COSMOS: Jurnal Ilmu Pendidikan, Ekonomi dan Teknologi
ISSN: 3046-4846 (Elektronik)
Vol. 2 No.3, April-Mei 2025

Antara Kemudahan dan Kerentanan: Analisis Yuridis Perlindungan Data Identitas Kependudukan dalam Aplikasi Digital

Mugiono[1]*, Sidi Ahyar Wiraguna[2]
Fakultas Hukum Universitas Esa Unggul Jakarta
Email Penulis Korespondensi: mugiono2712@student.esaunggul.ac.id,

Abstrak

Perkembangan teknologi digital mempercepat transformasi layanan publik melalui aplikasi identitas kependudukan, namun meningkatkan risiko kerentanan data pribadi. Penelitian ini menganalisis perlindungan hukum terhadap data identitas kependudukan dalam aplikasi digital dengan pendekatan yuridis normatif, mengacu pada Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan relevansinya dengan Pasal 28G ayat (1) UUD 1945 yang menjamin hak privasi. Tujuan penelitian mengkaji efektivitas regulasi tersebut dalam melindungi data pengguna serta mengidentifikasi celah hukum yang berpotensi dimanfaatkan oleh pihak tidak bertanggung jawab. Ruang lingkup penelitian terfokus pada implementasi UU PDP dalam konteks aplikasi kependudukan digital di Indonesia. Hasil penelitian menunjukkan bahwa meskipun UU PDP telah memberikan dasar hukum yang kuat, tiga tantangan utama masih menghambat perlindungan optimal, yaitu: (1) lemahnya mekanisme pengawasan, (2) rendahnya kesadaran pengguna, dan (3) ketidakjelasan sanksi bagi pelanggar. Implikasi penelitian mengarah pada rekomendasi kebijakan berupa penguatan lembaga pengawas, sosialisasi hak digital warga, dan penyempurnaan ketentuan sanksi. Simpulan penelitian menegaskan bahwa perlindungan data identitas kependudukan memerlukan sinergi antara regulasi, teknologi, dan partisipasi masyarakat.

Kata Kunci: *Aplikasi digital; Identitas kependudukan; Perlindungan data pribadi; UU PDP; Yuridis normatif.*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang pesat telah membawa dampak signifikan terhadap kehidupan masyarakat (Rosana, 2010), termasuk dalam hal pengelolaan data pribadi. Aplikasi identitas kependudukan digital merupakan salah satu inovasi yang bertujuan untuk mempermudah akses layanan publik dan meningkatkan efisiensi administrasi pemerintahan (Yulanda, 2023). Namun, di balik kemudahan tersebut, terdapat tantangan besar terkait perlindungan data pribadi

pengguna. Data pribadi yang dikelola dalam aplikasi ini berpotensi disalahgunakan jika tidak dilindungi dengan baik, sehingga menimbulkan risiko pelanggaran privasi (M Barthos, 2024).

Isu perlindungan data pribadi semakin mendesak untuk diperhatikan, terutama setelah disahkannya Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. Kerentanan data identitas kependudukan digital tercermin dari maraknya kasus penyalahgunaan data untuk kejahatan siber, seperti pemalsuan identitas dan penipuan finansial (Pusat Pelaporan dan Analisis Transaksi Keuangan/PPATK, 2023). Menurut data dari Kementerian Komunikasi dan Informatika, pada tahun 2022 terdapat lebih dari 200 kasus kebocoran data yang melibatkan informasi pribadi masyarakat. Survei Kementerian Kominfo (2024) mengungkapkan bahwa 65% pengguna aplikasi kependudukan digital tidak memahami mekanisme perlindungan data pribadi. Padahal, Pasal 28G ayat (1) UUD 1945 secara eksplisit menjamin hak privasi sebagai hak konstitusional warga negara. Hal ini menunjukkan bahwa meskipun regulasi telah ada, implementasinya masih menghadapi berbagai kendala. Penelitian sebelumnya menunjukkan bahwa kesadaran masyarakat akan hak-hak perlindungan data pribadi masih rendah, dan banyak pengguna yang tidak memahami risiko yang terkait dengan penggunaan aplikasi digital (Sari, 2023) (Shafa Salsabila, 2025). Disahkannya UU PDP belum sepenuhnya diikuti dengan kapasitas kelembagaan yang memadai, seperti terlihat dari keterbatasan sumber daya Komisi Perlindungan Data Pribadi (Kemenkominfo, 2024). Kondisi ini memperparah risiko pelanggaran data, terutama dalam sistem yang melibatkan banyak pihak seperti aplikasi kependudukan digital (Sri Mulyati, 2025).

Kesenjangan penelitian ini terletak pada kurangnya analisis mendalam mengenai efektivitas perlindungan hukum yang diberikan oleh Undang-Undang No. 27 Tahun 2022 dalam konteks aplikasi identitas kependudukan digital. Penelitian terdahulu lebih banyak berfokus pada aspek teknis dan kebijakan, sementara aspek yuridis dan perlindungan hukum terhadap pengguna masih kurang dieksplorasi. Oleh karena itu, penelitian ini bertujuan untuk mengisi gap tersebut dengan memberikan analisis yuridis yang komprehensif.

Penelitian ini berfokus pada analisis yuridis efektivitas UU PDP dalam melindungi data identitas kependudukan digital. Studi ini mengkaji tiga aspek utama: (1) kesesuaian regulasi dengan tantangan teknologi terkini, (2) mekanisme pengawasan dan penegakan hukum, serta (3) perlindungan hak pengguna berdasarkan prinsip *privacy by design*. Ruang lingkup penelitian mencakup implementasi UU PDP pada aplikasi berbasis populasi seperti E-KTP digital dan aplikasi Dukcapil. Pendekatan ini memungkinkan identifikasi celah hukum antara teori regulasi dan praktik di lapangan.

Studi sebelumnya oleh Sari (2023) mengkaji aspek teknis keamanan aplikasi kependudukan digital, namun kurang menyentuh analisis yuridis. Penelitian Yulanda (2023) fokus pada kebijakan pemerintah tanpa mengevaluasi efektivitas penegakan

hukum. Kesenjangan literatur tersebut diisi oleh penelitian ini melalui pendekatan yuridis normatif yang mengintegrasikan analisis regulasi dan empirisme. Referensi dari jurnal terindeks Sinta 1 seperti *Pandecta* (Vol. 18, No. 1, 2023) memperkuat dasar teoritis mengenai prinsip *accountability* dalam UU PDP.

Urgensi penelitian ini terletak pada kebutuhan untuk memahami dan mengevaluasi perlindungan hukum yang ada, serta memberikan rekomendasi untuk perbaikan kebijakan yang lebih efektif. Kebaruan penelitian ini juga terletak pada pendekatan normatif dan empiris yang digunakan untuk menganalisis regulasi yang ada, serta implikasinya terhadap perlindungan data pribadi pengguna aplikasi identitas kependudukan digital (Sidi, 2025).

Hasil penelitian memberikan kontribusi akademis berupa pengembangan teori perlindungan data dalam konteks *e-government*. Bagi pemerintah, temuan ini menjadi dasar penyusunan pedoman teknis UU PDP untuk aplikasi kependudukan. Praktisi hukum dapat memanfaatkan analisis ini sebagai rujukan dalam menangani sengketa pelanggaran data. Dampak jangka panjang mencakup peningkatan kepercayaan publik terhadap layanan digital pemerintah, sejalan dengan target transformasi digital Indonesia 2045 (RPJPN 2025-2045).

METODE PENELITIAN

Metode penelitian normatif lebih unggul dalam penyusunan kerangka hukum yang lebih jelas dan terstruktur namun terbatas dalam hal menangkap dinamika sosial serta empiris di masyarakat sebaliknya, pendekatan empiris dapat menyajikan data langsung dari lapangan dan memberikan wawasan yang lebih mendalam tentang praktik hokum yang konkrit, meskipun terkadang terdapat tantangan terkait validasi dan reliabilitas data (Wiraguna, 2024). Penelitian ini menggunakan metode penelitian normatif dan metode penelitian empiris. Metode normatif berfokus pada analisis terhadap peraturan perundang-undangan yang mengatur perlindungan data pribadi, termasuk Undang-Undang No. 27 Tahun 2022 dan regulasi terkait lainnya.

HASIL DAN PEMBAHASAN

Perlindungan hukum terhadap data pribadi pengguna layanan aplikasi identitas kependudukan digital berdasarkan Undang-Undang No. 27 Tahun 2022

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) memberikan kerangka hukum komprehensif untuk melindungi data pribadi dalam ekosistem digital (Disemadi, 2023), termasuk aplikasi identitas kependudukan. Pasal 4 UU PDP menetapkan prinsip perlindungan data yang meliputi: (1) kepastian hukum, (2) kepentingan yang sah, (3) tujuan yang spesifik, (4) keterbukaan, dan (5) akuntabilitas. Prinsip-prinsip ini menjadi landasan bagi penyelenggara aplikasi kependudukan digital dalam mengelola data pengguna.

Analisis terhadap implementasi UU PDP menunjukkan bahwa perlindungan data identitas kependudukan digital masih menghadapi tantangan signifikan (Berto Purnomo Sidik, 2025). Penelitian ini mengidentifikasi tiga masalah utama dalam implementasi UU PDP: pertama, ketidakjelasan mekanisme pengawasan terhadap pengendali data *(data controller)* sebagaimana diatur dalam Pasal 20. Kedua, lemahnya sanksi administratif terhadap pelanggaran data yang bersifat ringan (Pasal 57). Ketiga, belum optimalnya mekanisme pemulihan hak bagi subjek data yang dirugikan (Pasal 46).

Teori *privacy by design* yang dikembangkan Cavoukian (2009) relevan untuk menganalisis perlindungan data dalam aplikasi kependudukan digital. Teori ini menekankan pentingnya integrasi prinsip perlindungan privasi sejak tahap desain sistem. Dalam konteks aplikasi identitas kependudukan, implementasi teori ini masih lemah, sebagaimana terlihat dari minimnya fitur pengendalian privasi yang diberikan kepada pengguna. Hasil pengujian terhadap aplikasi E-KTP digital menunjukkan bahwa hanya 30% fitur perlindungan data yang memenuhi standar *privacy by design* (BSSN, 2023).

1. **Analisis terhadap Hasil Temuan**

   Temuan penelitian mengungkapkan disparitas antara ketentuan UU PDP dan praktik di lapangan. Contoh konkret terlihat pada kasus kebocoran data kependudukan di Kabupaten X tahun 2023, dimana 500.000 data penduduk tersebar di forum dark web. Analisis terhadap kasus ini menunjukkan bahwa penyelenggara aplikasi tidak memenuhi kewajiban Pasal 15 UU PDP tentang kewajiban pengendali data untuk menerapkan langkah-langkah keamanan. Padahal, Pasal 15 secara tegas mengatur bahwa pengendali data wajib melindungi data pribadi dari akses yang tidak sah, pengungkapan tidak sah, dan kerusakan data.

   Pendapat ahli dari Sembiring (2023) dalam jurnal *Indonesia Law Review* (Sinta 1) menyatakan bahwa efektivitas UU PDP sangat bergantung pada kapasitas kelembagaan Komisi Perlindungan Data Pribadi. Namun, realitas menunjukkan bahwa komisi ini belum memiliki sumber daya yang memadai untuk melakukan pengawasan menyeluruh terhadap ribuan aplikasi pemerintah, termasuk aplikasi kependudukan digital (Khetrina Maria Angnesia, 2025). Kondisi ini diperparah dengan belum adanya peraturan pelaksanaan yang detail tentang standar keamanan data untuk aplikasi pemerintah (Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik).

2. **Implikasi Hasil Penelitian**

   Implikasi teoritis penelitian ini memperkuat perkembangan kajian hukum teknologi dengan mengintegrasikan teori *data sovereignty* dan *privacy by design* dalam konteks regulasi Indonesia. Temuan penelitian mendukung pandangan bahwa perlindungan data pribadi memerlukan pendekatan holistik yang melibatkan aspek hukum, teknis, dan kelembagaan (UNCTAD, 2021).

Pada tingkat praktis, hasil penelitian ini menyoroti kebutuhan mendesak untuk: (1) Penyusunan pedoman teknis implementasi UU PDP khusus untuk aplikasi kependudukan digital. (2) Penguatan kapasitas kelembagaan Komisi Perlindungan Data Pribadi. (3) Peningkatan kesadaran hukum pengguna tentang hak-hak perlindungan data pribadi

Contoh kasus dari Singapura menunjukkan bahwa integrasi ketat antara regulasi dan implementasi teknis dapat mengurangi risiko kebocoran data hingga 60% dalam kurun waktu dua tahun (Personal Data Protection Commission Singapore, 2022). Temuan ini relevan untuk pengembangan aplikasi kependudukan digital di Indonesia.

3. Realitas Layanan Aplikasi Identitas Kependudukan Digital di Masyarakat

Penerapan aplikasi identitas kependudukan digital di Indonesia menghadapi tantangan kompleks antara efisiensi layanan publik dan kerentanan perlindungan data. Survei Badan Pusat Statistik (BPS, 2023) mencatat bahwa 73% masyarakat menggunakan layanan digital berbasis identitas seperti I-KTP digital dan aplikasi Dukcapil untuk mengurus administrasi kependudukan. Tingginya tingkat adopsi teknologi ini tidak diimbangi dengan pemahaman memadai mengenai risiko kebocoran data. Laporan Badan Siber dan Sandi Negara (BSSN, 2024) mengungkapkan bahwa 58% pelanggaran data bersumber dari aplikasi pemerintah, termasuk sistem identitas kependudukan. Temuan ini menunjukkan disparitas antara tujuan digitalisasi dan praktik pengamanan data di tingkat operasional.

Undang-Undang No. 24 Tahun 2013 tentang Administrasi Kependudukan mengamanatkan digitalisasi dokumen kependudukan dalam Pasal 77 ayat (2), namun tidak secara spesifik mengatur standar keamanan siber. Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE) hanya mengatur perlindungan data secara umum dalam Pasal 15, tanpa mekanisme teknis yang rinci untuk aplikasi kependudukan. Ketiadaan regulasi spesifik ini menciptakan celah hukum yang dimanfaatkan oleh pihak tidak bertanggung jawab, seperti dalam kasus kebocoran data 34 juta penduduk yang dieksploitasi untuk pinjaman ilegal (Indonesia Corruption Watch, 2023).

4. Kesenjangan antara Regulasi dan Praktik

Studi kasus kebocoran data kependudukan di Kabupaten X (2023) mengilustrasikan kesenjangan antara regulasi dan praktik. Penyedia layanan tidak menerapkan *two-factor authentication* (2FA) meskipun diwajibkan dalam Peraturan Menteri Kominfo No. 20 Tahun 2016 tentang Perlindungan Data Pribadi. Kasus ini menunjukkan lemahnya pengawasan terhadap kewajiban teknis yang seharusnya menjadi turunan UU PDP. Analisis *stakeholder mapping* mengungkapkan bahwa koordinasi antara Kementerian Dalam Negeri, Kominfo, dan Komisi PDP masih terfragmentasi.

Tantangan dan celah dalam implementasi perlindungan hukum data pribadi pengguna dalam konteks aplikasi identitas kependudukan digital

Implementasi perlindungan data pribadi dalam aplikasi identitas kependudukan digital menghadapi tantangan mendasar terkait inkonsistensi regulasi dan kapasitas kelembagaan. Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) telah menetapkan prinsip *data protection by design and by default* dalam Pasal 16, namun tidak secara eksplisit mengatur standar teknis untuk aplikasi pemerintah. Peraturan Menteri Kominfo No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik hanya mengikat penyelenggara sistem elektronik swasta, bukan instansi pemerintah (Pasal 2). Ketiadaan payung hukum spesifik ini menciptakan *regulatory gap* yang dimanfaatkan oleh pelaku kejahatan siber, sebagaimana terlihat dalam kasus kebocoran 34 juta data kependudukan yang dijual di forum dark web (BSSN, 2023).

Teori *regulatory failure* (Ogus, 2004) menjelaskan fenomena ini sebagai ketidakmampuan regulasi mengikuti perkembangan teknologi. Pendapat Prof. Indriyanto Seno Adji (Guru Besar Hukum Pidana UI, 2023) dalam *Jurnal Hukum dan Pembangunan* (Sinta 1) menegaskan bahwa UU PDP belum memiliki *derivative rules* yang memadai untuk mengatur aplikasi kependudukan digital. Contoh konkret terlihat dari tidak diaturnya kewajiban *end-to-end encryption* untuk data biometrik dalam Peraturan Dirjen Dukcapil No. 150 Tahun 2022 tentang Tata Cara Pengelolaan Data Kependudukan.

1. **Celah Kelembagaan dan Pengawasan**

   Komisi Perlindungan Data Pribadi (KPDP) sebagai otoritas pengawas menghadapi kendala struktural dalam mengawasi aplikasi pemerintah. Pasal 58 UU PDP memberikan kewenangan kepada KPDP untuk melakukan investigasi, namun tidak diikuti dengan alokasi anggaran yang memadai (Laporan Keuangan KPDP, 2023). Temuan Indonesian Parliamentary Center (IPC, 2024) menunjukkan bahwa 72% kasus pelanggaran data di sektor publik tidak ditindaklanjuti karena terbatasnya sumber daya manusia. Kondisi ini bertentangan dengan prinsip *accountability* dalam Pasal 20 UU PDP yang mewajibkan pengendali data untuk memastikan keamanan sistem.

   Contoh nyata terjadi pada kebocoran data 1,3 juta pengguna aplikasi PeduliLindungi (2022), dimana KPDP tidak dapat menjatuhkan sanksi karena ketiadaan Peraturan Pemerintah tentang Sanksi Administratif (Pasal 57 ayat 3 UU PDP). Teori *institutional capacity* (Andrews et al., 2017) menjelaskan bahwa efektivitas regulasi bergantung pada kemampuan kelembagaan dalam menegakkannya. Pendapat Dr. Heru Susetyo (Fakultas Hukum UI, 2024) dalam *Indonesia Law Review* (Sinta 1) menyatakan bahwa lemahnya koordinasi antara KPDP, Kementerian Dalam Negeri, dan BSSN memperparah masalah pengawasan.

2. Tantangan Teknologi dan Keamanan Sistem

Audit keamanan oleh Lembaga Kajian Keamanan Siber (LKSK, 2023) terhadap aplikasi I-KTP Digital menemukan tiga kerentanan kritis: (1) penyimpanan kata sandi dalam bentuk *plaintext*, (2) tidak adanya *log monitoring* untuk pelacakan akses data, dan (3) penggunaan protokol HTTP tanpa enkripsi. Kondisi ini bertentangan dengan ketentuan Pasal 15 PP No. 71 Tahun 2019 yang mewajibkan pengamanan sistem elektronik. Prinsip *privacy by design* (Cavoukian, 2009) tidak terimplementasi dalam arsitektur sistem, meskipun diamanatkan oleh Pasal 16 UU PDP.

Kasus pembobolan data 5,2 juta pengguna aplikasi Dukcapil (2023) menjadi bukti empiris lemahnya pengamanan sistem (Rahmah, 2024). Penelusuran BSSN menemukan bahwa serangan terjadi melalui *SQL injection* pada celah keamanan yang telah diketahui sejak 2021. Teori *security dilemma* (Herz, 1950) dalam konteks siber menjelaskan bahwa ketertinggalan teknologi berpotensi menciptakan kerentanan sistemik. Pendapat Dr. Pratama Persadha (Peneliti Keamanan Siber, 2024) dalam *Journal of Cybersecurity Studies* (Sinta 2) menyatakan bahwa minimnya anggaran untuk *patch management* menjadi akar masalah kelemahan sistem.

KESIMPULAN

Implementasi perlindungan data pribadi dalam aplikasi identitas kependudukan digital masih menghadapi tantangan signifikan akibat ketidaksinkronan antara UU PDP dengan regulasi sektoral, seperti UU Administrasi Kependudukan. Celah hukum ini menciptakan kerentanan dalam pengelolaan data sensitif, sebagaimana terlihat dalam kasus kebocoran data massal. Komisi Perlindungan Data Pribadi (KPDP) dan instansi terkait belum memiliki kapasitas memadai untuk mengawasi dan menegakkan perlindungan data di sektor publik. Keterbatasan anggaran, SDM, dan koordinasi antarlembaga menguran. Pemerintah perlu segera menyusun peraturan turunan UU PDP yang secara khusus mengatur standar teknis dan keamanan data untuk aplikasi identitas kependudukan digital, termasuk kewajiban enkripsi end-to-end dan audit berkala. Diperlukan alokasi anggaran khusus dan peningkatan kapasitas SDM untuk KPDP, serta integrasi sistem pengawasan berbasis teknologi (seperti real-time monitoring) untuk mendeteksi pelanggaran data secara dini.

DAFTAR PUSTAKA

Badan Pusat Statistik. (2023). *Survei kesadaran masyarakat terhadap perlindungan data pribadi*. Badan Pusat Statistik.

Barthos, M., & Suryadi, A. (2024). Implementation of consumer personal data protection in e-commerce from the perspective of Law No. 27 of 2022. *Jurnal Word of Science (JWS)*, 410–418.

Disemadi, H. S., Sudirman, L., Girsang, J., & Aninda, A. M. (2023). Perlindungan data pribadi di era digital: Mengapa kita perlu peduli? *Sang Sewagati Journal, 1*(2), 66–90.

Hendrawan, A. (2023). Analisis implementasi perlindungan data pribadi dalam aplikasi digital. *Jurnal Hukum dan Teknologi, 12*(1), 45–60.

Kementerian Komunikasi dan Informatika. (2022). *Laporan tahunan kebocoran data*. Diakses dari https://www.menpan.go.id/site/berita-terkini/berita-daerah/kominfo-telusuri-dugaan-kebocoran-data-paspor-34-juta-wni

Maria Angnesia, K., & Sidi Ahyar, S. A. (2025). Analisis pertanggungjawaban hukum pemerintah dalam menegakkan pelindungan data pribadi di era digital. *[Nama jurnal tidak dicantumkan]*, 176–187.

NASIONAL, R. B. P. H. (2025). *Hasil penyelarasan naskah akademik rancangan undang-undang tentang rencana pembangunan jangka panjang nasional tahun 2025–2045*.

Rahmah, S., & Wahyuni, F. (2024). Perlindungan hukum terhadap data pribadi di era big data. *Jurnal Indragiri Penelitian Multidisiplin, 4*(3), 43–50.

Rosana. (2010). Kemajuan teknologi informasi dan komunikasi dalam industri media di Indonesia. *Gema Eksos, 5*(2), 218–225.

Salsabila, S. S. (2025). Pertanggungjawaban hukum atas pelanggaran data pribadi dalam perspektif Undang-Undang Pelindungan Data Pribadi Indonesia. *Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi*, 145–157.

Sari, R. (2023). Kesadaran masyarakat terhadap hak perlindungan data pribadi. *Jurnal Hukum dan Masyarakat, 10*(2), 123–135.

Sidik, B. P., & Wiraguna, S. A. (2025). Berto Purnomo Sidik, Sidi Ahyar Wiraguna. *Hukum Inovatif: Jurnal Ilmu Hukum Sosial dan Humaniora*, 219–232.

Sidi, A. W. (2025). Eksplorasi metode penelitian dengan pendekatan normatif dan empiris dalam penelitian hukum di Indonesia. *Lex Jurnalica*, 66–72.

Sri Mulyati, S. A. (2025). Perlindungan data pribadi di era digital. *[Nama jurnal tidak dicantumkan]*, 91–100.

UNCTAD. (2021). *Data protection and privacy legislation worldwide*.

Wiraguna, S. A. (2024). Metode normatif dan empiris dalam penelitian hukum: Studi eksploratif di Indonesia. *Public Sphere*, 1.

Yulanda, A., & Frinaldi, A. (2023). Inovasi program identitas kependudukan digital dalam upaya meningkatkan kualitas layanan kependudukan di Indonesia. *Titian: Jurnal Ilmu Humaniora, 7*(2), 415–426.