU PERLINDUNGAN DATA PRIBADI: TANGGUNG JAWAB HUKUM KEBOCORAN DATA PEDULILINDUNGI

Alwi Suhaya[1*], Qeysha Ayle Viorella[2], Salsabila[3]

Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Pamulang,
Kota Tangerang Selatan, Indonesia

Email: alwishy1@gmail.com[1*], qeysha.av02@gmail.com[2], bilah.salsa0104@gmail.com[3]

ABSTRAK

Penelitian ini bertujuan mengkaji secara komprehensif dimensi hukum yang timbul akibat insiden pembocoran data pribadi pengguna aplikasi PeduliLindungi. Dengan menggunakan pendekatan yuridis normatif, analisis berlandaskan peraturan perundang-undangan, asas-asas hukum, putusan pengadilan, dan praktik hukum terkait. Fokus utama adalah pada tanggung jawab hukum penyelenggara sistem elektronik berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 (UU ITE) dan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE). Penelitian ini juga mengaitkan kebocoran data dengan prinsip hak asasi manusia, khususnya hak atas privasi dalam Pasal 28G ayat (1) UUD 1945. Hasil kajian menegaskan bahwa penyelenggara sistem elektronik memiliki kewajiban mutlak menjamin kerahasiaan, keutuhan, dan ketersediaan data pribadi. Ketidakpatuhan mengakibatkan konsekuensi hukum administratif, perdata, dan berpotensi pidana bila terdapat unsur kesengajaan atau kelalaian berat. Oleh karena itu, mendesak pengesahan Undang-Undang Perlindungan Data Pribadi untuk mengisi kekosongan hukum substantif perlindungan data di Indonesia.

Kata Kunci: Pembocoran Data Pribadi, PeduliLindungi, Pertanggungjawaban Hukum.

ABSTRACT

This study aims to comprehensively examine the legal dimensions arising from the personal data breach incident affecting users of the PeduliLindungi application. Utilizing a normative juridical approach, the analysis is grounded in statutory regulations, legal principles, court decisions, and relevant legal practices. The primary focus is on the legal liability of electronic system providers under Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 19 of 2016 (ITE Law), and Government Regulation Number 71 of 2019 on

Article History
Received: Juni 2025
Reviewed: Juni 2025
Published: Juni 2025
Plagirism Checker No 234
Prefix DOI:
10.8734/CAUSA.v1i2.365
Copyright : Author
Publish by : CAUSA

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Jurnal Hukum dan Kewarganegaraan
Vol 14 No 9 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

the Operation of Electronic Systems and Transactions (PP PSTE). This research also links data breach issues to human rights principles, particularly the right to privacy enshrined in Article 28G paragraph (1) of the 1945 Constitution. The findings affirm that electronic system providers have an absolute obligation to ensure the confidentiality, integrity, and availability of personal data. Non-compliance leads to administrative, civil, and potentially criminal liabilities if elements of intent or gross negligence are present. Hence, the enactment of a Personal Data Protection Law is urgently needed to address the substantive legal vacuum in Indonesia's data protection framework.

***Keywords**: Data Breach, PeduliLindungi, ITE Law, Legal Liability.*

PENDAHULUAN

Pandemi COVID-19 memaksa pemerintah dan masyarakat beradaptasi dengan solusi digital untuk penanganan kesehatan. Salah satu inovasi utama adalah aplikasi PeduliLindungi, yang berfungsi sebagai media pelacakan kontak, verifikasi status vaksinasi, dan pemberian izin akses ke berbagai fasilitas publik. Dengan lebih dari 100 juta unduhan pada tahun 2021, aplikasi ini menjadi bagian tak terpisahkan dari strategi mitigasi penyebaran virus di Indonesia.

Implementasi PeduliLindungi menimbulkan tantangan baru terkait perlindungan data pribadi. Aplikasi ini mengumpulkan data sensitif pengguna, termasuk lokasi *real-time*, riwayat kesehatan, dan identitas personal. *Volume* data yang sangat besar ini mengharuskan penyelenggara sistem elektronik dalam hal ini Kementerian Kesehatan dan mitra pengembang untuk memastikan mekanisme keamanan yang memadai.

Pada kuartal kedua tahun 2022, beredar laporan dugaan kebocoran data pengguna PeduliLindungi di forum *online* dan media sosial. Informasi privasi seperti nama lengkap, nomor telepon, hingga hasil tes COVID-19 dilaporkan dijual di pasar gelap digital. Insiden ini memicu keresahan masyarakat dan menimbulkan pertanyaan mendasar: sejauh mana tanggung jawab hukum penyelenggara sistem ketika terjadi pelanggaran keamanan data?

Reaksi publik terhadap dugaan kebocoran ini sangat kuat. Perhimpunan Bantuan Hukum dan HAM Indonesia (PBHI) mengajukan gugatan ke Pengadilan Tata Usaha Negara (PTUN) terhadap Kementerian Kesehatan, menyoroti dugaan kelalaian dan abainya pemeliharaan sistem sesuai standar keamanan yang ditetapkan. Gugatan ini mempertegas konflik antara kepentingan publik dalam penanganan pandemi dan hak individu untuk privasi dan perlindungan data.

Secara hukum, tanggung jawab penyelenggara sistem elektronik diatur dalam UU No. 11/2008 jo. UU No. 19/2016 (UU ITE) dan PP No. 71/2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Pasal 15 UU ITE mengharuskan penyelenggara untuk menjamin keandalan dan keamanan sistem, sedangkan Pasal 26 mengatur hak subjek data dalam memberikan persetujuan dan ganti rugi. Ketentuan ini menjadi landasan utama untuk menilai kewajiban hukum Pelaksana PeduliLindungi.

Meskipun kerangka hukum sektoral telah ada, belum terdapat regulasi khusus yang komprehensif untuk personal data protection. Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) telah dibahas sejak 2019, namun hingga saat ini belum disahkan. Kekosongan

Jurnal Hukum dan Kewarganegaraan
Vol 14 No 9 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

ini menimbulkan celah hukum yang dapat dimanfaatkan oleh pelaku kejahatan siber dan menimbulkan risiko sistemik bagi keamanan data nasional.

Kajian ini bertujuan menggali fenomena kebocoran data PeduliLindungi dari perspektif yuridis normatif, menilai kecukupan UU ITE dan PP PSTE, serta merumuskan rekomendasi kebijakan. Dengan demikian, penelitian diharapkan memberikan kontribusi akademik dan solusi praktis bagi pembuat kebijakan untuk memperkuat perlindungan data pribadi di era digital.

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)

Menurut Pasal 1 angka 1 UU No. 11/2008 jo. UU No. 19/2016, Sistem Elektronik didefinisikan sebagai serangkaian perangkat dan prosedur elektronik untuk memperoleh, menyimpan, mengolah, menampilkan, mengumumkan, dan/atau menyebarkan Informasi Elektronik. Hal ini menegaskan ruang lingkup aplikasi PeduliLindungi sebagai penyelenggara sistem elektronik yang wajib menerapkan standar keamanan data.

Menurut Pasal 15 UU ITE, penyelenggara sistem elektronik wajib menjamin keandalan dan keamanan sistem yang dikelolanya. Pasal ini menempatkan beban tanggung jawab awal pada pengelola aplikasi, termasuk kewajiban melakukan verifikasi, enkripsi, dan audit keamanan secara berkala. Menurut Pasal 26 UU ITE, penggunaan data pribadi hanya dapat dilakukan setelah mendapat persetujuan tegas dari pemilik data, serta pemilik data berhak memperoleh ganti rugi jika terjadi pelanggaran. Menurut Pasal 32 UU ITE, setiap orang dilarang mengakses, mentransmisikan, atau menggunakan Informasi Elektronik tanpa hak. Ketentuan ini menjadi dasar hukum pengenaan tanggung jawab pidana apabila terbukti terjadi peretasan atau penyebaran data pengguna secara melawan hukum.

Peraturan Pemerintah No. 71 Tahun 2019 (PP PSTE)

Menurut Pasal 3 PP PSTE, setiap penyelenggara sistem elektronik wajib menyelenggarakan sistem yang andal, aman, dan bertanggung jawab atas pengoperasiannya. Menurut Pasal 5 ayat (2) PP PSTE, penyelenggara wajib melakukan pembaruan teknologi dan prosedur keamanan untuk melindungi integritas serta kerahasiaan data, serta menyediakan mekanisme *contingency plan* jika terjadi insiden pelanggaran data. Menurut Pasal 15 PP PSTE, penyelenggara wajib memberitahukan secara tertulis kepada pejabat berwenang apabila terjadi kegagalan sistem yang berpotensi menimbulkan kerugian bagi pengguna.

Studi Sebelumnya

Pertanggungjawaban hukum penyelenggara PeduliLindungi atas potensi kebocoran data terletak pada Pasal 15 ayat (2) UU ITE, yang mewajibkan pengelola untuk mengamankan setiap transaksi elektronik dan mengantisipasi akses illegal (Alfian *et al*, 2023). Layanan kesehatan digital seperti PeduliLindungi memerlukan payung hukum PDP untuk melindungi konsumen, karena Pasal 26 UU ITE bersifat umum dan belum mampu menampung perkembangan teknologi informasi terkini (Dewi *et al,* 2022).

Belum adanya *lex specialis* perlindungan data pribadi di Indonesia menyebabkan fragmentasi regulasi antara UU ITE, UU Kesehatan, dan UU Administrasi Kependudukan, sehingga perlu harmonisasi peraturan (Nurhidayati *et al, 2023*). Rentannya sistem PeduliLindungi terhadap serangan siber menunjukkan kurangnya standarisasi keamanan nasional, dan menekankan kebutuhan adopsi prinsip legalitas, proporsionalitas, dan akuntabilitas ala GDPR (Thaher, 2024).

Penelitian menyoroti bahwa dari 145 negara yang telah memiliki undang-undang perlindungan data pribadi, sebagian besar mengadopsi prinsip-prinsip utama dari GDPR, seperti

CAUSA
ISSN 3031-0369

Jurnal Hukum dan Kewarganegaraan
Vol 14 No 9 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

persetujuan eksplisit, hak akses dan penghapusan data, serta kewajiban pelaporan insiden (Greenleaf, 2021). Temuan ini memperkuat argumen bahwa Indonesia perlu segera mengadopsi UU Perlindungan Data Pribadi secara komprehensif agar selaras dengan standar global dan dapat menjamin hak konstitusional warga negara atas privasi data pribadi.

Perlindungan Hukum Korban Kebocoran Data korban publikasi data pribadi berhak atas reparasi materiil dan imateriil berdasarkan prinsip keadilan restoratif, serta UU ITE Pasal 26 perlu ditafsirkan untuk mencakup kerugian psikologis dan reputasi (Putri, 2023). Kasus publikasi data pada putusan pengadilan menegaskan pentingnya hak penghapusan *(right to erasure)* dan koreksi data yang keliru sebagai upaya perlindungan procedural, yang relevan untuk PeduliLindungi. Mekanisme penegakan hukum atas kebocoran data di SPBE terhambat oleh kurangnya koordinasi antar-penyelenggara dan lemahnya sanksi administratif, sehingga diperlukan unit koordinatif khusus di BSSN untuk menangani pengaduan korban (Matsna, 2022).

METODE PENELITIAN

Penelitian ini menggunakan pendekatan yuridis normatif yang mengkaji ketentuan hukum melalui dokumen resmi dan analisis kualitatif. Metode yang digunakan mencakup pendekatan perundang-undangan untuk menganalisis UU ITE dan PP 71/2019, pendekatan konseptual untuk mendefinisikan istilah hukum utama, serta pendekatan kasus dengan menelaah gugatan PBHI terhadap Kemenkes. Pendekatan komparatif juga digunakan dengan membandingkan kerangka hukum Indonesia dengan GDPR Uni Eropa. Sumber data terdiri atas bahan hukum primer dan sekunder yang dianalisis secara sistematis menggunakan teknik triangulasi dokumen untuk menjamin validitas temuan.

HASIL PEMBAHASAN

Analisis Kewajiban Hukum Penyelenggara Sistem Elektronik

Berdasarkan pendekatan perundang-undangan, Pasal 15 PP 71/2019 menegaskan bahwa setiap penyelenggara sistem elektronik wajib menyediakan sistem yang andal, aman, dan sesuai prosedur teknis yang telah ditetapkan. Hasil pemetaan terhadap dokumentasi teknis PeduliLindungi menunjukkan bahwa hingga 2022, belum ada laporan audit keamanan independen yang dipublikasi secara transparan. Kondisi ini membuktikan adanya *gap* antara ketentuan hukum dan praktik lapangan, yang memerlukan penguatan mekanisme pengawasan pemerintah dan audit pihak ketiga.

Selain itu, Pasal 26 UU ITE mengharuskan adanya persetujuan tegas *(opt-in)* dari subjek data sebelum pengumpulan data pribadi (Republik Indonesia, 2008). Berdasarkan data pengguna, implementasi *opt-in* di PeduliLindungi masih bersifat otomatis tanpa penjelasan rinci, sehingga berpotensi melanggar asas keterbukaan dan persetujuan informatif.

Secara konseptual, *duty of care* (kewajiban kehati-hatian) menempatkan beban proaktif pada penyelenggara untuk melakukan Data Protection Impact Assessment (DPIA) guna menilai risiko kebocoran data sebelum peluncuran fitur baru. Praktik di GDPR menunjukkan bahwa DPIA menjadi standar minimal, sedangkan di Indonesia hal ini belum diatur secara eksplisit.

Tabel 1. Prinsip Perlindungan Data Dalam PeduliLindungi

Prinsip	PeduliLindungi
Persetujuan eksplisit	Tidak diterapkan
Hak akses/koreksi	Terbatas

Jurnal Hukum dan Kewarganegaraan
Vol 14 No 9 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

Pemberitahuan insiden	Tidal konsisten
Penilaian dampak (DPIA)	Tidak tersedia

Tabel 1. menggambarkan keterbatasan implementasi prinsip-prinsip dasar perlindungan data oleh PeduliLindungi. Tidak adanya persetujuan eksplisit dan mekanisme DPIA mengindikasikan belum terpenuhinya prinsip akuntabilitas dan transparansi sebagaimana diatur dalam norma perlindungan data yang ideal.

Evaluasi Kasus Kebocoran Data

Pendekatan kasus menggali laporan kebocoran data di pasar gelap digital. Investigasi forensik *online* menunjukkan ribuan rekaman data PeduliLindungi yang diperjualbelikan antara Juni–Agustus 2022. Temuan ini konsisten dengan studi (Alfian *et al.*, 2023), yang melaporkan adanya celah keamanan pada API e-HAC terintegrasi dan menegaskan perlunya patching berkala. Putusan PTUN atas gugatan PBHI dengan Kemenkes menyoroti kelalaian administrasi Kemenkes dalam memenuhi kewajiban notifikasi insiden (Pasal 15 PP PSTE). Majelis Hakim dalam putusan memperingatkan pentingnya transparansi publik dan pemberitahuan resmi untuk meminimalisir potensi dampak bagi hak warga negara.

Kasus ini juga menunjukkan bahwa aspek teknis dan administratif saling terkait; kegagalan teknis memicu tanggung jawab hukum administratif. Oleh karena itu, analisis komparatif dengan GDPR mengindikasikan bahwa selain sanksi denda, mekanisme remediasi (pemberitahuan publik, kompensasi korban) sangat penting.

Tabel 2. Insiden Kebocoran Data Instansi Publik (2021-2023)

Instansi	2021	2022	2023	Total	Sanksi
PeduliLindungi	1	2	2	5	1
Dukcapil	0	1	1	2	0

Tinjauan Sanksi dan Mekanisme Penegakan

Hasil analisis konten terhadap UU ITE dan PP PSTE memperlihatkan bahwa sanksi administratif meliputi teguran, pembatasan akses, hingga pencabutan izin penyelenggaraan sistem. Sanksi perdata dapat berupa ganti rugi material dan immaterial, sedangkan sanksi pidana diatur dalam Pasal 32 UU ITE, dengan ancaman kurungan dan denda. Namun, implementasi sanksi di Indonesia masih minim.

Berdasarkan Laporan Tahunan BSSN, tercatat insiden kebocoran data yang melibatkan berbagai instansi pemerintah dan layanan publik, termasuk 5 insiden pada PeduliLindungiantara 2021–2023 (BSSN, 2024). Dari total insiden, hanya kasus yang berujung sanksi administratif dan 4 kasus yang diteruskan ke proses hukum perdata maupun pidana (BSSN, 2024).

Implikasi Kebijakan dan Rekomendasi Praktis

Berdasarkan data empiris dan analisis yuridis, beberapa rekomendasi praktis dapat diajukan:

1. Pengesahan UU PDP
   Mengatur prosedur DPIA, pelaporan insiden, dan mekanisme remediasi korban secara rinci.
2. Pembangunan Database Insiden Nasional
   Untuk memantau dan menindaklanjuti setiap laporan kebocoran data.
3. Standar Sertifikasi Keamanan

Jurnal Hukum dan Kewarganegaraan
Vol 14 No 9 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

Bersifat wajib bagi penyelenggara sistem elektronik, termasuk PeduliLindungi, yang diperbarui setiap 6 bulan.

4. Mekanisme Kompensasi
   Dengan melibatkan dana asuransi *cyber* untuk mengganti kerugian korban kebocoran data.
5. Transparansi Publik
   Melalui portal resmi yang memuat laporan audit keamanan dan respons insiden.

Dengan implementasi rekomendasi tersebut, diharapkan penegakan hukum dan proteksi data pribadi di Indonesia dapat berjalan lebih efektif dan profesional.

Tabel 3. Regulasi Hukum Terkait Kebocoran Data

Regulasi	Pasal	Kewajiban	Sanksi
UU ITE	15, 26, 32	Keamanan sistem, persetujuan, larangan akses	Administratif, perdata, pidana
PP 71/2019	3, 5	Audit, enkripsi, notifikasi	Teguran, pembatasan
	15	Insiden	Pencabutan izin

Tabel 3. menunjukkan bahwa tanggung jawab hukum penyelenggara sistem elektronik telah secara jelas diatur dalam UU ITE dan PP PSTE. Setiap regulasi mengandung kewajiban khusus dan sanksi yang beragam. Hal ini memperkuat dasar hukum yang dapat digunakan untuk menilai kelalaian dalam kasus PeduliLindungi.

Implikasi Kebijakan dan Rekomendasi Praktis

Berdasarkan temuan di atas, kekosongan regulasi PDP menjadi akar masalah utama. RUU PDP yang komprehensif perlu mencakup kewajiban DPIA, definisi pelanggaran data, dan mekanisme penyelidikan insiden. Pemerintah harus memperkuat lembaga pengawas, seperti BSSN, dengan kewenangan penindakan yang jelas dan sumber daya memadai. Selain itu, audit keamanan independen wajib dipublikasikan untuk memastikan transparansi.

Akhirnya, perlu diadopsi mekanisme remediasi korban, mencakup pemberitahuan publik, kompensasi finansial, dan rehabilitasi reputasi. Praktik ini selaras dengan GDPR dan dapat memperkuat kepercayaan publik terhadap sistem digital nasional.

Urgensi Legislasi Perlindungan Data Pribadi

Menekankan bahwa absennya UU PDP menyebabkan ketidakpastian hukum dalam penanganan kebocoran data di sektor publik. UU PDP mendesak untuk segera disahkan karena berfungsi tidak hanya sebagai dasar hukum perlindungan data, tetapi juga sebagai panduan prosedural penanganan insiden, mekanisme kompensasi, dan pemulihan hak korban.

KESIMPULAN

Penyelenggara aplikasi PeduliLindungi memiliki kewajiban hukum untuk melindungi data pribadi pengguna sebagaimana diatur dalam UU ITE dan PP 71/2019. Kebocoran data yang terjadi akibat kelalaian atau kelemahan sistem keamanan menimbulkan konsekuensi hukum baik secara administratif maupun perdata. Fakta ini menunjukkan adanya celah perlindungan hukum terhadap data pribadi di Indonesia yang masih belum optimal. Oleh karena itu, urgensi pengesahan RUU Perlindungan Data Pribadi sangat penting sebagai langkah untuk memperkuat kerangka hukum perlindungan data secara komprehensif. Pemerintah juga perlu meningkatkan koordinasi antar lembaga seperti BSSN, memperkuat fungsi pengawasan dan audit keamanan sistem elektronik, serta menjamin transparansi dan akuntabilitas dalam penanganan setiap insiden kebocoran data. Langkah-langkah tersebut diharapkan dapat membangun sistem hukum

yang lebih tangguh dan menjamin hak konstitusional warga atas privasi dan keamanan informasi.

SARAN

Untuk memperbaiki tata kelola keamanan data, disarankan agar penyelenggara PeduliLindungi menerapkan standar sertifikasi ISO/IEC 27001 dan melakukan Data Protection Impact Assessment (DPIA) sebelum setiap pembaruan fitur. Pemerintah perlu mempercepat pengesahan Undang-Undang Perlindungan Data Pribadi yang memuat mekanisme penanganan insiden, hak subjek data atas koreksi dan penghapusan informasi, serta sanksi administratif dan pidana yang tegas. BSSN harus dibekali wewenang koordinatif untuk membangun Database Insiden Nasional dan menyelenggarakan audit keamanan independen secara berkala. Selain itu, mekanisme kompensasi finansial dan rehabilitasi reputasi bagi korban kebocoran data, serta portal publik yang menampilkan laporan insiden dan audit keamanan, akan membantu memulihkan kepercayaan masyarakat. Dengan langkah-langkah ini, diharapkan perlindungan data pribadi di Indonesia menjadi lebih tangguh, responsif, dan akuntabel.

DAFTAR PUSTAKA

Alfian, F. S., Alam, M. Z., & Maharani, D. P. (2023). Pertanggungjawaban Hukum Penyelenggara Sistem Elektronik PeduliLindungi Terhadap Potensi Kebocoran Data Pribadi. *Brawijaya Law Student Journal, 12*(1), 45–60.

Amiruddin, & Asikin, Z. (2016). *Pengantar Ilmu Hukum*. Prenadamedia Group.

BSSN. (2024). *Laporan Tahunan Badan Siber dan Sandi Negara 2023*. BSSN.

Dewi, N. M. M., Budiartha, I. N. P., & Subamia, I. N. (2022). Tanggung Jawab Penyedia Layanan Kesehatan Aplikasi PeduliLindungi terhadap Keamanan Data Pribadi Konsumen. *Jurnal Preferensi Hukum, 3*(2), 407–412.

GDPR. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data. *Official Journal of the European Union*.

Greenleaf, G. (2021). Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance. *Privacy Laws & Business International Report, 169*, 10–13.

Kausar, T. R. (2022). *Implementasi Hak Penghapusan dan Koreksi Data dalam SPBE*. Skripsi, Institut Agama Negeri (IAN).

Kementerian Kesehatan Republik Indonesia. (2021). *Penjelasan Kemenkes soal Kebocoran Data di Aplikasi PeduliLindungi*. Detik Finance.

Matsna, S. (2022). *Penegakan Hukum atas Kebocoran Data di Sistem Pemerintahan Berbasis Elektronik*. Fakultas Syariah dan Hukum.

Nurhidayati, N., Sugiyah, S., & Yuliantari, K. (2023). Pengaturan Perlindungan Data Pribadi Dalam Penggunaan Aplikasi PeduliLindungi. *Widya Cipta: Jurnal Sekretari dan Manajemen, 7*(1), 112–125.

Putri Azzahra, R. (2023). *Perlindungan Hukum Bagi Korban Atas Publikasi Data Pribadi Pada Kasus Tindak Pidana Kesusilaan di Situs Mahkamah Agung*. Universitas Warmadewa.

Rahman, F. (2021). Kerangka Hukum Perlindungan Data Pribadi dalam Penerapan Sistem Pemerintahan Berbasis Elektronik di Indonesia. *Jurnal Legislasi Indonesia, 18*(1), 81–102.

Jurnal Hukum dan Kewarganegaraan
Vol 14 No 9 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

Republik Indonesia. (2008*). Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik* jo. UU No. 19 Tahun 2016. JDIH Kemenkeu.

Republik Indonesia. (2019). *Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik*. JDIH Komdigi.

Saleh, R. (2019). *Hukum Siber di Indonesia*. Rajawali Pers.

Thaher, I. (2024). Politik Hukum: Perlindungan Data Pribadi pada Aplikasi PeduliLindungi di Indonesia. *Jurnal Pendidikan Tambusai, 9*(2), 78–89.