VOLUME 26 NO 2 DESEMBER 2025 ISSN CETAK 1412-6877
ISSN ONLINE 2528-0538

DAMPAK PERKEMBANGAN TEKNOLOGI TERHADAP SISTEM PEMBUKTIAN DALAM PROSES PIDANA: STUDI KASUS *CYBERCRIME*

Elvi Susanti Syam[1], Asfiani.B[2], Asfendi Wijaya Abu Bakar[3]

[1,2,3] Magister Ilmu Hukum, Institut Andi Sapada, Parepare, Indonesia

Email :
elvisusantisyam@gmail.com[1], asfianib1703@gmail.com[2], wijayaasfendi123@gmaill.com[3]

==========

ABSTRACT

The advancement of digital technology has transformed the paradigm of criminal evidence systems in Indonesia, shifting from conventional physical evidence toward complex and cross-border electronic evidence. This study aims to analyze the effectiveness and adaptability of Indonesia's criminal evidentiary framework in responding to the dynamics of digital evidence in the cyber era. This research employs a qualitative legal method through a literature-based approach, examining the Criminal Procedure Code (KUHAP), the Electronic Information and Transactions Law, and its implementing regulations, complemented by an analysis of empirical findings and international practices.

The results reveal that Indonesia's evidentiary system remains rooted in traditional models and has yet to fully respond to the distinctive characteristics of digital evidence, which demand authenticity, integrity, and data security. Regulatory fragmentation, limited technical capacity among law enforcement officers, and the absence of national authentication standards constitute major obstacles to the effectiveness of electronic evidence. This study underscores the urgency of reforming the criminal procedure law toward an integrated digital evidentiary system through the establishment of a Digital Chain Management System and the reinforcement of digital forensic ethics. The findings are expected to contribute to the development of a more adaptive criminal procedural law that ensures substantive justice in technology-based law enforcement in Indonesia.

Keywords electronic evidence, criminal proof, criminal procedure law, cybercrime.

ABSTRAK

Perkembangan teknologi digital telah mengubah paradigma sistem pembuktian pidana di Indonesia, dari bukti konvensional menuju bukti elektronik yang kompleks dan lintas batas. Penelitian ini bertujuan menganalisis efektivitas dan adaptabilitas kerangka hukum pembuktian pidana nasional terhadap dinamika bukti digital di era siber. Metode yang digunakan ialah penelitian hukum kualitatif berbasis studi pustaka, dengan menelaah ketentuan dalam KUHAP, Undang-Undang Informasi dan Transaksi Elektronik, serta berbagai peraturan pelaksananya, disertai analisis terhadap temuan empiris dan praktik internasional.

Hasil penelitian menunjukkan bahwa sistem pembuktian di Indonesia masih berorientasi pada model klasik dan belum sepenuhnya responsif terhadap karakteristik bukti digital yang menuntut keotentikan, integritas, dan keamanan data. Fragmentasi regulasi, keterbatasan kapasitas aparat penegak hukum, dan absennya standar autentikasi nasional menjadi kendala utama yang menghambat efektivitas pembuktian elektronik. Penelitian ini menegaskan perlunya reformasi hukum acara pidana menuju sistem pembuktian digital yang terpadu melalui pembentukan Digital Chain Management System serta penguatan etika forensik digital. Hasil kajian ini diharapkan berkontribusi terhadap pengembangan hukum acara pidana yang lebih adaptif dan menjamin keadilan substantif dalam penegakan hukum berbasis teknologi di Indonesia.

Kata Kunci : bukti elektronik, pembuktian pidana, hukum acara pidana, kejahatan siber

1. PENDAHULUAN

Perkembangan layanan digital di Indonesia mengalami peningkatan yang sangat cepat. Pertumbuhan tersebut terutama terlihat pada sektor e-commerce, fintech, dan layanan pembayaran berbasis digital. Penggunaan QRIS memperlihatkan lonjakan yang sangat tinggi dalam kurun satu tahun terakhir dengan pertumbuhan mencapai 162% hingga 226%, yang menunjukkan semakin banyaknya pengguna dan merchant yang beralih ke metode transaksi nontunai. Nilai transaksi digital banking juga meningkat pesat hingga mencapai triliunan rupiah, dengan pertumbuhan tahunan berada pada kisaran 19% sampai 35%. Perubahan ini menjadi penanda bahwa aktivitas ekonomi kini semakin bertumpu pada transaksi elektronik (Komdigi, 2024).

Kemajuan tersebut tidak datang tanpa ancaman. Peningkatan kasus kebocoran dan penyalahgunaan data pribadi semakin sering terjadi bersamaan dengan bertambahnya aktivitas digital masyarakat(Mugiono & Wiraguna, 2025). Beberapa kasus besar mencuat di ruang publik seperti kebocoran data kependudukan Ditjen Dukcapil serta data NPWP jutaan wajib pajak yang melibatkan data pejabat tinggi negara bahkan hingga Presiden(Sitorus et al., 2025). Data yang bocor diperjualbelikan melalui platform ilegal dan dark web, sehingga memunculkan resiko besar bagi keamanan dan privasi pemilik data (Lawidya, 2024).

Kerugian yang ditimbulkan tidak hanya menyasar individu tetapi juga perusahaan dan negara. Masyarakat yang terdampak berpotensi mengalami kehilangan dana akibat penipuan digital, ancaman pada reputasi, dan tekanan psikologis yang memengaruhi kondisi mental korban. Perusahaan yang mengalami insiden serupa kehilangan kepercayaan publik serta menghadapi potensi penurunan nilai perusahaan. Pada lingkup lebih luas, kondisi tersebut dapat mengurangi kepercayaan masyarakat terhadap ekosistem digital yang sedang dibangun pemerintah (Erikha & Hoesein, 2025).

Kebutuhan akan penguatan perlindungan data menjadi semakin mendesak. UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi diharapkan mampu menjadi instrumen kuat yang memberikan hak lebih tegas bagi masyarakat dalam mengendalikan data pribadinya. Selain itu, UU tersebut juga memberikan kewajiban bagi pengendali data agar memperlakukan

data secara aman dan bertanggung jawab. Dengan adanya landasan hukum yang jelas, diharapkan ekosistem transaksi elektronik di Indonesia menjadi lebih aman dan terpercaya (Manurung & Thalib, 2022).

Ancaman serangan digital pada infrastruktur teknologi di Indonesia masih sangat tinggi. Tercatat sekitar 133,4 juta serangan siber yang menargetkan berbagai sektor penting pada tahun 2025. Serangan tersebut meliputi eksploitasi celah keamanan sistem, serangan DDoS, hingga malware pencuri data seperti infostealer yang banyak menyasar sektor finansial dan layanan digital lainnya. Beberapa di antaranya memanfaatkan celah zero-day yang belum memiliki pembaruan keamanan, sehingga sistem menjadi rentan ditembus dan rawan menyebabkan kebocoran data dalam skala luas (R. P. Sari, 2025).

Pelaku usaha digital belum sepenuhnya menerapkan standar keamanan yang baik sebagaimana diamanatkan regulasi. Kewajiban seperti enkripsi data, audit keamanan secara berkala, hingga pembentukan tim respons insiden siber masih sering diabaikan. Kendala yang sering ditemukan antara lain kurangnya pemahaman teknis, minimnya anggaran khusus keamanan, dan lemahnya pengawasan dari pemerintah. Sektor swasta terutama UMKM butuh percepatan penerapan standar keamanan nasional agar mampu melindungi data pengguna dengan optimal (Sihotang et al., 2025).

Kemampuan masyarakat dalam menjaga keamanan data pribadi juga belum merata. Banyak pengguna internet yang masih belum memahami bahaya memberikan data sembarangan pada aplikasi yang tidak kredibel. Pola penggunaan kata sandi yang mudah ditebak, kebiasaan mengklik tautan tidak jelas, serta rendahnya kewaspadaan terhadap modus phishing menyebabkan masyarakat menjadi sasaran empuk para pelaku kejahatan siber. Program peningkatan pemahaman keamanan digital secara nasional diperlukan agar pengguna aktif berperan melindungi dirinya sendiri ketika beraktivitas secara daring (Fitriana et al., 2025).

Maraknya pelanggaran yang berlangsung terus menerus memperlihatkan bahwa keberadaan undang-undang saja tidak cukup. Masih banyak insiden kebocoran yang disebabkan kelalaian internal, kesalahan teknis, maupun tindakan dari orang dalam organisasi itu sendiri. Upaya perlindungan data membutuhkan pendekatan menyeluruh yang menggabungkan kesiapan sistem, aparat penegak hukum yang responsif, komitmen pelaku usaha, serta kepatuhan seluruh pengguna layanan digital dalam menjaga haknya atas data pribadi (Wildan et al., 2024).

Status implementasi UU PDP belum menunjukkan hasil yang efektif. Kelemahan paling utama terletak pada belum lengkapnya aturan pelaksana seperti peraturan pemerintah sebagai pedoman teknis. Banyak ketentuan dalam undang-undang yang belum dapat diterapkan secara jelas karena menunggu penyusunan prosedur operasional yang memadai. Standar keamanan yang wajib diterapkan, tata kelola data yang harus diikuti, serta mekanisme penegakan sanksi belum bekerja maksimal sehingga pelanggaran masih kerap terjadi di berbagai sektor (Cahyani & Marianata, 2024).

Lembaga pengawas yang diamanatkan dalam regulasi yaitu Badan Perlindungan Data Pribadi juga belum beroperasi penuh sebagai otoritas yang memiliki kekuatan untuk mengendalikan dan menegakkan aturan. Ketiadaan lembaga yang kuat membuat tindak

ISSN CETAK 1412-6877
ISSN ONLINE 2528-0538

pelanggaran sering tidak diikuti dengan sanksi yang tegas. Ketidakseimbangan antara aturan yang sudah berlaku dengan kenyataan di lapangan memperlihatkan bahwa perlindungan data di Indonesia masih dalam tahap awal dan membutuhkan penguatan serius pada sistem pengawasan dan penegakan.

Fenomena penyalahgunaan data yang semakin kompleks memperlihatkan adanya kesenjangan besar antara kebutuhan perlindungan hukum dan kondisi sistem saat ini. Penelitian terhadap efektivitas UU PDP menjadi penting untuk menjawab apakah regulasi telah dijalankan sesuai tujuan pembentukannya. Analisis yang mendalam dapat menjadi rujukan bagi pemerintah dan seluruh pemangku kepentingan dalam memperbaiki kelemahan implementasi guna memastikan keamanan data masyarakat tetap terjaga seiring meningkatnya transaksi elektronik di Indonesia.

2. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan peraturan perundang-undangan dan analisis konseptual. Kajian dilakukan melalui penelusuran bahan hukum primer seperti UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi dan regulasi terkait tata kelola transaksi elektronik, serta bahan hukum sekunder berupa publikasi ilmiah, laporan resmi, dan data valid mengenai serangan siber dan penyalahgunaan data di Indonesia. Analisis dilakukan secara kualitatif dengan menelaah kesesuaian antara pengaturan hukum dan kondisi faktual penegakan perlindungan data dalam perkembangan transaksi elektronik, sehingga dapat menilai efektivitas pembentukan norma dan pelaksanaannya di lapangan.

3. HASIL PENELITIAN DAN PEMBAHASAN

A. Efektivitas Undang-Undang Nomor 27 Tahun 2022 dalam Menangani Penyalahgunaan Data Pribadi pada Transaksi Elektronik

Pengaturan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menegaskan bahwa data pribadi meliputi baik data umum seperti nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, maupun data spesifik yang lebih sensitif, seperti data kesehatan, biometrik, genetika, catatan kejahatan, data anak dan data keuangan pribadi. Regulasi ini berlaku bagi setiap orang, badan publik, maupun organisasi internasional yang mengumpulkan, menyimpan, memproses atau mengungkapkan data pribadi warga negara Indonesia, baik secara elektronik maupun nonelektronik (Suryanto & Riyanto, 2024).

Prinsip pemrosesan data pribadi dalam undang-undang tersebut meliputi legalitas, yaitu bahwa pemrosesan harus memiliki dasar hukum/transparansi, artinya subjek data diberitahu secara jelas jenis data, tujuan, jangka waktu pemrosesan; pembatasan tujuan, akurasi dan kelengkapan data, keamanan, dan akuntabilitas pihak pengolah data. Ketaatan kepada prinsip-prinsip ini menjadi tolok ukur sejauh mana pengendali maupun prosesor data menjalankan kewajiban mereka dalam melindungi informasi pribadi individu secara memadai (Rauf et al., 2025).

Kewajiban pengendali data dikodifikasikan dengan cukup mendetail dalam undang-undang, termasuk memiliki dasar pemrosesan yang sah seperti persetujuan eksplisit dari subjek data, pelaksanaan perjanjian, pelaksanaan kewajiban

hukum, perlindungan kepentingan vital, dan kepentingan umum atau sah lainnya. Pengendali data juga wajib memberikan informasi seperti rincian jenis data yang dikumpulkan, jangka waktu pemrosesan, serta hak subjek data terhadap informasi tersebut (Nurhabibah et al., 2023).

Di lain pihak, prosesor data wajib bertindak berdasarkan instruksi pengendali dan menjaga keamanan data sesuai ketentuan yang berlaku. Hak subjek data pribadi ditegaskan dalam undang-undang ini, di antaranya hak untuk memperoleh akses terhadap data yang diproses, hak memperbaiki atau memperbarui data yang tidak akurat, hak menghapus atau memusnahkan data apabila tidak lagi diperlukan atau pemrosesan tidak sah, serta hak menarik persetujuan dan menolak pemrosesan otomatis yang berdampak signifikan.

Maka dari itu, individu memiliki kontrol yang lebih besar atas bagaimana data pribadinya digunakan oleh pengendali maupun prosesor. Sanksi administratif dan pidana yang diatur menunjukkan komitmen pembuat undang-undang untuk memberikan efek jera. Sanksi administratif mencakup teguran tertulis, penghentian sementara pemrosesan data, penghapusan atau pemusnahan data, dan denda administratif hingga dua persen dari pendapatan tahunan pelaku pelanggaran.

Pelanggaran berat yang menimbulkan kerugian signifikan dapat dikenakan sanksi pidana. Subjek data juga dapat mengajukan gugatan perdata akibat kerugian yang dialaminya. Kekuatan dari undang-undang ini terletak pada kejelasan norma mengenai hak, kewajiban dan sanksi yang sebelumnya belum terintegrasi secara sistematis. Substansi hukum sudah mencakup aspek jenis data, pemrosesan, kewajiban dan hak subjek data. Namun kelemahannya terletak pada struktur implementasi, terutama aturan pelaksana yang masih belum sepenuhnya diterbitkan sehingga banyak ketentuan teknis belum optimal dijalankan (Fikri & Rusdiana, 2023).

Dalam praktik sehari-hari, muncul kebiasaan masyarakat yang membagikan data pribadi secara bebas tanpa mempertimbangkan risiko yang melekat. Contohnya publik membagikan nomor KTP, foto, alamat, nomor telepon, atau informasi keuangan di platform digital atau media sosial tanpa proteksi yang memadai, sehingga memicu vulnerabilitas data pribadi terhadap kebocoran dan penyalahgunaan. Rendahnya literasi digital dan kesadaran keamanan memperparah situasi ini karena pengguna tidak memahami cara menjaga data pribadinya dengan benar (Adelika & Nurbaiti, 2023).

Pelaku usaha pun belum sepenuhnya mematuhi ketentuan undang-undang tersebut. Banyak perusahaan mengumpulkan data secara massal tanpa transparansi, kurang melakukan audit risiko atau menerapkan sistem keamanan yang memadai. Beberapa praktik ilegal seperti jual beli data pribadi masih ditemukan, padahal undang-undang secara tegas melarang pengungkapan atau pendistribusian data yang dilakukan tanpa izin subjek (Ritonga, 2024).

Tingkat kepatuhan yang rendah ini menjadi hambatan utama dalam mencapai perlindungan data yang efektif.Kondisi kelembagaan masih menunjukkan tantangan besar. Lembaga otoritas pengawas khusus belum berdiri secara penuh meskipun undang-undang mengamanatkan pembentukan lembaga tersebut, termasuk wewenang pengawasan,

penegakan sanksi, penyelesaian sengketa serta kerja sama internasional. Tanpa struktur pengawasan yang kuat, fungsi kontrol, audit dan penegakan hukum atas pelanggaran data pribadi menjadi kurang optimal dan implementasi undang-undang terganggu (Rusmanto et al., 2025).

Analisis menggunakan kerangka teori efektivitas hukum dari Soerjono Soekanto menunjukkan bahwa substansi undang-undang sudah mencakup aspek norma, namun struktur pelaksanaannya masih lemah dan budaya atau kultur hukum masyarakat serta pelaku usaha belum mendukung sepenuhnya. Kultur kepatuhan yang rendah, kesadaran masyarakat yang terbatas, dan kondisi teknis pelaksanaan yang belum matang mengakibatkan gap antara norma dan praktik nyata di lapangan. (H. P. Sari et al., 2024)

Pada akhirnya, efektivitas keseluruhan undang-undang ini masih dapat disebut sebagai "cukup efektif" karena meskipun fondasi hukum telah terbentuk, implementasi dan penegakan masih menghadapi kendala besar (Sangojoyo et al., 2022). Perbaikan harus ditunjukkan melalui penerbitan aturan pelaksana secara cepat, pembentukan lembaga pengawas yang kredibel, serta program edukasi masyarakat dan pelaku usaha yang berkelanjutan agar norma hukum benar-benar hidup dan memberikan perlindungan data pribadi sesuai harapan.

B. Hambatan Implementasi dan Upaya Optimalisasi Penegakan Hukum UU Perlindungan Data Pribadi dalam Kasus Penyalahgunaan Data pada Transaksi Elektronik

Perkembangan transaksi elektronik di Indonesia mendorong pertumbuhan ekosistem digital yang semakin luas, mulai dari layanan *e-commerce*, *perbankan digital*, *fintech*, hingga aplikasi kesehatan dan transportasi. Interaksi masyarakat yang semakin intens di ruang digital berimplikasi pada meningkatnya volume data pribadi yang diproses setiap hari. Situasi ini menuntut adanya perlindungan hukum yang mampu menjaga privasi dan keamanan data secara memadai agar kepercayaan publik terhadap layanan digital tetap terjaga (Widjaya & Fasa, 2025).

Namun, pertumbuhan pemanfaatan teknologi belum diiringi dengan peningkatan literasi privasi data masyarakat. Banyak pengguna platform digital yang masih dengan mudah membagikan informasi sensitif seperti foto KTP, nomor induk kependudukan, alamat rumah, hingga identitas rekening bank melalui media sosial maupun aplikasi pesan. Kebiasaan ini memperbesar peluang data tersebut dicuri atau disalahgunakan oleh pihak yang tidak bertanggung jawab dalam skema kejahatan seperti pemalsuan identitas dan penipuan daring (Terniawan, 2025).

Kerentanan publik semakin diperparah oleh kecenderungan memberikan izin akses data tanpa membaca syarat ketentuan pada aplikasi digital. Ketika suatu aplikasi meminta akses kamera, lokasi, atau daftar kontak, pengguna sering kali langsung menyetujui demi kemudahan layanan. Padahal, praktik tersebut membuka celah bagi aplikasi untuk mengumpulkan dan mendistribusikan data tanpa pengawasan yang jelas, sehingga risiko kebocoran semakin besar (Haria, 2021).

Pada sisi pelaku usaha, masih terdapat banyak perusahaan dan platform daring yang belum menerapkan tata kelola keamanan data secara memadai. Penyimpanan data dilakukan tanpa enkripsi yang kuat, pembaruan

sistem keamanan tidak dilakukan berkala, dan proses audit internal kerap diabaikan. Praktik yang kurang disiplin tersebut meningkatkan peluang terjadinya serangan siber maupun pemanfaatan data secara ilegal oleh pihak internal.

Meningkatnya kasus kebocoran data, yang melibatkan lembaga besar dan penyedia sistem elektronik strategis, menunjukkan urgensi penerapan regulasi yang ketat terhadap pengendalian data pribadi di Indonesia. Ketiadaan kontrol yang memadai mengakibatkan banyak insiden kebocoran tidak terlaporkan, bahkan korban tidak mengetahui bahwa datanya telah bocor dan dimanfaatkan untuk tujuan criminal (Maharani & Prakoso, 2024).

Keberadaan Undang-Undang Perlindungan Data Pribadi menjadi langkah penting untuk memperbaiki kondisi tersebut karena menyediakan payung hukum dalam pengelolaan data pribadi. Akan tetapi, efektifitasnya belum maksimal karena masih terdapat ruang yang belum diatur secara detail dalam praktik teknis. Regulasi ini perlu diterjemahkan ke dalam instruksi operasional yang jelas agar pengendali data dapat menjalankan kewajiban perlindungan secara konsisten (Yaw et al., 2025).

Belum terbitnya aturan pelaksana seperti peraturan pemerintah, peraturan menteri, serta pedoman teknis menjadi hambatan utama bagi pelaksanaan perlindungan data pribadi secara konkret di lapangan. Tanpa SOP yang baku terkait pemrosesan data, standar keamanan, dan pelaporan insiden, pelaku usaha tidak memiliki pedoman komprehensif untuk memastikan kepatuhan terhadap UU PDP. (Khair & Wiraguna, 2025)

Selain itu, definisi dan terminologi dalam UU PDP masih menyisakan ruang multitafsir. Perbedaan pemahaman mengenai istilah seperti “pengendali data”, “pemroses data”, hingga klasifikasi “data sensitif” berpotensi menciptakan ketidaksinkronan dalam penerapan hukum. Aparat penegak hukum, pelaku usaha, dan lembaga pemerintah dapat memiliki interpretasi berbeda sehingga implementasi kebijakan tidak terarah secara seragam (Falahudin, 2023).

Penguatan perlindungan data pribadi juga terhambat oleh kapasitas sumber daya manusia yang belum memadai. Keterbatasan tenaga ahli digital forensic, auditor privasi, dan investigator siber membuat proses penanganan pelanggaran data berlangsung lambat dan kurang efektif. Padahal, kejahatan digital membutuhkan respons profesional yang cepat dan presisi tinggi.

Koordinasi antar lembaga yang terlibat dalam pengawasan data juga masih belum optimal. Beragamnya regulasi dan otoritas yang memegang kewenangan di bidang digital menyebabkan fragmentasi penanganan saat insiden kebocoran terjadi. Tanpa alur koordinasi yang terintegrasi, proses identifikasi pelaku dan pemulihan hak korban sering kali terhambat oleh birokrasi dan kendala teknis (Sabila & Atman, 2025).

Upaya penegakan hukum terhadap pelanggaran data pribadi belum mampu memberikan efek jera yang kuat. Banyak kasus berhenti di tahap investigasi tanpa sanksi tindak lanjut. Selain itu, kesadaran publik tentang hak privasi masih rendah sehingga tekanan masyarakat untuk menindak pelanggaran belum berkembang secara signifikan. Tanpa dukungan penegakan yang tegas dan partisipasi publik yang kuat, tujuan perlindungan data yang efektif belum sepenuhnya tercapai (Sidik & Wiraguna, 2025).

ISSN CETAK 1412-6877
ISSN ONLINE 2528-0538

4. PENUTUP

1. Berdasarkan hasil analisis, efektivitas UU Perlindungan Data Pribadi dalam menangani penyalahgunaan data pada transaksi elektronik masih belum optimal. Walaupun UU PDP telah memberikan dasar hukum yang kuat mengenai hak subjek data dan kewajiban pengendali data, penerapannya belum mampu menjawab tantangan yang terus berkembang di era digital. Kebiasaan masyarakat yang masih sering membagikan data pribadi secara sembarangan, minimnya literasi privasi, serta lemahnya tata kelola keamanan data pada berbagai platform digital berkontribusi terhadap tingginya risiko kebocoran dan penyalahgunaan data dalam transaksi elektronik.

2. Hambatan dalam penerapan UU PDP juga bersumber dari belum tersedianya pedoman teknis, kapasitas sumber daya manusia yang belum memadai, lemahnya koordinasi antar lembaga, serta mekanisme penegakan hukum yang belum memberikan efek jera. Kekosongan operasional akibat belum terbentuknya lembaga pengawas independen menyebabkan pelaporan dan penanganan insiden sering terlambat dan tidak konsisten. Oleh karena itu, percepatan penerbitan regulasi turunan, peningkatan kompetensi aparat dan pelaku usaha, serta penguatan kesadaran masyarakat menjadi faktor kunci untuk memastikan perlindungan data pribadi berjalan efektif dan memberikan kepastian hukum yang nyata di Indonesia.

DAFTAR PUSTAKA

Adelika, A., & Nurbaiti, N. (2023). Upaya Pencegahan Terjadinya Pencurian Data Pada E-Ktp Bagi Penduduk Pada Dinas Kependudukan Dan Pencatatan Sipil Kota Medan. *Jurnal Pengabdian Masyarakat Khatulistiwa*, *6*(2), 124–133.

Cahyani, W. D., & Marianata, A. (2024). Analisis Kebijakan Perlindungan Data Pribadi Di Kota Bengkulu: Studi Implementasi UU PDP Dalam Era Digital. *Jurnal Kajian Hukum Dan Kebijakan Publik| E-ISSN: 3031-8882*, *2*(1), 623–626.

Erikha, A., & Hoesein, Z. A. (2025). Strategi pencegahan kebocoran data pribadi melalui peran Kominfo dan gerakan Siberkreasi dalam edukasi digital. *Jurnal Retentum*, *4*(1), 48–64.

Falahudin, A. R. (2023). *Analisis yuridis undang-undang nomor 27 tahun 2022 tentang perlindungan data pribadi perspektif Maqoshid Syariah*. Universitas Islam Negeri Maulana Malik Ibrahim.

Fikri, M., & Rusdiana, S. (2023). Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Posistif Indonesia. *Ganesha Law Review*, *5*(1), 39–57.

Fitriana, D. Z. W., Pradipta, F., Wulandari, H., Setyawati, Y. A., & Billah, M. B. (2025). *Peningkatan Kesadaran Anti-Phising Melalui Aplikasi Truecaller Di Era Digitalisasi Pada Kelurahan Gunung Sari*.

Haria, P. (2021). *Perancangan Aplikasi Pemesanan Dan Penyewaan Lapangan Badminton Di Kota Batam Berbasis Android*. Prodi Teknik Informatika.

Khair, F., & Wiraguna, S. A. (2025). Data Protection Impact Assessment

(DPIA) sebagai Instrumen Kunci Menjamin Kepatuhan UU PDP 2022 di Indonesia. *Politika Progresif: Jurnal Hukum, Politik Dan Humaniora*, *2*(2), 246–254.

Komdigi. (2024). *Transaksi QRIS Melonjak 226,54%, Revolusi Pembayaran Digital di Indonesia*. Komdigi RI. https://www.komdigi.go.id/berita/ekonomi-digital/detail/transaksi-qris-melonjak-22654-revolusi-pembayaran-digital-di-indonesia

Lawidya, A. T. (2024). *KEBIJAKAN SATU DATA UNTUK MENINGKATKAN KUALITAS PELAYANAN PUBLIK (STUDI TENTANG INTEGRASI NOMOR INDUK KEPENDUDUKAN DAN NOMOR POKOK WAJIB PAJAK)*. Universitas Muhammadiyah Malang.

Maharani, R., & Prakoso, A. L. (2024). Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital. *Jurnal USM Law Review*, *7*(1), 333–347.

Manurung, E. A. P., & Thalib, E. F. (2022). Tinjauan yuridis perlindungan data pribadi berdasarkan UU nomor 27 tahun 2022. *Jurnal Hukum Saraswati*, *4*(2), 139–148.

Mugiono, M., & Wiraguna, S. A. (2025). Between Ease and Vulnerability: Juridical Analysis of Population Identity Data Protection in Digital Applications: Antara Kemudahan dan Kerentanan: Analisis Yuridis Perlindungan Data Identitas Kependudukan dalam Aplikasi Digital. *COSMOS: Jurnal Ilmu Pendidikan, Ekonomi Dan Teknologi*, *2*(3), 684–691.

Nurhabibah, N. I., Rosadi, S. D., & Nasution, F. U. (2023). Tanggung Jawab Pengendali Data Dalam Memberikan Pelindungan Data Pribadi Anak di Indonesia: Studi Komparasi Negara Inggris. *MORALITY: Jurnal Ilmu Hukum*, *9*(2), 207–223.

Rauf, A., Annah, A., Hardi, H., & Mudarsep, M. (2025). Pelindungan Hukum Terhadap Data Pribadi Di Indonesia. *SISITI: Seminar Ilmiah Sistem Informasi Dan Teknologi Informasi*, *14*(2), 117–126.

Ritonga, P. (2024). Transparansi Dan Akuntabilitas: Peran Audit Dalam Meningkatkan Kepercayaan Stakeholder. *Equilibrium: Jurnal Ilmiah Ekonomi, Manajemen Dan Akuntansi*, *13*(2), 323–336.

Rusmanto, W., Sos, S., Permatasari, A., Sos, S., Sopandi, E., & Sos, S. (2025). *Governansi Digital*. PT Penerbit Qriset Indonesia.

Sabila, S. N., & Atman, W. (2025). Studi Kasus Kebocoran Data SIM Card oleh Bjorka: Dampaknya terhadap Kepercayaan Publik terhadap Keamanan Digital di Indonesia. *Sosial Simbiosis: Jurnal Integrasi Ilmu Sosial Dan Politik*, *2*(3), 142–154.

Sangojoyo, B. F., Kevin, A., & Sunlaydi, D. B. (2022). Urgensi pembaharuan hukum mengenai perlindungan data pribadi e-commerce di Indonesia. *Kosmik Hukum*, *22*(1), 27–39.

Sari, H. P., Mulyani, D. I., Nilamsari, M. A., Sitorus, D. D. F., & Harimurti, Y. W. (2024). Efektivitas Hukum Perlindungan Data Pribadi Terhadap Kejahatan Siber di Indonesia. *Jurnal Media Akademik (JMA)*, *2*(12).

Sari, R. P. (2025). *Ancaman Digital 2025: 133,4 Juta Serangan Siber Terjadi di RI*. Cyberhub.Id. https://cyberhub.id/berita/ancaman-digital-2025-serangan-siber-ri

Sidik, B. P., & Wiraguna, S. A. (2025). Tinjauan Hukum terhadap Aplikasi

Digital sebagai Upaya Meningkatkan Kesadaran Perlindungan Hak Privasi Data Pribadi. *Hukum Inovatif: Jurnal Ilmu Hukum Sosial Dan Humaniora*, *2*(2), 219–232.

Sihotang, H. T. M., Putri, M. A., & Riwanda, N. (2025). Pentingnya Keamanan Data Pada Bisnis Digital: Regulasi, Tantangan, dan Implementasi di Indonesia. *Jebital: Jurnal Ekonomi Dan Bisnis Digital*, *2*(2), 34–48.

Sitorus, H. R. P., Lumbanbatu, D. P., Sidebang, D. D., Pratama, D. E., & Gaol, R. S. L. (2025). Tinjauan Hukum dan Upaya Pencegahan terhadap Kasus Kebocoran Data NPWP. *ASPIRASI: Publikasi Hasil Pengabdian Dan Kegiatan Masyarakat*, *3*(4), 14–18.

Suryanto, D., & Riyanto, S. (2024). Implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dalam Industri Ritel Tinjauan terhadap Kepatuhan dan Dampaknya pada Konsumen. *Veritas*, *10*(1), 121–135.

Terniawan, D. (2025). KTP dalam genggaman: Revolusi akses layanan adminduk di era digital. *Jurnal Ilmu Sosial Dan Humaniora*, *3*(2), 170–183.

Widjaya, M. A., & Fasa, M. I. (2025). Analisis Peran E-commerce dalam Mendorong Pertumbuhan Ekonomi Digital di Indonesia. *Jurnal Bersama Ilmu Ekonomi (EKONOM)*, *1*(2), 96–102.

Wildan, M., Ramadhan, D. R. C., & Wijayanti, Z. R. (2024). Analisis Tanggung Jawab Bank Terhadap Kebocoran Data Nasabah: Ditinjau Dalam Perspektif Hukum Perbankan. *Media Hukum Indonesia (MHI)*, *2*(4).

Yaw, T., YB, S. B., Sampurna, A., & Utami, L. S. (2025). Tanggung Jawab Hukum atas Penyalahgunaan Consent oleh Pelaku Telemarketing dalam Perspektif Undang-Undang Perlindungan Data Pribadi. *Journal of Syntax Literate*, *10*(6).