



Paradigma Daktiloskopi Kontemporer: Antara Efisiensi Administrasi dan Privasi Warga Negara

Ferry Candra^{1*}, Ratna Artha Windari², Oloan C.H Marpaung³

¹⁻²Program Studi Ilmu Hukum, Fakultas Hukum dan Ilmu Sosial, Universitas Pendidikan Ganesha, Indonesia

³Sub Bagian Tata Usaha Direktorat Jenderal Pidana, Kementerian Hukum Republik Indonesia

*Penulis Korespondensi: ferry.candra@student.ac.id

Abstract. *This study discusses the contemporary paradigm of non-criminal fingerprint use in Indonesia by highlighting the dialectic between state administrative efficiency and the protection of citizens' privacy. Through an interdisciplinary approach integrating technical, legal, and social perspectives, this research analyzes the implementation of e-KTP, which has recorded more than 270 million citizens in a centralized biometric database, as well as the expansion of fingerprint usage in banking, telecommunications, e-SIM, and various other public service sectors. The analysis results indicate that non-criminal fingerprinting provides significant benefits in improving operational efficiency, preventing fraud, and strengthening security. However, its implementation also creates serious privacy risks, including the irreversible nature of biometric data, vulnerability to spoofing, single-modal system accuracy ranging from 87–92%, and the potential for mass surveillance. Law Number 27 of 2022 on Personal Data Protection represents an important advancement in the national legal framework; however, its implementation still faces challenges due to the lack of an optimal independent supervisory authority and incomplete implementing regulations. This study recommends strengthening data governance, implementing privacy by design, adopting multimodal biometrics, ensuring transparency in data management, limiting usage based on the principle of proportionality, improving digital literacy, and harmonizing regulations with international standards to maintain a balance between technological innovation and citizens' fundamental right to privacy.*

Keywords: *Biometrics; Data Privacy; Data Protection; Fingerprints; Regulation.*

Abstrak. Penelitian ini membahas paradigma kontemporer penggunaan sidik jari nonkriminal di Indonesia dengan menyoroti dialektika antara efisiensi administrasi negara dan perlindungan privasi warga negara. Melalui pendekatan interdisipliner yang mengintegrasikan perspektif teknis, hukum, dan sosial, penelitian ini menganalisis implementasi e-KTP yang telah merekam lebih dari 270 juta penduduk dalam basis data biometrik terpusat, serta perluasan penggunaan sidik jari pada sektor perbankan, telekomunikasi, e-SIM, dan berbagai layanan publik lainnya. Hasil analisis menunjukkan bahwa sidik jari nonkriminal memberikan manfaat signifikan dalam meningkatkan efisiensi operasional, mencegah penipuan, dan memperkuat keamanan. Namun, penerapannya juga menimbulkan risiko serius terhadap privasi, seperti sifat data biometrik yang tidak dapat diubah, kerentanan terhadap pemalsuan, akurasi sistem tunggal yang masih berkisar 87–92%, serta potensi pengawasan massal. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menjadi kemajuan penting dalam kerangka hukum nasional, tetapi implementasinya masih menghadapi tantangan akibat belum optimalnya lembaga pengawas independen dan regulasi pelaksana. Penelitian ini merekomendasikan penguatan tata kelola data, penerapan privacy by design, penggunaan biometrik multimodal, transparansi pengelolaan data, pembatasan penggunaan berbasis proporsionalitas, peningkatan literasi digital, dan harmonisasi regulasi internasional untuk menjaga keseimbangan antara inovasi teknologi dan hak privasi warga negara.

Kata Kunci: Biometrik; Perlindungan Data; Privasi Data; Regulasi; Sidik Jari.

1. LATAR BELAKANG

Daktiloskopi awalnya dikembangkan dan dimanfaatkan secara eksklusif dalam ranah penegakan hukum dan investigasi kriminal, daktiloskopi kini telah berevolusi menjadi teknologi biometrik yang merambah berbagai sektor kehidupan masyarakat modern. Perkembangan teknologi kecerdasan buatan dan pembelajaran mesin telah mendorong pemanfaatan sidik jari melampaui batas-batas forensik tradisional, memasuki domain administrasi kependudukan, layanan keuangan, sistem keamanan, hingga perangkat teknologi konsumen sehari-hari (Ghosh et al., 2025). Pergeseran paradigma ini menandai era baru

daktiloskopi yang tidak lagi semata-mata berorientasi pada penanganan kejahatan, melainkan sebagai instrumen efisiensi dalam tata kelola pemerintahan dan pelayanan masyarakat. Sistem *Automated Fingerprint Identification System* (AFIS) yang telah berkembang dengan integrasi *deep learning* kini mampu memproses jutaan identifikasi biometrik dalam hitungan detik, menandai lompatan kuantum dalam kapasitas pemrosesan data dibandingkan metode manual tradisional (Sreehari & Anzar, 2025).

Implementasi daktiloskopi non-kriminal di Indonesia mencapai momentum penting dengan diluncurkannya program *e-KTP* (Kartu Tanda Penduduk elektronik) pada tahun 2011 yang mengintegrasikan data biometrik sidik jari seluruh warga negara dalam satu sistem administrasi kependudukan nasional. Program ini berhasil mencatat lebih dari 270 juta warga negara dalam basis data biometrik terpusat, menjadikan Indonesia sebagai salah satu negara dengan implementasi sistem identitas biometrik terbesar di dunia (Ghosh et al., 2025). Sistem ini dirancang untuk meningkatkan efisiensi pelayanan publik, mencegah duplikasi identitas, dan memfasilitasi integrasi data kependudukan lintas sektor. Teknologi daktiloskopi telah diadopsi secara luas oleh berbagai institusi pemerintah dan swasta, mulai dari sistem *e-SIM* dengan registrasi biometrik yang dimandatkan sejak 2025, verifikasi *Know Your Customer* (KYC) pada sektor perbankan dan *fintech*, sistem absensi pegawai, kontrol akses keamanan, hingga autentikasi perangkat pribadi seperti *smartphone* (Kim, 2025 ; Consulting, 2020). Penetrasi yang masif ini mencerminkan kepercayaan institusional terhadap keandalan sidik jari sebagai penanda identitas yang bersifat unik, permanen, dan sulit dipalsukan, sekaligus menjanjikan efisiensi operasional dan pengurangan birokrasi yang selama ini menjadi hambatan dalam pelayanan publik di Indonesia.

Ekspansi penggunaan daktiloskopi ke ranah non-kriminal menimbulkan urgensi untuk mengkaji implikasi hukum, etika, dan sosial yang menyertainya. Berbeda dengan konteks kriminal yang memiliki landasan hukum jelas dalam kerangka sistem peradilan pidana, penggunaan daktiloskopi untuk tujuan administratif menghadirkan zona abu-abu dalam perlindungan data pribadi dan hak privasi warga negara. Pertanyaan mendasar muncul: sejauh mana negara dan korporasi dapat mengumpulkan, menyimpan, dan mengolah data biometrik yang bersifat sangat sensitif dan permanen? Bagaimana mekanisme pengawasan dan akuntabilitas dalam pengelolaan basis data sidik jari yang tersentralisasi? Apa konsekuensi dari kebocoran atau penyalahgunaan data biometrik yang tidak dapat diubah layaknya kata sandi? Minimnya regulasi yang komprehensif sebelum disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) telah menciptakan kekosongan hukum selama lebih dari satu dekade sejak peluncuran *e-KTP*, di mana data biometrik jutaan

warga negara diproses tanpa kerangka perlindungan yang memadai. Meskipun UU PDP telah berlaku sejak 17 Oktober 2022 dengan masa transisi yang berakhir Oktober 2024, implementasinya masih menghadapi berbagai tantangan termasuk belum terbentuknya otoritas pengawas data pribadi yang independen dan belum selesainya penyusunan peraturan pelaksana (Agus Ahadi Deradjat, 2025).

Penilaian paradigma kontemporer daktiloskopi non-kriminal di Indonesia dengan fokus pada dialektika antara kebutuhan efisiensi administrasi negara dan jaminan perlindungan privasi warga negara melalui pendekatan interdisipliner yang mengintegrasikan perspektif teknis, hukum, dan sosial. Penelitian ini berupaya menjawab bagaimana Indonesia dapat mengoptimalkan manfaat daktiloskopi untuk pelayanan publik tanpa mengorbankan hak fundamental warga negara atas privasi dan perlindungan data pribadi, serta merumuskan rekomendasi kebijakan yang mengakomodasi kedua kepentingan tersebut secara berimbang dalam konteks implementasi UU PDP yang masih dalam tahap transisi.

2. KAJIAN TEORITIS

Dalam penelitian ini empat kerangka teori sebagai landasan dibentuknya kajian demi menghasilkan kepastian, keadilan dan kebermanfaatan hukum. Landasan teori ini memberikan arahan demi memberikan sebuah pembaharuan yang dapat menjamin kesejahteraan masyarakat dalam hal keamanan dan ketentraman dalam mengikuti perkembangan teknologi hingga masa yang akan datang. Seluruh teori dasar ini tidak hanya digunakan sebagai pondasi dasar untuk tujuan mengetahui semata, akan tetapi teori ini memungkinkan analisis yang menjawab apa yang terjadi, dan juga mengapa dan untuk kepentingan siapa.

Privacy Informational Theory: Teori Privasi Informasional sebagai Dasar Analisa Kebijakan

Teori privasi informasional memandang privasi bukan sekadar hak untuk "dibiarkan sendiri" (*the right to be let alone*) sebagaimana konsepsi privasi klasik, melainkan sebagai hak individu untuk mengontrol arus informasi mengenai dirinya sendiri, termasuk menentukan kapan, bagaimana, dan sejauh mana informasi pribadinya dikomunikasikan kepada pihak lain. Dalam konteks data biometrik seperti sidik jari, teori ini menjadi relevan karena data biometrik memiliki karakteristik yang secara fundamental berbeda dari data pribadi konvensional: bersifat unik, melekat secara permanen pada tubuh individu, dan tidak dapat diubah atau dicabut kembali (*irrevocable*) apabila telah disalahgunakan atau bocor (Kokolakis, 2017). Teori ini juga memperkenalkan konsep *privacy paradox*, yaitu kesenjangan antara kekhawatiran yang dinyatakan individu terhadap privasi datanya dengan perilaku aktual

mereka yang tetap menyerahkan data biometrik demi kemudahan administratif atau layanan, sebuah fenomena yang tampak jelas dalam penerimaan luas masyarakat Indonesia terhadap program e-KTP meskipun disertai kekhawatiran laten terhadap penyalahgunaan data (Kokolakis, 2017).

Biometric Function Transformation Theory: Landasan Teori sebagai Alasan Rekonstruksi Fungsi Biometrik

Pergeseran paradigmatik penggunaan teknologi identifikasi biometrik dari fungsi awalnya yang eksklusif dalam ranah penegakan hukum dan investigasi kriminal (*criminal justice function*) menuju fungsi yang jauh lebih luas dalam ranah administrasi negara dan pelayanan publik (*civil administration function*). Dalam kerangka ini, biometrik berfungsi sebagai *tool of suspicion*, yakni teknologi yang secara inheren melekat pada konteks kecurigaan, penyelidikan, dan pembuktian tindak pidana, sehingga pengumpulannya secara historis dibatasi hanya kepada individu yang berstatus tersangka, terdakwa, atau narapidana (van der Ploeg, 2018).

Transformasi mendasar terjadi ketika negara-negara modern, termasuk Indonesia, mengadopsi teknologi biometrik untuk tujuan yang berbeda dari fungsi awalnya, yaitu sebagai instrumen identifikasi sipil untuk membangun basis data kependudukan yang akurat, mencegah duplikasi identitas, dan mengefisienkan pelayanan administrasi publik. (Lyon, 2018) menyebut pergeseran ini sebagai proses *de-criminalisation* fungsi biometrik, yaitu lepasnya teknologi identifikasi biometrik dari konteks kecurigaan pidana menuju konteks administrasi negara yang bersifat netral

Data Protection Theory: Teori Perlindungan Data Pribadi Dasar sebagai Dasar Kepastian Hukum

Teori perlindungan data pribadi, yang berkembang sebagai turunan operasional dari hak privasi di era digital dan menjadi basis normatif berbagai instrumen hukum internasional maupun nasional, termasuk UU PDP Indonesia. Teori ini menekankan sejumlah prinsip fundamental yang harus dipenuhi dalam setiap pemrosesan data pribadi, antara lain *lawfulness*, *fairness*, and *transparency* (keabsahan, keadilan, dan transparansi pemrosesan), *purpose limitation* (pembatasan tujuan penggunaan data sesuai maksud awal pengumpulan), *data minimization* (pengumpulan data seminimal mungkin sesuai kebutuhan), *accuracy* (akurasi data), *storage limitation* (pembatasan jangka waktu penyimpanan), serta *integrity and confidentiality* (keutuhan dan kerahasiaan data) (Christopher Kuner, 2020). Prinsip-prinsip ini menjadi tolak ukur untuk menilai sejauh mana implementasi daktiloskopi non-kriminal di Indonesia baik dalam program e-KTP, registrasi *e-SIM*, maupun KYC perbankan telah selaras

dengan standar perlindungan data yang diakui secara internasional. Selain itu, teori ini juga mengenal konsep data *subject rights* atau hak-hak pemilik data, mencakup hak untuk mengakses, mengoreksi, membatasi pemrosesan, hingga menghapus data pribadinya (*right to erasure*), yang dalam konteks data biometrik menghadirkan tantangan tersendiri mengingat sifatnya yang permanen dan sulit benar-benar "dihapus" dari sistem yang telah terintegrasi lintas sektor (Christopher Kuner, 2020).

3. METODE PENELITIAN

Dalam penelitian ini, pendekatan kualitatif deskriptif-analitis dengan pendekatan yuridis normatif dan interdisipliner, berbasis studi kepustakaan (*library research*) digunakan sebagai dasar penelitian agar relevansi kajian yang diteliti sesuai dengan yang diharapkan. Hal ini terlihat jelas karena penulis sama sekali tidak melakukan pengumpulan data primer seperti survei, wawancara, atau eksperimen sendiri, seluruh data dan temuan yang disajikan mulai dari angka akurasi sistem biometrik sebesar 87–92%, jumlah 270 juta warga negara dalam basis data e-KTP, hingga 73% responden yang mengkhawatirkan *surveillance* massal, merupakan kutipan dari sumber sekunder seperti jurnal ilmiah, laporan lembaga, dan situs resmi pemerintah (Ghosh et al., 2025). Penulis mengumpulkan, membandingkan, dan menyintesis lebih dari dua puluh sumber tersebut menjadi satu narasi analitis baru, yang merupakan ciri utama dari studi kepustakaan.

Analisis ini berfokus pada kesenjangan antara regulasi yang secara formal sudah berlaku (*law in the books*) dengan kenyataan penerapannya yang masih menghadapi kekosongan otoritas pengawas independen dan peraturan pelaksana yang belum lengkap (*law in action*), tanpa disertai data lapangan mengenai bagaimana masyarakat benar-benar mengalami penerapan hukum tersebut. Karakter interdisipliner penelitian ini juga ditegaskan secara eksplisit dalam abstrak, yang menyatakan bahwa kajian mengintegrasikan perspektif teknis, hukum, dan sosial sekaligus, sebagaimana tercermin dari percampuran pembahasan mengenai akurasi dan kerentanan teknis sistem AFIS, kerangka hukum perlindungan data, serta kekhawatiran dan literasi digital masyarakat dalam satu kesatuan analisis.

4. HASIL DAN PEMBAHASAN

Indonesia menjadi salah satu negara dengan implementasi sistem identitas biometrik terbesar di dunia melalui program e-KTP yang diluncurkan pada tahun 2011, berhasil mencatat lebih dari 270 juta warga negara dalam basis data biometrik terpusat (Ghosh et al., 2025). Direktorat Jenderal Administrasi Hukum Umum melakukan digitalisasi arsip daktiloskopi

melalui aplikasi *E-SMART* dengan target menginput 10.000 data dalam waktu 4 hari untuk meningkatkan efisiensi pelayanan dan memungkinkan penemuan kembali data sidik jari seseorang dengan cepat dan akurat (Ditjen AHU, 2024). Pemerintah juga menyusun perubahan Permenkumham Nomor 37 Tahun 2016 tentang Daktiloskopi dengan tujuan optimalisasi pemanfaatan sidik jari, penyediaan database sidik jari, pemberian layanan sidik jari, efisiensi waktu pelayanan, dan integrasi layanan sistem sidik jari antar kementerian/lembaga (AHU, 2023). Ekspansi daktiloskopi non-kriminal mencakup registrasi *e-SIM* dengan verifikasi biometrik yang dimandatkan sejak 2025 untuk penguatan keamanan nasional (FaceTec, 2025), verifikasi *Know Your Customer* (KYC) pada sektor perbankan dengan proyeksi 18% dari *banking digital onboarding global* menggunakan sistem AI pada tahun 2025 (iProov, 2025), serta sistem absensi, kontrol akses, dan *patient identification* di berbagai sektor (Fabrizio, 2025).

Implementasi daktiloskopi non-kriminal memberikan manfaat substantif dalam meningkatkan efisiensi administrasi publik dan pelayanan masyarakat. Pertama, sistem biometrik menawarkan tingkat keandalan superior karena karakteristik biometrik bersifat unik dan tidak dapat dengan mudah dipalsukan, dengan integrasi AI dan machine learning meningkatkan akurasi identifikasi serta mengurangi *false positive* dan *false negative* (Toscano, 2025). Kedua, efisiensi operasional dicapai melalui eliminasi kebutuhan password yang kompleks, pengurangan *security fatigue*, dan percepatan proses autentikasi, di mana 45% dari bank terbesar di Amerika Serikat mampu membuka rekening nasabah secara online dalam waktu kurang dari 30 menit melalui *biometric authentication* (iProov, 2025). Ketiga, daktiloskopi berkontribusi signifikan dalam pencegahan fraud dan duplikasi identitas, dengan sistem e-KTP Indonesia yang mengintegrasikan data biometrik 270 juta penduduk dirancang untuk mengeliminasi duplikasi yang menjadi celah dalam program bantuan sosial dan layanan pemerintah. Keempat, personalisasi dan pengalaman pengguna ditingkatkan melalui kemampuan sistem menggunakan data biometrik untuk mempersonalisasi pengaturan pengguna dan preferensi, menciptakan pengalaman yang disesuaikan untuk setiap individu (Jolly, 2025).

Hasil analisis menunjukkan bahwa daktiloskopi di Indonesia telah mengalami perluasan fungsi secara masif dari ranah forensik kriminal menuju berbagai sektor administrasi sipil. Tabel 1 merangkum sektor implementasi, manfaat utama, dan risiko privasi dominan yang teridentifikasi dari sintesis literatur.

Tabel 1. Matriks Sektor Implementasi, Manfaat, dan Risiko Privasi Daktiloskopi Non-Kriminal di Indonesia.

Sektor	Bentuk Implementasi	Manfaat Utama	Risiko Privasi Dominan
Administrasi Kependudukan	e-KTP (sejak 2011), digitalisasi arsip via E-SMART	Pencegahan duplikasi identitas; efisiensi pelayanan publik	Sentralisasi data 270 juta penduduk tanpa kerangka hukum memadai selama >1 dekade
Telekomunikasi	Registrasi e-SIM wajib biometrik (sejak 2025)	Penguatan keamanan nasional; pencegahan penyalahgunaan nomor	Perluasan tujuan penggunaan data (<i>function creep</i>) di luar konteks kependudukan
Perbankan & Fintech	Verifikasi KYC berbasis biometrik	Percepatan <i>onboarding</i> nasabah (<30 menit); pengurangan fraud	Ketergantungan pada akurasi sistem <i>single-modal</i> yang belum memenuhi standar kritis
Ketenagakerjaan/Institusi	Sistem absensi dan kontrol akses	Efisiensi operasional; pengurangan manipulasi kehadiran	Minimnya transparansi pengelolaan data di tingkat institusi non-negara

Namun, ekspansi daktiloskopi ke ranah non-kriminal menimbulkan risiko dan tantangan privasi yang serius. Risiko pertama dan paling fundamental adalah sifat *irreversible* dari data biometrik yang berbeda dengan password yang dapat diubah ketika terkompromisasi, di mana kebocoran database biometrik seperti kasus Suprema pada tahun 2019 yang mengekspos sidik jari lebih dari satu juta orang, serta kebocoran data fingerprint 5,6 juta pegawai federal Amerika Serikat pada tahun 2015, menimbulkan risiko jangka panjang terhadap *identity theft* dan *surveillance* (TeamPassword, 2025). Risiko kedua adalah kerentanan teknis sistem biometrik terhadap *spoofing* dan *deepfake technology*, dengan penelitian pada tahun 2025 mendemonstrasikan bahwa penyerang dengan akses administrator lokal dapat memanipulasi *biometric templates* sehingga sistem menerima sidik jari penyerang, sementara kasus 2019 menunjukkan *fingerprint* dapat diangkat dari gelas dan digunakan untuk membuka kunci smartphone dalam waktu kurang dari 20 menit (Center, 2021). Risiko ketiga adalah potensi *surveillance* massal dan pelanggaran kebebasan sipil, dengan *Federal Trade Commission* (FTC) memperingatkan bahwa penggunaan informasi biometrik yang meningkat menimbulkan kekhawatiran signifikan terhadap privasi konsumen, keamanan data, serta potensi bias dan diskriminasi, di mana survei menunjukkan 73% responden mengkhawatirkan pengawasan massal melalui basis data yang terhubung (Henderson, 2023).

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menandai *milestone* penting dalam kerangka hukum perlindungan data Indonesia dengan mengkategorikan data biometrik sebagai "data pribadi yang bersifat spesifik" yang memerlukan perlindungan lebih ketat (Agus Ahadi Deradjat, 2025). UU PDP mengadopsi prinsip-prinsip fundamental yang sejalan dengan standar internasional termasuk GDPR, meliputi prinsip *consent*, *data minimization*, dan *right to access and deletion* (Faiz Rahman,

2025, pp. 281-300) Namun, implementasi UU PDP menghadapi tantangan substantif di mana meskipun telah berlaku sejak 17 Oktober 2022 dengan masa transisi yang berakhir Oktober 2024, otoritas pengawas data pribadi yang independen belum terbentuk hingga awal tahun 2025, menciptakan vacuum dalam *enforcement* dan *monitoring* kepatuhan (Agus Ahadi Deradjat, 2025). Peraturan pelaksana yang diperlukan untuk operasionalisasi UU PDP juga belum selesai disusun secara komprehensif, menciptakan ketidakpastian hukum yang mempengaruhi bagaimana organisasi menginterpretasikan kewajiban mereka dalam pengelolaan data biometrik (Faiz Rahman, 2025).

Kesenjangan antara ketentuan formal UU PDP dan realitas implementasinya, sebagai elaborasi dari teori perlindungan data pribadi (Christopher Kuner, 2020).

Tabel 2. Kesenjangan Antara Regulasi Formal (*Law in the Books*) dan Implementasi (*Law in Action*) UU PDP terhadap Data Biometrik.

Aspek Regulasi	Ketentuan Formal (<i>De Jure</i>)	Kondisi Implementasi (<i>De Facto</i>)	Implikasi
Kelembagaan Pengawas	UU PDP mengamanatkan otoritas pengawas independen	Otoritas pengawas belum terbentuk hingga awal 2025	Kekosongan <i>enforcement</i> dan mekanisme audit kepatuhan
Peraturan Pelaksana	UU PDP berlaku efektif sejak 17 Oktober 2022, transisi berakhir Oktober 2024	Peraturan pelaksana belum tersusun komprehensif	Ketidakpastian hukum bagi pengelola data biometrik
Kategori Data Biometrik	Dikategorikan sebagai "data pribadi bersifat spesifik" dengan perlindungan lebih ketat	Belum ada standar teknis wajib (mis. enkripsi, <i>multimodal</i>) yang dijalankan seragam	Praktik pengamanan data bervariasi antarlembaga
Hak Subjek Data	UU PDP menjamin hak akses, koreksi, dan penghapusan data	Data biometrik bersifat permanen dan terintegrasi lintas sistem, sulit "dihapus" sepenuhnya	Hak <i>right to erasure</i> secara teknis sulit dipenuhi untuk data biometrik

Dalam implementasi *e-KTP* program yang telah berjalan sejak 2011 mengoperasikan sistem biometrik terpusat tanpa kerangka perlindungan hukum yang memadai selama lebih dari satu dekade, menciptakan risiko sistemik terhadap privasi 270 juta warga negara. Penelitian empiris menunjukkan bahwa sistem *single-modal traditional* yang digunakan dalam *e-KTP* hanya mencapai tingkat akurasi 87-92% dalam kondisi riil di Indonesia, jauh di bawah standar 99% yang diperlukan untuk aplikasi kritis, dengan faktor lingkungan tropis seperti kelembaban tinggi mempengaruhi kualitas pembacaan sidik jari (Ghosh et al., 2025). Temuan lapangan mengungkapkan berbagai persoalan praktis mulai dari kegagalan teknis pembacaan sidik jari pada kelompok usia lanjut, kekhawatiran masyarakat akan penyalahgunaan data, hingga kasus ribuan *e-KTP* yang tercecer di tempat umum tanpa mekanisme pengamanan memadai (Wimpie Tangkilisan, 2021, pp. 182-194). Ketiadaan transparansi dalam pengelolaan basis data nasional yang melibatkan data 270 juta penduduk, tanpa mekanisme yang jelas untuk audit publik atau

pengawasan independen, semakin memperparah kekhawatiran publik terhadap penyalahgunaan data biometrik.

Risiko keempat yang signifikan adalah ketidaktransparan dan kurangnya kontrol pengguna atas data biometrik mereka, di mana pengguna sering tidak memahami bagaimana data biometrik mereka dikumpulkan, disimpan, dan digunakan, menciptakan ketidakpastian yang mengurangi kepercayaan terhadap sistem biometrik. Kekhawatiran ini diperparah oleh temuan bahwa data biometrik telah muncul di dark web, dengan banyak sistem menyimpan templates tanpa enkripsi atau dengan kontrol yang lemah, mengekspos pengguna pada risiko identitas jangka panjang. Risiko kelima adalah ketidakkonsistenan regulasi dan perlindungan hukum, di mana berbagai negara dan industri mengikuti tingkat perlindungan privasi biometrik yang berbeda-beda, dengan ketiadaan regulasi seragam menciptakan inkonsistensi yang meninggalkan data biometrik rentan terhadap penyalahgunaan. Di Indonesia, meskipun UU PDP telah disahkan, tantangan implementasi termasuk belum terbentuknya otoritas pengawas independen dan belum selesainya peraturan pelaksana menunjukkan gap antara regulasi *de jure* dan perlindungan *de facto* terhadap data biometrik warga negara (Faiz Rahman, 2025).

Berdasarkan analisis terhadap manfaat, risiko, dan kerangka hukum daktiloskopi non-kriminal di Indonesia, beberapa rekomendasi kebijakan komprehensif diperlukan untuk menyeimbangkan kebutuhan efisiensi administrasi dengan perlindungan privasi warga negara. Pertama, percepatan pembentukan otoritas pengawas data pribadi yang independen dengan kewenangan investigasi dan enforcement yang kuat, kapasitas teknis untuk audit sistem biometrik berkala, independensi struktural dan fungsional, serta transparansi operasi dan pelaporan kepada publik (Faiz Rahman, 2025). Kedua, implementasi *privacy by design* dan *security by default* dalam setiap sistem daktiloskopi non-kriminal, termasuk minimalisasi pengumpulan data, *on-device processing*, *decentralized storage models*, enkripsi end-to-end, dan implementasi *secure hardware* seperti *Trusted Platform Module* (TPM). Ketiga, adopsi *multimodal biometrics* dan *liveness detection* untuk mengatasi kelemahan sistem *single-modal* e-KTP, dengan penelitian menunjukkan bahwa *fusi face* dan *finger match scores* dapat mengurangi transaksi "*undetermined*" unimodal hingga 98% (Ghosh et al., 2025).

Rekomendasi keempat adalah memastikan transparansi dan akuntabilitas dalam pengelolaan data melalui publikasi regular audit reports, mekanisme clear untuk data *subject access requests*, *notification requirements* dalam waktu 72 jam jika terjadi *data breach*, dan *establishment of data protection impact assessments* (DPIA) yang wajib sebelum implementasi sistem biometrik baru (Agus Ahadi Deradjat, 2025). Kelima, pembatasan penggunaan dan *purpose limitation* yang ketat di mana data biometrik yang dikumpulkan untuk tujuan

administrasi kependudukan tidak boleh digunakan untuk *surveillance* atau *profiling* tanpa basis hukum yang jelas, dengan penggunaan *facial recognition* untuk *mass surveillance* diatur secara ketat dengan *parliamentary oversight* dan *judicial review* mengingat risiko terhadap *civil liberties* (Henderson, 2023). Keenam, program komprehensif untuk meningkatkan literasi digital masyarakat tentang teknologi biometrik, mencakup edukasi tentang data biometrik dan sensitivitasnya, informasi tentang hak-hak individu di bawah UU PDP, panduan praktis perlindungan data biometrik, dan mekanisme pelaporan dugaan pelanggaran privasi. Ketujuh, harmonisasi regulasi Indonesia dengan standar internasional termasuk *alignment* dengan GDPR, partisipasi aktif dalam *standards-making bodies international*, bilateral dan multilateral *agreements* untuk *cross-border cooperation*, serta *adoption of best practices* dari *jurisdictions leading* seperti Uni Eropa, California (CCPA), dan Illinois (BIPA) (Faiz Rahman, 2025).

5. KESIMPULAN DAN SARAN

Paradigma daktiloskopi kontemporer di Indonesia menunjukkan transformasi fundamental dari penggunaan eksklusif forensik kriminal menuju aplikasi non-kriminal yang masif dalam berbagai sektor kehidupan masyarakat. Implementasi e-KTP yang mengintegrasikan data biometrik 270 juta warga negara, ekspansi ke registrasi *e-SIM*, verifikasi KYC perbankan, dan sistem autentikasi di berbagai institusi mencerminkan kepercayaan terhadap teknologi biometrik sebagai solusi efisiensi administrasi publik. Teknologi ini menawarkan manfaat substantif dalam keamanan, efisiensi operasional, pencegahan fraud, dan personalisasi layanan. Namun, penelitian ini mengidentifikasi dialektika krusial antara manfaat efisiensi dan risiko privasi yang inheren, termasuk sifat *irreversible* data biometrik, kerentanan terhadap *spoofing* dan *deepfake*, potensi *surveillance* massal, ketidaktransparan pengelolaan data, dan keterbatasan teknis sistem single-modal yang hanya mencapai akurasi 87-92% dalam kondisi riil Indonesia.

Kerangka hukum perlindungan data pribadi Indonesia telah mengalami kemajuan signifikan dengan disahkannya UU PDP yang mengkategorikan data biometrik sebagai data pribadi spesifik dengan perlindungan lebih ketat. Namun, implementasi menghadapi tantangan substantif berupa ketiadaan otoritas pengawas independen, ketidaklengkapan peraturan pelaksana, dan gap antara regulasi *de jure* dengan perlindungan *de facto*. Optimalisasi paradigma kontemporer memerlukan pendekatan holistik melalui tujuh rekomendasi kebijakan komprehensif: percepatan pembentukan otoritas pengawas independen, implementasi *privacy by design* dan *security by default*, adopsi *multimodal biometrics* dan *liveness detection*, transparansi dan akuntabilitas pengelolaan data, pembatasan penggunaan dengan *purpose*

limitation yang ketat, program literasi digital masyarakat, dan harmonisasi regulasi dengan standar internasional. Implementasi rekomendasi ini akan memungkinkan Indonesia mengoptimalkan manfaat daktiloskopi untuk pelayanan publik tanpa mengorbankan hak fundamental warga negara atas privasi dan perlindungan data pribadi

DAFTAR REFERENSI

- Agus Ahadi Deradajat, M. T. (2025, Maret 11). *Data Privacy Imperatives in Business: How Indonesia's PDP Law Has Evolved to Accommodate the AI, Healthcare and Financial Services Sectors*. Retrieved from Chambers and Partners: <https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2025/indonesia/trends-and-developments>
- AHU, H. D. (2023, Maret 21). *Ditjen AHU Gandeng BSK Bahas Rancangan Perubahan Permenkumham No. 37 Tahun 2016 Tentang Daktiloskopi*. Retrieved from AHU Pengayoman: <https://portal.ahu.go.id/id/detail/75-berita-lainnya/3455-ditjen-ahu-gandeng-bsk-bahas-rancangan-perubahan-permenkumham-no-37-tahun-2016-tentang-daktiloskopi>
- AHU, H. D. (2024, Juni 13). *Digitalisasi Daktiloskopi: Misi Baru Direktorat Pidana dalam Pelayanan Masyarakat*. Retrieved from digitalisasi daktiloskopi misi baru direktorat pidana dalam pelayanan masyarakat: <https://portal.ahu.go.id/id/detail/75-berita-lainnya/4362-digitalisasi-daktiloskopi-misi-baru-direktorat-pidana-dalam-pelayanan-masyarakat>
- Buchanan, K. (2022, October 17). *Indonesia: Personal Data Protection Act Enters into Force*. Retrieved from Library of Congress: <https://www.loc.gov/item/global-legal-monitor/2022-12-18/indonesia-personal-data-protection-act-enters-into-force>
- Center, B. P. (2021, September 20). *Prevalence of Biometric Data and Security Concerns*. Retrieved from prevalence of biometric data and security concerns: <https://bipartisanpolicy.org/article/prevalence-of-biometric-data-and-security-concerns/>
- Christopher Kuner, L. A. (2020). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford: Oxford University Press.
- Consulting, M. (2020). *Existing KYC practices in Indonesia and opportunities for implementing e-KYC to accelerate financial inclusion*. Senayan: Microsave Consulting.
- Fabrizio, V. (2025, January 23). *What's on the Horizon: 10 Biometric Trends for 2025*. Retrieved from What Horizon 10 Biometric Trends: <https://blog.hidglobal.com/whats-horizon-10-biometric-trends-2025>
- FaceTec. (2025, April 14). *Indonesia Mandates Biometric e-SIM Registration in National Security Push*. Retrieved from ID TECH: <https://idtechwire.com/indonesia-mandates-biometric-e-sim-registration-in-national-security-push/>
- Faiz Rahman, 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*, 281-300. Retrieved from tandfonline.
- Ghosh, P., Jana, S., Ghosh, S., & Dhar, R. (2025). *Hyperparameter Optimization in Deep Learning Techniques for Multimodal Biometric Verification*. 6(9), 967–981.
- Henderson, J. G. (2023, May 18). *FTC Warns About Misuses of Biometric Information and Harm to Consumers*. Retrieved from ftc warns about misuses biometric information

- harm consumers: <https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-warns-about-misuses-biometric-information-harm-consumers>
- Hunter Dorwart, K. D. (2022, Oktober 19). *Indonesia's Personal Data Protection Bill: Overview, Key Takeaways, and Context*. Retrieved from Future of Privacy Forum: <https://fpf.org/blog/indonesias-personal-data-protection-bill-overview-key-takeaways-and-context/>
- iProov. (2025, January 1). *The Numbers Don't Lie: 70+ Biometric Statistics*. Retrieved from Biometrics Statistic: <https://www.iproov.com/blog/biometric-statistics-70>
- Jolly, G. (2025, Maret 26). *Future use of biometrics: AI, fraud prevention, and industry expansion*. Retrieved from identity verification news the future of biometric technology: <https://www.veriff.com/identity-verification/news/the-future-of-biometric-technology>
- Kim, J.-s. (2025, April 14). *Indonesia Mandates Biometric e-SIM Registration in National Security Push*. Retrieved from ID TECH: <https://idtechwire.com/indonesia-mandates-biometric-e-sim-registration-in-national-security-push/>
- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computer & Security*, 122-134.
- Lyon, D. (2018). *The Culture of Surveillance: Watching as a Way of Life*. Kingston: Polity.
- Martins, Y. (2025, June 2). *Biometrics in 2025: trends and technological innovations*. Retrieved from Biometric Technology: <https://www.biopassid.com/post/biometric-technology-trends>
- Rahman, F., Leiden, U., & Mada, U. G. (2025). *Uum journal of legal studies*. 16(1), 1–18.
- Sreehari, S., & Anzar, S. M. (2025). Touchless fingerprint recognition: A survey of recent developments and challenges. *Computers and Electrical Engineering*, 122, 109894. <https://doi.org/https://doi.org/10.1016/j.compeleceng.2024.109894>
- TeamPassword. (2025, Oktober 8). *The Dark Side of Convenience: 7 Disadvantages of Biometric Security You Can't Ignore*. Retrieved from disadvantages of biometrics: <https://teampassword.com/blog/disadvantages-of-biometrics>
- Teteng. (2023, Desember 15). *Biometrik; Inovasi Sistem Keamanan Digital dan Perkembangannya*. Retrieved from CSIRT UNAIR: <https://csirt.unair.ac.id/biometrik-inovasi-sistem-keamanan-digital-dan-perkembangannya/>
- Toscano, J. (2025, April 18). *7 Key Advantages of Biometrics for Enterprises in 2025*. Retrieved from 7 ways enterprises are taking advantage biometrics: <https://www.pingidentity.com/en/resources/blog/post/7-ways-enterprises-are-taking-advantage-biometrics.html>
- Ughade, N. (2025, February 26). *Future Of Biometrics: Trends, Innovations, And Challenges Ahead*. Retrieved from Future of Biometrics: <https://hyperverge.co/blog/future-of-biometrics/>
- Wimpie TANGKILISAN, B. R. (2021). Inconsistency of Misusing Electronic Identity Card (E-KTP) Data in General Elections in Indonesia. *Universidad DEL ZULIA*, 182-194.
- Wimpie TANGKILISAN, B. R. (2021, February 10). Inconsistency of misusing electronic identity card (E-KTP) data in general elections in Indonesia. *Utopía y Praxis Latinoamericana*, 182-194. Retrieved from Utopía y Praxis Latinoamericana.
- Woolf, M. (2025, Desember 10). *29+ Biometrics Statistics for 2026*. Retrieved from Biometrics statistic: <https://photoaid.com/blog/biometrics-statistics/>