

TINJAUAN YURIDIS PENGUMPULAN DATA BIOMETRIK BERBASIS ARTIFICIAL INTELLIGENCE TANPA PERSETUJUAN DI INDONESIA

Legal Review of Artificial Intelligence-Based Biometric Data Collection Without Consent in Indonesia

Astri Maisarah Fadhilah¹, Aisyah Amini², Yuliani Darmawan³, Padil Ramdani⁴, Sri Septiani Dewi⁵

Universitas Nusa Putra, Sukabumi¹²³⁴⁵

astri.maisarah_hk23@nusaputra.ac.id, aisyah.amini_hk23@nusaputra.ac.id, yuliani.darmawan_hk23@nusaputra.ac.id,
padil.ramdani_hk23@nusaputra.ac.id, sri.septiani_hk23@nusaputra.ac.id

ABSTRACT

This study examines the collection of biometric data based on Artificial Intelligence (AI) without the consent of data subjects within the framework of Indonesia's data protection law. The research background arises from the increasing practice of biometric scanning by public and private entities without clear legal authorization, as seen in the Tools for Humanity (Worldcoin) and illegal online lending application cases. The objective is to analyze the conformity of such practices with the legal principles under Law Number 27 of 2022 on Personal Data Protection (PDP Law) and their implications for individuals' privacy rights. The study employs a normative juridical method with a descriptive-analytical approach through the analysis of legal regulations, academic literature, and real case studies. The findings indicate that collecting biometric data without explicit consent violates the principles of lawfulness, fairness, and transparency, and may result in administrative, civil, and criminal liability. Furthermore, the lack of digital infrastructure readiness and independent oversight mechanisms poses significant challenges to PDP Law enforcement. This study recommends establishing an independent supervisory body, enforcing accountability and transparency principles in AI usage, and enhancing public digital literacy to ensure biometric data protection in the age of artificial intelligence.

Keywords: *artificial intelligence; biometric data; personal data protection; law; privacy*

ABSTRAK

Penelitian ini mengkaji pengumpulan data biometrik berbasis *Artificial Intelligence (AI)* tanpa persetujuan subjek data dalam perspektif hukum perlindungan data pribadi di Indonesia. Latar belakang penelitian berangkat dari maraknya praktik pemindaian biometrik oleh entitas publik dan swasta tanpa dasar hukum yang jelas, seperti kasus *Tools for Humanity (Worldcoin)* dan aplikasi pinjaman online ilegal. Tujuan penelitian ini adalah menganalisis kesesuaian praktik tersebut dengan prinsip-prinsip hukum dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) serta implikasinya terhadap hak privasi masyarakat. Metode yang digunakan adalah pendekatan yuridis normatif dengan sifat deskriptif-analitis melalui analisis peraturan perundang-undangan, literatur hukum, dan studi kasus aktual. Hasil penelitian menunjukkan bahwa pengumpulan data biometrik tanpa persetujuan merupakan pelanggaran terhadap prinsip *lawfulness*, *fairness*, dan *transparency*, serta berpotensi menimbulkan tanggung jawab administratif, perdata, dan pidana. Selain itu, kurangnya kesiapan infrastruktur digital dan mekanisme pengawasan independen menjadi tantangan besar dalam penegakan UU PDP. Penelitian ini menyarankan pembentukan lembaga pengawas independen, penerapan prinsip akuntabilitas dan transparansi dalam penggunaan AI, serta peningkatan literasi digital masyarakat untuk menjamin perlindungan data biometrik di era kecerdasan buatan.

Kata Kunci: *kecerdasan buatan; data biometrik; perlindungan data pribadi; hukum; privasi*

PENDAHULUAN

1. Latar Belakang Masalah

Perkembangan pesat teknologi Kecerdasan Buatan (*Artificial Intelligence/AI*) telah membawa perubahan fundamental dalam cara pengumpulan dan pemrosesan data, termasuk data biometrik seperti wajah, sidik jari, atau iris mata. Data biometrik merupakan data pribadi spesifik yang sangat sensitif dan melekat erat pada identitas individu, sehingga memerlukan perlindungan yang ketat.¹

Di Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) telah menjadi payung hukum utama yang menegaskan bahwa pengolahan data pribadi, terutama data sensitif, wajib didasarkan pada persetujuan eksplisit dari subjek data, serta memenuhi prinsip transparansi, legalitas, dan akuntabilitas. Prinsip ini sejalan dengan standar global seperti *General Data Protection Regulation (GDPR)*.²

Namun, dalam praktiknya, banyak entitas publik maupun swasta yang memanfaatkan sistem AI untuk mengumpulkan data biometrik tanpa mekanisme transparansi yang memadai dan tanpa persetujuan yang sah. Kasus-kasus seperti pengumpulan data iris mata oleh Tools for Humanity (Worldcoin) tanpa terdaftar sebagai Penyelenggara Sistem Elektronik (PSE) yang sah, serta praktik pinjaman online (pinjol) ilegal yang menyedot data biometrik tanpa izin, menunjukkan adanya potensi pelanggaran hak privasi dan hak asasi manusia yang serius di era digital.³

Kondisi ini menciptakan tantangan yuridis dan regulatory gap. Karakteristik AI yang bekerja secara otonom, kompleks, dan seringkali bersifat black box mempersulit penentuan pihak yang bertanggung jawab secara hukum (*liability principle*) ketika terjadi pelanggaran. Oleh karena itu, penelitian ini menjadi sangat penting untuk mengkaji secara mendalam bagaimana pertanggungjawaban hukum dapat ditegakkan terhadap pelaku pengumpulan data biometrik berbasis AI tanpa persetujuan, serta bagaimana prinsip akuntabilitas dan transparansi UU PDP harus diimplementasikan secara efektif untuk mencegah pelanggaran di masa depan.⁴

2. Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, timbul pertanyaan-pertanyaan krusial, diantaranya; Bagaimanakah pengaturan dan implikasi hukum dari tindakan pengumpulan data biometrik berbasis Artificial Intelligence tanpa persetujuan subjek data berdasarkan Undang-Undang Perlindungan Data Pribadi? dan jalur pertanggungjawaban hukum apa saja yang dapat diterapkan terhadap pelaku? mengingat tantangan yuridis yang ditimbulkan oleh sifat otonom sistem AI.

3. Tujuan dan Manfaat Penelitian

a. Tujuan Penelitian

1. Menganalisis dan menjelaskan secara komprehensif pengaturan hukum pengumpulan data biometrik berbasis AI tanpa persetujuan berdasarkan UU PDP.
2. Mengidentifikasi dan mengkaji jalur pertanggungjawaban hukum yang dapat dikenakan kepada pengendali data yang melakukan pengumpulan data biometrik tanpa persetujuan.
3. Merumuskan urgensi dan rekomendasi penguatan prinsip akuntabilitas dan transparansi, serta pembaharuan regulasi untuk mengisi regulatory gap yang timbul akibat perkembangan teknologi AI.

b. Manfaat Penelitian

1. Secara Teoritis: Menambah khazanah ilmu hukum, khususnya di bidang hukum siber dan perlindungan data pribadi, dengan memberikan analisis mendalam mengenai isu pertanggungjawaban hukum dalam konteks penggunaan AI dan data biometrik.
2. Secara Praktis: Memberikan masukan yuridis bagi pemerintah, khususnya Kementerian Komunikasi dan Informatika (Kominfo) dan lembaga pengawas data pribadi, dalam merumuskan kebijakan, memperkuat penegakan hukum, dan mempercepat harmonisasi regulasi di era AI. Selain itu, menjadi pedoman bagi pengendali data dalam memastikan kepatuhan terhadap UU PDP.

¹ Laina Rafianti Patriciana Edina Sembiring, Ahmad M. Ramli, "Implementasi Desain Privasi Sebagai Pelindungan Privasi Atas Data Biometrik," *Veritas et Justitia*, June 29, 2024, <https://doi.org/10.25123/vej.v10i1.7622>.

² S.H., LL.M. in IT Law Dr. Danrivanto Budhijanto, *Hukum Pelindungan Data Pribadi Di Indonesia: Cyberlaw & Cybersecurity* (Pt Refika Aditama, 2023), https://refika.co.id/626-hukum-perindungan-data-pribadi-di-indonesia-cyberlaw-cybersecurity.html?utm_source=chatgpt.com.

³ Ainunnisa Rezky Asokawati, "Perlindungan Data Biometrik Dalam Sektor Perbankan Di Indonesia Dan Amerika Serikat," *Legal Standing : Jurnal Ilmu Hukum* 8, no. 3a (2024): 895–907, <https://doi.org/10.24269/ls.v8i3a.10775>.

⁴ Dwi Nugroho Masudianto and Megawati Barthos, "Optimization of Personal Data Rights Protection in Artificial Intelligence Era Under Indonesia's Cybersecurity Law," *Interdisciplinary Journal and Humanity (INJURITY)* 4, no. 7 (2025): 452–62, <https://doi.org/10.58631/injury.v4i7.1451>.

4. Rangkuman Kajian Teoritik

Kajian ini berlandaskan pada teori dan doktrin utama hukum perlindungan data pribadi dan hukum pertanggungjawaban. Data biometrik dikategorikan sebagai data spesifik yang memerlukan perlindungan ekstra. Prinsip fundamental yang dikaji adalah persetujuan eksplisit (*explicit consent*), yang merupakan dasar legitimasi utama pengolahan data sensitif (Pasal 16 UU PDP), serta prinsip akuntabilitas dan transparansi.⁵

Terkait pertanggungjawaban, penelitian ini menyoroti bahwa pengumpulan data tanpa dasar yang sah merupakan perbuatan melawan hukum (*onrechtmatige daad*) (Pasal 1365 KUHPerdata). Tantangan yuridisnya adalah sifat otonom AI, di mana tanggung jawab tidak dapat dilekatkan pada AI sebagai subjek hukum, melainkan dialihkan kepada pengembang, pengelola, atau badan hukum yang menggunakan AI, melalui prinsip *vicarious liability* atau *strict liability*.⁶ Pelanggaran terhadap UU PDP dapat memicu sanksi administratif (Pasal 57-60), perdata (ganti rugi), dan pidana (Pasal 65), yang menuntut adanya lembaga pengawas independen untuk mengatasi masalah black box dan menjamin akuntabilitas sistem AI.⁷

METODE PENELITIAN

Penelitian ini menggunakan pendekatan yuridis normatif karena fokusnya adalah menelaah norma dan doktrin hukum yang relevan serta menggambarkan dan menganalisis praktik pengumpulan data biometrik berbasis Kecerdasan Buatan (AI) tanpa persetujuan, khususnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Penelitian hukum normatif dipengaruhi oleh doktrin hukum murni. Tahapan dalam penelitian hukum normatif diawali dengan pengumpulan data sekunder melalui studi pustaka, kemudian dilakukan analisis dengan menggunakan logika berfikir secara deduktif dengan menekankan kepada norma, yurisprudensi dan doktrin.⁸

⁵ Patriciana Edina Sembiring, Ahmad M. Ramli, "Implementasi Desain Privasi Sebagai Pelindungan Privasi Atas Data Biometrik."

⁶ Eka Nanda Ravizki and Lintang Yudhantaka, "Artificial Intelligence Sebagai Subjek Hukum: Tinjauan Konseptual Dan Tantangan Pengaturan Di Indonesia," *Notaire* 5, no. 3 (2022): 351–76, <https://doi.org/10.20473/ntr.v5i3.39063>.

⁷ Loso Judijanto et al., "Kajian Hukum Dampak Kecerdasan Buatan Terhadap Perlindungan Privasi Data Dalam Hukum Siber Indonesia," *Sanskara Hukum Dan HAM* 3, no. 02 (2024): 68–76, <https://doi.org/10.58812/shh.v3i02.498>.

Teknik pengumpulan data dilakukan melalui studi dokumentasi atau penelitian pustaka (*library research*) terhadap bahan hukum (UU PDP, UU ITE, peraturan pelaksana, putusan) dan literatur akademik (jurnal, artikel, makalah), termasuk mengumpulkan dan menganalisis undang-undang serta jurnal dari Google Scholar. Keunggulan utama pendekatan normatif adalah kemampuannya menciptakan kerangka hukum yang jelas dan terstruktur.⁹ Data diolah dengan metode analisis kualitatif normatif.

Analisis yuridis normatif dimulai dengan analisis bahan hukum primer, bahan hukum sekunder dan tersier secara normatif berdasarkan pendekatan konseptual dan peraturan perundang-undangan atau pendekatan lain yang sesuai dengan rumusan masalah.¹⁰ Pendekatan analisis yang digunakan adalah pendekatan perundang-undangan (*statute approach*) untuk mengevaluasi norma hukum, pendekatan konseptual (*conceptual approach*) untuk menguji konsep hukum, dan pendekatan perbandingan (*comparative approach*) untuk membandingkan regulasi Indonesia dengan standar internasional seperti GDPR. Metode ini diharapkan dapat mengungkap ketidaksesuaian regulasi, menilai kecukupan UU PDP terhadap tantangan AI, serta memberikan saran konseptual untuk memperkuat pengamanan data biometrik di Indonesia.

PEMBAHASAN DAN ANALISIS

Pengumpulan data biometrik melalui teknologi Artificial Intelligence (AI) tanpa persetujuan subjek data bertentangan dengan prinsip dasar perlindungan privasi yang diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Pasal 16 UU PDP menegaskan bahwa pengolahan data pribadi hanya dapat dilakukan berdasarkan persetujuan eksplisit dari pemilik data.

⁸ Wiwik Sri Widiarty, "Buku Ajar Metode Penelitian Hukum," *RISTANSI: Riset Akuntansi* 17 (2019): 2, <http://repository.uki.ac.id/14688/1/BukuAjarMetodePenelitianHukum.pdf>.

⁹ Sidi Ahyar Wiraguna, "Metode Normatif Dan Empiris Dalam Penelitian Hukum: Studi Eksploratif Di Indonesia," *Public Sphere: Jurnal Sosial Politik, Pemerintahan Dan Hukum* 3, no. 3 (2024), <https://doi.org/10.59818/jps.v3i3.1390>.

¹⁰ Kimmy Baby Kirana and Wilma Silalahi, "Tantangan Regulasi Kecerdasan Buatan (AI) Dalam Perspektif Hukum Perlindungan Data Pribadi Di Indonesia," *Cerdika: Jurnal Ilmiah Indonesia* 5, no. 6 (2025): 1807–17, <https://doi.org/10.59141/cerdika.v5i6.2711>.

Hal ini sejalan dengan prinsip *lawfulness, fairness, and transparency* sebagaimana juga tercantum dalam *General Data Protection Regulation (GDPR)*.¹¹

Data biometrik dikategorikan sebagai data sensitif karena secara langsung berkaitan dengan identitas individu, sehingga memerlukan pengamanan yang lebih ketat dibandingkan data pribadi biasa.¹² Namun dalam praktiknya, banyak entitas publik maupun swasta yang memanfaatkan teknologi AI untuk mengumpulkan data biometrik seperti wajah, sidik jari, atau pola suara tanpa mekanisme transparansi yang memadai. Kondisi ini menimbulkan potensi pelanggaran hak privasi karena subjek data tidak mengetahui sejauh mana datanya diproses dan untuk tujuan apa.

Pengumpulan data pribadi oleh sistem AI tanpa dasar pemrosesan yang sah pun merupakan pelanggaran hukum dan menimbulkan tanggung jawab bagi pengendali data.¹³ AI yang bekerja secara otonom sering kali tidak memberikan pemberitahuan (*notice*) atau kesempatan bagi individu untuk menyetujui penggunaan datanya. Oleh karena itu, dari perspektif UU PDP, tindakan tersebut termasuk dalam kategori pemrosesan data yang melawan hukum, sehingga pelaku dapat dikenai sanksi administratif maupun pidana sesuai ketentuan dalam Pasal 57–60 dan Pasal 65 UU PDP.

Pertanggungjawaban hukum terhadap pelaku pengumpulan data biometrik menggunakan AI tanpa persetujuan dapat dijalankan melalui tiga jalur hukum utama, yaitu administratif, perdata, dan pidana. Secara administratif, Pasal 57 sampai dengan Pasal 60 UU PDP memberikan kewenangan kepada otoritas perlindungan data untuk menjatuhkan sanksi berupa teguran tertulis, penghentian sementara pengolahan data, penghapusan data, hingga denda administratif hingga Rp5 miliar. Ketentuan ini berfungsi sebagai bentuk akuntabilitas hukum preventif, agar pengendali data mematuhi prinsip kehati-hatian sebelum memproses data biometrik berbasis AI.¹⁴

Dalam ranah perdata, tindakan pengumpulan data biometrik tanpa izin termasuk perbuatan melawan hukum (*onrechtmatige daad*) sebagaimana diatur dalam Pasal 1365 KUHPerdata. Subjek data berhak menuntut ganti rugi atas kerugian yang timbul akibat pemrosesan data tanpa dasar hukum yang sah. Karakteristik AI yang otonom dan kompleks menciptakan kesulitan dalam menentukan siapa pihak yang bertanggung jawab secara hukum, karena AI tidak memiliki status subjek hukum.¹⁵ Oleh karena itu, tanggung jawab dialihkan kepada pengembang, pengelola data, atau badan hukum yang menggunakan AI tersebut, berdasarkan prinsip *vicarious liability* atau *strict liability*.

Di sisi lain, dari aspek pidana, Pasal 65 UU PDP menegaskan ancaman hukuman penjara hingga 5 tahun dan/atau denda hingga Rp5 miliar bagi pihak yang secara sengaja memperoleh atau memproses data pribadi orang lain secara melawan hukum. Namun, sebagaimana dijelaskan oleh Judijanto dkk.¹⁶ tantangan utama dalam konteks AI adalah kesulitan pembuktian dan keterbatasan akses ke sistem algoritmik (*black box*), sehingga diperlukan badan pengawas independen untuk melakukan audit teknis dan menjamin akuntabilitas sistem AI.

Dalam konteks pengumpulan data biometrik berbasis *Artificial Intelligence (AI)*, prinsip akuntabilitas dan transparansi merupakan elemen fundamental yang harus ditegakkan oleh setiap pengendali data pribadi. Prinsip ini tidak hanya tercantum dalam Pasal 3 ayat (2) huruf f dan g UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), tetapi juga menjadi standar etika internasional sebagaimana termuat dalam *General Data Protection Regulation (GDPR)* Pasal 5 ayat (2) yang menekankan *accountability principle*.¹⁷

Pengendali data wajib memastikan bahwa setiap tahapan pengolahan data biometrik dapat dipertanggungjawabkan secara hukum, teknis, dan etis.

¹¹ Dewan Perwakilan Rakyat, “Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi,” Republik Indonesia § (2022), <https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022>.

¹² Patriciana Edina Sembiring, Ahmad M. Ramli, “Implementasi Desain Privasi Sebagai Pelindungan Privasi Atas Data Biometrik.”

¹³ Akmal Muhammad Abdullah, “Pelindungan Hak Privasi Terhadap Pengumpulan Data Pribadi Oleh AI Generatif Berdasarkan Percakapan Dengan Pengguna,” *Padjadjaran Law Review* 12, no. 2 (2024): 145–56, <https://doi.org/10.56895/plr.v12i2.1796>.

¹⁴ Silawati Dayang G, Sandra Olivia Putri L, and Ananda Kyara Putri K, “Urgensi Pembentukan Lembaga Pengawas Dalam Pembaharuan Hukum Perlindungan Data Pribadi

Menurut Undang-Undang PDP,” *Locus* 4, no. 2 (2025): 106–13.

¹⁵ Ravizki and Lintang Yudhantaka, “Artificial Intelligence Sebagai Subjek Hukum: Tinjauan Konseptual Dan Tantangan Pengaturan Di Indonesia.”

¹⁶ Judijanto et al., “Kajian Hukum Dampak Kecerdasan Buatan Terhadap Perlindungan Privasi Data Dalam Hukum Siber Indonesia.”

¹⁷ European Parliament and the Council of the European Union, “General Data Protection Regulation — GDPR” (2016), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>.

Artinya, setiap pengumpulan, penyimpanan, dan pemanfaatan data biometrik harus terdokumentasi secara jelas, termasuk mekanisme persetujuan yang diberikan oleh subjek data.¹⁸ Dalam konteks AI, penerapan prinsip transparansi menghadapi tantangan serius karena sebagian besar sistem AI bersifat *black box*, yang berarti mekanisme internal algoritmanya sulit diakses atau dipahami oleh publik maupun otoritas pengawas.

Selain itu, penggunaan AI untuk analisis wajah atau pengenalan pola perilaku (*behavioral analytics*) berisiko tinggi terhadap penyalahgunaan data apabila tidak dilengkapi dengan sistem audit algoritmik yang ketat. Oleh karena itu, pengendali data wajib melakukan *data protection impact assessment (DPIA)* sebelum menggunakan sistem AI yang memproses data biometrik. Langkah ini penting untuk menilai potensi risiko terhadap hak privasi dan menentukan langkah mitigasi yang sesuai agar tidak terjadi pelanggaran hukum maupun etika.¹⁹

Penerapan prinsip akuntabilitas dan transparansi juga menuntut adanya pengawasan eksternal yang independen. Lembaga pengawas data pribadi yang diamanatkan UU PDP harus memiliki kewenangan memadai untuk melakukan audit terhadap sistem AI yang digunakan oleh lembaga publik dan swasta. Dengan demikian, pengawasan preventif ini tidak hanya mencegah terjadinya pelanggaran, tetapi juga memperkuat kepercayaan masyarakat terhadap penggunaan AI di bidang pengolahan data pribadi. Perkembangan pesat teknologi AI menuntut pembaruan hukum agar dapat mengakomodasi karakteristik AI yang kompleks, otonom, dan adaptif. UU PDP sejauh ini telah menjadi payung hukum utama dalam melindungi data pribadi, namun belum sepenuhnya mengatur mekanisme spesifik terkait tanggung jawab hukum atas tindakan AI yang bersifat otomatis. Kondisi ini menyebabkan adanya *regulatory gap* antara kemajuan teknologi dan kemampuan hukum dalam memberikan perlindungan efektif terhadap hak privasi.²⁰

Menurut Lase, Indonesia perlu membentuk lembaga pengawas perlindungan data pribadi yang bersifat independen dan memiliki kompetensi teknis di bidang kecerdasan buatan. Lembaga ini tidak hanya bertugas menegakkan UU PDP, tetapi juga berperan

dalam menetapkan standar teknis keamanan data, melakukan sertifikasi sistem AI, serta melakukan audit terhadap sistem pengenalan biometrik yang berpotensi melanggar hak privasi.²¹

Selain itu, diperlukan pembaruan regulasi yang mengatur:

1. Kewajiban transparansi algoritma, agar pengendali data wajib membuka informasi dasar tentang cara kerja sistem AI yang memproses data biometrik.
2. Klasifikasi tingkat risiko teknologi AI, di mana sistem dengan risiko tinggi seperti pengenalan wajah atau verifikasi biometrik harus melewati uji etika dan pengawasan ketat sebelum digunakan.
3. Penegasan prinsip tanggung jawab hukum (*liability principle*) bagi pengembang atau entitas yang memanfaatkan AI untuk pemrosesan data sensitif, dengan skema pertanggungjawaban kolektif (*collective responsibility*).

Pendekatan ini sejalan dengan arah kebijakan hukum Uni Eropa melalui *EU Artificial Intelligence Act 2024*, yang membagi kategori risiko AI dan menetapkan kewajiban kepatuhan berbeda berdasarkan potensi dampaknya terhadap hak asasi manusia. Dengan mengadopsi prinsip serupa, Indonesia dapat memastikan keseimbangan antara inovasi teknologi dan perlindungan hak privasi warga negara.²²

Pengumpulan data biometrik oleh sistem *Artificial Intelligence (AI)* tidak hanya menimbulkan persoalan hukum, tetapi juga memunculkan dilema etika dan hak asasi manusia (HAM). Menurut Pasal 28G ayat (1) UUD 1945, setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda. Dalam konteks digital, perlindungan diri pribadi ini meliputi juga hak atas privasi data pribadi, termasuk data biometrik.²³

Namun, praktik di lapangan menunjukkan bahwa pengumpulan data biometrik sering dilakukan tanpa mekanisme persetujuan yang eksplisit, dengan dalih efisiensi layanan publik atau keamanan nasional. Misalnya, penggunaan teknologi face recognition di

¹⁸ Patriciana Edina Sembiring, Ahmad M. Ramli, "Implementasi Desain Privasi Sebagai Pelindungan Privasi Atas Data Biometrik."

¹⁹ Kirana and Silalahi, "Tantangan Regulasi Kecerdasan Buatan (AI) Dalam Perspektif Hukum Perlindungan Data Pribadi Di Indonesia."

²⁰ Judijanto et al., "Kajian Hukum Dampak Kecerdasan Buatan Terhadap Perlindungan Privasi Data Dalam Hukum Siber Indonesia."

²¹ G, L, and K, "Urgensi Pembentukan Lembaga Pengawas Dalam Pembaharuan Hukum Perlindungan Data Pribadi Menurut Undang-Undang PDP."

²² European Commission, "Regulatory Framework Proposal on Artificial Intelligence (Artificial Intelligence Act)" (2024), <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>.

²³ Republik Indonesia., "Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (Amandemen Keempat)" (1945), <https://peraturan.bpk.go.id/Home/Details/53201/naskah-uud-1945>.

ruang publik sering kali tidak disertai dengan

pemberitahuan yang jelas kepada masyarakat mengenai tujuan, masa simpan, dan pengendali datanya. Hal ini menimbulkan potensi pelanggaran terhadap prinsip *proportionality* dan *necessity*, di mana setiap pembatasan terhadap hak privasi harus memiliki dasar hukum yang sah dan tidak berlebihan. Dari perspektif etika profesi hukum dan teknologi, prinsip “*privacy by design and by default*” sebagaimana dianut oleh GDPR harus diterapkan dalam setiap tahap pengembangan dan penerapan sistem AI. Artinya, perlindungan privasi bukan hanya diterapkan di akhir proses, tetapi diintegrasikan sejak tahap perancangan algoritma. Pendekatan ini mendorong pengembang dan pengendali data untuk bertanggung jawab terhadap nilai kemanusiaan yang melekat dalam setiap proses pengolahan data.²⁴

Lebih jauh, pengumpulan data biometrik tanpa persetujuan dapat mengancam hak atas kebebasan berekspresi dan berkumpul secara damai, terutama ketika digunakan untuk pengawasan massal (*mass surveillance*). Oleh karena itu, diperlukan keseimbangan antara kepentingan keamanan dan hak privasi individu agar teknologi AI tidak berubah menjadi instrumen pelanggaran HAM.

Meskipun UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah disahkan sebagai tonggak penting perlindungan privasi, implementasinya masih menghadapi sejumlah tantangan serius. Salah satu kendala utama adalah minimnya kesiapan infrastruktur digital dan kesadaran hukum baik di kalangan penyelenggara sistem elektronik maupun masyarakat umum.²⁵

Sebagian besar instansi pemerintah dan korporasi masih belum memiliki *data governance policy* yang komprehensif. Banyak pengelola data belum memahami konsep dasar pengendali dan prosesor data sebagaimana diatur dalam Pasal 1 angka (4) dan (5) UU PDP. Akibatnya, mekanisme pengawasan internal dan prosedur keamanan data sering kali lemah, sehingga memungkinkan kebocoran atau penyalahgunaan data biometrik tanpa disadari.

Selain itu, keterbatasan sumber daya manusia yang memiliki keahlian di bidang *cyber law*, *AI ethics*, dan *data protection* juga menjadi hambatan besar. Diperlukan kolaborasi antara pemerintah, akademisi, dan sektor swasta untuk membangun kapasitas nasional melalui pelatihan, sertifikasi, dan pembentukan lembaga riset interdisipliner. Dalam konteks penegakan

overlapping regulasi antara UU PDP, UU ITE, dan peraturan sektoral lain seperti UU Administrasi Kependudukan dan UU Telekomunikasi. Oleh karena itu, harmonisasi peraturan menjadi kunci untuk memastikan penerapan prinsip perlindungan data biometrik yang konsisten di seluruh sektor.

Terakhir, untuk mendorong efektivitas hukum, diperlukan strategi literasi publik digital agar masyarakat memahami hak-haknya sebagai subjek data. Tanpa kesadaran hukum masyarakat, perlindungan data pribadi akan sulit diterapkan secara substantif, meskipun telah memiliki dasar hukum yang kuat.

Pada tahun 2021, perusahaan asing bernama Tools for Humanity (TFH) mulai beroperasi di Indonesia melalui proyek bernama Worldcoin, yang bertujuan menciptakan sistem identitas digital global (*World ID*) berbasis data biometrik iris mata. TFH menggunakan perangkat khusus berbentuk bola logam bernama Orb untuk memindai iris mata masyarakat. Kegiatan ini dilakukan di berbagai tempat umum, termasuk kampus dan pusat perbelanjaan, dengan iming-iming hadiah dalam bentuk aset kripto agar masyarakat bersedia memberikan data iris mereka. Data tersebut kemudian diproses dan diklaim telah diubah menjadi bentuk terenkripsi (*iris code*) untuk dijadikan dasar identitas digital.²⁶

Namun, seiring meningkatnya kegiatan tersebut, pemerintah Indonesia melalui Kementerian Komunikasi dan Informatika (Kominfo) menerima laporan dari masyarakat dan mulai melakukan penelusuran. Ditemukan bahwa TFH belum memiliki Tanda Daftar sebagai Penyelenggara Sistem Elektronik (PSE), padahal mereka telah mengumpulkan dan memproses data pribadi sensitif, yaitu data biometrik iris mata warga negara Indonesia. Selain itu, TFH juga dinilai tidak memberikan pemberitahuan atau persetujuan eksplisit kepada para subjek data sesuai ketentuan dalam Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP).²⁷

Sebagai respons atas temuan tersebut, pada Juli 2024, Kominfo melalui Direktorat Jenderal Aplikasi Informatika dan Komisi Komunikasi dan Digital (Komdigi) memutuskan untuk menanggukkan Tanda Daftar PSE TFH, serta memerintahkan penghentian semua kegiatan pemindaian dan pemrosesan data iris di Indonesia. TFH juga diwajibkan untuk menghapus

²⁴ Patriciana Edina Sembiring, Ahmad M. Ramli, “Implementasi Desain Privasi Sebagai Pelindungan Privasi Atas Data Biometrik.”

²⁵ Dewan Perwakilan Rakyat, Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

hukum, Indonesia masih menghadapi persoalan

²⁶ Worldcoin menawarkan insentif berupa aset kripto kepada peserta yang bersedia memindai iris mereka. Lihat: CNBC Indonesia, “Ramai Pemindaian Bola Mata di RI, Ini Fakta Proyek Worldcoin,” diakses 13 Oktober 2025, <https://www.cnbcindonesia.com/>

²⁷ Kementerian Komunikasi dan Informatika Republik Indonesia, *Kominfo Lakukan Penelusuran Aktivitas Worldcoin di Indonesia*, 2 Agustus 2023, diakses 13 Oktober 2025, <https://www.kominfo.go.id/>

seluruh data biometrik yang telah dikumpulkan, termasuk data yang telah dienkripsi. Kasus ini menjadi perhatian publik karena menunjukkan adanya praktik pengumpulan data biometrik tanpa dasar hukum yang sah, serta menjadi peringatan bagi perusahaan teknologi yang menggunakan kecerdasan buatan (AI) dalam pemrosesan data sensitif agar tetap tunduk pada prinsip transparansi, akuntabilitas, dan persetujuan yang sah sesuai UU PDP.²⁸

Masalah utama dalam kasus ini terletak pada fakta bahwa Tools for Humanity (TFH), sebagai penyelenggara sistem elektronik, tidak terdaftar secara resmi sebagai Penyelenggara Sistem Elektronik (PSE) di Indonesia saat mulai mengoperasikan teknologi pemindaian iris mata. Padahal, sesuai peraturan yang berlaku, setiap entitas yang mengumpulkan, mengelola, dan memproses data pribadi masyarakat Indonesia, terutama data pribadi spesifik seperti data biometrik, wajib terdaftar sebagai PSE lingkup privat. Tanpa status PSE, TFH dianggap tidak memiliki dasar hukum yang sah untuk menjalankan kegiatan pemrosesan data di wilayah yurisdiksi Indonesia. Ketidakterdaftarannya ini menimbulkan persoalan serius terkait legalitas operasional TFH, transparansi dalam pengumpulan data, serta perlindungan hak subjek data sebagaimana diatur dalam Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Hal ini memperkuat dugaan bahwa aktivitas TFH tidak hanya melanggar ketentuan administratif, tetapi juga berpotensi melanggar prinsip dasar perlindungan data pribadi, terutama karena dilakukan tanpa pemberitahuan dan persetujuan eksplisit dari pengguna.²⁹

Menanggapi aktivitas ilegal yang dilakukan oleh Tools for Humanity (TFH), Komisi Komunikasi dan Digital (Komdigi) di bawah Kementerian Komunikasi dan Informatika (Kominfo) segera mengambil tindakan tegas. Setelah dilakukan klarifikasi dan pemeriksaan mendalam, Komdigi menyimpulkan bahwa TFH telah melakukan pengumpulan data biometrik iris mata warga Indonesia sejak tahun 2021 tanpa dasar hukum yang sah, karena belum terdaftar sebagai Penyelenggara Sistem Elektronik (PSE) pada saat itu. Menindaklanjuti temuan tersebut, Komdigi secara resmi menanggukuhkan Tanda Daftar PSE TFH, yang telah didaftarkan pada Februari 2025, dan memerintahkan

penghentian seluruh kegiatan pemindaian dan pemrosesan data biometrik yang telah dilakukan. Selain itu, TFH juga diwajibkan untuk menghapus seluruh data iris mata warga Indonesia, termasuk data yang telah dikodekan atau dienkripsi dalam bentuk iris code. Komdigi menegaskan bahwa penghapusan data ini bersifat mutlak sebagai bentuk perlindungan hak subjek data pribadi dan sebagai upaya mendorong penegakan prinsip transparansi, legalitas, dan persetujuan eksplisit sebagaimana diatur dalam Undang-Undang Perlindungan Data Pribadi. Langkah ini juga menjadi sinyal kuat bahwa pemerintah tidak akan mentolerir praktik pengumpulan data sensitif yang tidak mematuhi peraturan nasional.³⁰ Kasus pengumpulan data biometrik iris mata oleh Tools for Humanity (TFH) sangat relevan dengan ketentuan dalam Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Data iris mata termasuk dalam kategori data pribadi spesifik yang memiliki sensitivitas tinggi, sehingga pengolahannya harus memenuhi persyaratan yang ketat, seperti memperoleh persetujuan eksplisit dari subjek data. Dalam kasus ini, TFH diduga melakukan pemrosesan data tanpa persetujuan yang jelas dan tanpa memenuhi prinsip transparansi, keamanan, serta keadilan yang diatur dalam UU PDP. Selain itu, TFH tidak terdaftar sebagai Penyelenggara Sistem Elektronik (PSE) sebagaimana diwajibkan, sehingga tidak memenuhi kewajiban administratif dan perlindungan yang diamanatkan oleh UU PDP. Oleh karena itu, kasus ini menjadi contoh nyata pentingnya penerapan UU PDP dalam menjaga hak-hak individu terkait data pribadi, terutama data biometrik yang sangat sensitif dan rentan disalahgunakan.³¹

Pemerintah Indonesia menegaskan bahwa pelanggaran dalam pengumpulan dan pengolahan data biometrik tanpa persetujuan dan tanpa izin resmi sebagai Penyelenggara Sistem Elektronik (PSE) dapat dikenakan berbagai sanksi sesuai dengan Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Sanksi administratif yang dapat diberikan meliputi peringatan tertulis, denda hingga Rp7 miliar, pembatasan atau penghentian sementara aktivitas pemrosesan data, serta pencabutan izin PSE. Selain itu, jika pelanggaran tersebut menyebabkan kerugian bagi subjek data atau kebocoran data pribadi, pelaku juga dapat dikenai sanksi pidana berupa pidana

²⁸ Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Pasal 20–22, mengatur kewajiban transparansi, akuntabilitas, serta persetujuan eksplisit dalam pemrosesan data pribadi sensitif, termasuk data biometrik.

²⁹ Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Pasal 1 angka 2 dan Pasal 20, menetapkan bahwa pemrosesan data pribadi wajib dilandasi oleh dasar hukum yang sah.

³⁰ Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Pasal 20, 21, dan 58, menyatakan bahwa pemrosesan data pribadi sensitif harus berdasarkan persetujuan eksplisit dan prinsip transparansi serta akuntabilitas.

³¹ Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP).

penjara hingga 6 tahun dan denda maksimal Rp10 miliar. Sanksi ini diperberat khususnya apabila melibatkan data pribadi yang sangat sensitif, seperti data biometrik iris mata, yang memiliki risiko tinggi terhadap penyalahgunaan. Sebagai contoh, dalam kasus Tools for Humanity (TFH), pemerintah telah menanggguhkan izin operasional dan memerintahkan penghapusan data yang dikumpulkan secara ilegal, serta membuka kemungkinan tindakan hukum lebih lanjut sesuai dengan ketentuan UU PDP.³²

Perkembangan teknologi kecerdasan buatan (Artificial Intelligence) telah mendorong penggunaan teknologi biometrik, khususnya pengenalan wajah, sebagai metode verifikasi identitas dalam berbagai layanan keuangan digital, termasuk aplikasi pinjaman online. Meskipun teknologi ini menawarkan kemudahan dan kecepatan verifikasi, penerapannya sering kali dilakukan tanpa transparansi yang memadai dan tanpa memperoleh persetujuan eksplisit dari pengguna. Beberapa aplikasi pinjaman online diketahui mengumpulkan dan menyimpan data biometrik wajah pengguna tanpa menyampaikan informasi secara jelas atau meminta izin yang sah. Praktik ini berpotensi melanggar Undang-Undang Perlindungan Data Pribadi (UU No. 27 Tahun 2022), yang mengatur bahwa pengolahan data biometrik sebagai data sensitif harus dilakukan dengan persetujuan yang sah dan dilandasi prinsip transparansi serta perlindungan keamanan data. Ketidakpatuhan ini menimbulkan risiko besar terhadap pelanggaran privasi dan potensi penyalahgunaan data oleh pihak tidak bertanggung jawab.³³

Kasus kebocoran data pribadi pada aplikasi pinjaman online ilegal dimulai dengan maraknya penyebaran aplikasi pinjol yang tidak terdaftar resmi di Indonesia pada tahun 2023. Aplikasi-aplikasi ini mengundang pengguna dengan proses pengajuan pinjaman yang cepat dan tanpa jaminan, sehingga banyak masyarakat tertarik untuk menggunakan layanan tersebut. Namun, dalam prosesnya, aplikasi ini mengumpulkan data pribadi pengguna secara berlebihan, termasuk data biometrik dan informasi perangkat, tanpa memberikan penjelasan yang transparan atau meminta persetujuan yang sah. Seiring,

waktu, terungkap adanya celah keamanan pada server aplikasi yang memungkinkan data-data tersebut bocor dan tersebar luas di internet. Kebocoran ini kemudian dimanfaatkan oleh pihak-pihak tidak bertanggung jawab untuk melakukan penipuan, pengajuan pinjaman ilegal, dan tindakan merugikan lainnya terhadap para korban.³⁴

Pemerintah Indonesia, melalui Kementerian Komunikasi dan Informatika (Kominfo) dan Satgas Penanganan Aplikasi Pinjaman Online Ilegal (PAKI), mengambil tindakan tegas dalam menanggapi kasus kebocoran data pada aplikasi pinjaman online ilegal. Langkah pertama yang diambil adalah melakukan investigasi terhadap aplikasi-aplikasi yang diduga melakukan pelanggaran keamanan data dan pengumpulan data tanpa persetujuan yang sah. Pemerintah kemudian memblokir akses aplikasi-aplikasi ilegal tersebut agar tidak dapat diunduh atau digunakan oleh masyarakat luas. Selain itu, Kominfo memberikan sanksi administratif kepada pengelola aplikasi, termasuk denda dan pencabutan izin operasional. Pemerintah juga meningkatkan sosialisasi kepada masyarakat mengenai bahaya penggunaan aplikasi pinjol ilegal dan pentingnya menjaga keamanan data pribadi. Melalui langkah-langkah ini, pemerintah berupaya menegakkan Undang-Undang Perlindungan Data Pribadi serta melindungi masyarakat dari potensi penyalahgunaan data yang merugikan.³⁵

KESIMPULAN

Dari hasil penelitian ini, dapat disimpulkan bahwa pengumpulan data biometrik berbasis Artificial Intelligence (AI) tanpa persetujuan subjek data memiliki hubungan erat dengan pelanggaran prinsip-prinsip hukum perlindungan data pribadi sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Variabel pengumpulan data biometrik tanpa persetujuan terbukti memengaruhi tingkat pelanggaran hak privasi individu dan menimbulkan pertanggungjawaban hukum baik secara administratif, perdata, maupun pidana.

³⁴ SAFEnet, *Laporan Investigasi Perlindungan Data oleh Aplikasi Pinjaman Online Ilegal di Indonesia*, 2023, diakses 13 Oktober 2025, <https://safenet.or.id/>

³⁵ Kementerian Komunikasi dan Informatika Republik Indonesia, *Penguatan Penanganan Aplikasi Pinjaman Online Ilegal oleh Satgas PAKI*, 2024, <https://www.kominfo.go.id/>

³² Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), Pasal 57 ayat (1).

³³ Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Pasal 3 huruf c dan Pasal 20–22.

Selain itu, masih lemahnya prinsip akuntabilitas dan transparansi dalam penerapan AI menunjukkan adanya ketimpangan antara perkembangan teknologi dan kesiapan hukum nasional, sehingga menimbulkan tantangan dalam penegakan prinsip akuntabilitas, pengawasan independen, serta pemenuhan hak asasi manusia di bidang privasi digital. Kondisi ini menjelaskan bahwa, keterkaitan antara regulasi, praktik teknologi, dan etika menjadi kunci utama untuk mewujudkan sistem hukum yang adaptif, adil, dan berorientasi pada perlindungan hak individu dalam era kecerdasan buatan.

SARAN

Untuk mewujudkan perlindungan hukum yang efektif, diperlukan langkah konkret dalam memperkuat regulasi dan implementasi UU PDP, terutama dengan membentuk lembaga pengawas independen yang memiliki kompetensi di bidang kecerdasan buatan dan keamanan data. Pemerintah dan sektor swasta perlu meningkatkan transparansi dalam penggunaan algoritma, menerapkan prinsip *privacy by design and by default*, serta melakukan *data protection impact assessment* sebelum menggunakan teknologi AI yang memproses data biometrik. Disamping itu, harmonisasi regulasi antar peraturan perundang-undangan dan peningkatan literasi digital masyarakat menjadi langkah penting agar kesadaran hukum terhadap hak privasi semakin tinggi. Kolaborasi lintas sector antara akademisi, pengembang teknologi, dan pembuat kebijakan juga penting untuk memastikan keseimbangan antara inovasi AI dan perlindungan hak asasi manusia di Indonesia.

DAFTAR KEPUSTAKAAN

- Abdullah, Akmal Muhammad. "Pelindungan Hak Privasi Terhadap Pengumpulan Data Pribadi Oleh AI Generatif Berdasarkan Percakapan Dengan Pengguna." *Padjadjaran Law Review* 12, no. 2 (2024): 145–56. <https://doi.org/10.56895/plr.v12i2.1796>.
- Asokawati, Ainunnisa Rezky. "Perlindungan Data Biometrik Dalam Sektor Perbankan Di Indonesia Dan Amerika Serikat." *Legal Standing : Jurnal Ilmu Hukum* 8, no. 3a (2024): 895–907. <https://doi.org/10.24269/lis.v8i3a.10775>.
- Dewan Perwakilan Rakyat. Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Republik Indonesia § (2022). <https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022>.
- Dr. Danrivanto Budhijanto, S.H., LL.M. in IT Law.

Hukum Pelindungan Data Pribadi Di Indonesia: Cyberlaw & Cybersecurity. Pt Refika Aditama, 2023. https://refika.co.id/626-hukum-perlindungan-data-pribadi-di-indonesia-cyberlaw-cybersecurity.html?utm_source=chatgpt.com.

- European Commission. Regulatory Framework Proposal on Artificial Intelligence (Artificial Intelligence Act) (2024). <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>.
- European Parliament and the Council of the European Union. General Data Protection Regulation — GDPR (2016). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>.
- G, Silawati Dayang, Sandra Olivia Putri L, and Ananda Kyara Putri K. "Urgensi Pembentukan Lembaga Pengawas Dalam Pembaharuan Hukum Perlindungan Data Pribadi Menurut Undang-Undang PDP." *Locus* 4, no. 2 (2025): 106–13.
- Judijanto, Loso, T. Saiful Basri, Rabith Madah Khulaili Harsya, Arnes Yuli Vandika, and Andrew Shandy Utama. "Kajian Hukum Dampak Kecerdasan Buatan Terhadap Perlindungan Privasi Data Dalam Hukum Siber Indonesia." *Sanskara Hukum Dan HAM* 3, no. 02 (2024): 68–76. <https://doi.org/10.58812/shh.v3i02.498>.
- Kirana, Kimmy Baby, and Wilma Silalahi. "Tantangan Regulasi Kecerdasan Buatan (AI) Dalam Perspektif Hukum Perlindungan Data Pribadi Di Indonesia." *Cerdika: Jurnal Ilmiah Indonesia* 5, no. 6 (2025): 1807–17. <https://doi.org/10.59141/cerdika.v5i6.2711>.
- Masudianto, Dwi Nugroho, and Megawati Barthos. "Optimization of Personal Data Rights Protection in Artificial Intelligence Era Under Indonesia's Cybersecurity Law." *Interdisciplinary Journal and Humanity (INJURITY)* 4, no. 7 (2025): 452–62. <https://doi.org/10.58631/injury.v4i7.1451>.
- Patriciana Edina Sembiring, Ahmad M. Ramli, Laina Rafianti. "Implementasi Desain Privasi Sebagai Pelindungan Privasi Atas Data Biometrik." *Veritas et Justitia*, June 29, 2024. <https://doi.org/10.25123/vej.v10i1.7622>.
- Ravizki, Eka Nanda, and Lintang Yudhantaka. "Artificial Intelligence Sebagai Subjek Hukum: Tinjauan Konseptual Dan Tantangan Pengaturan Di Indonesia." *Notaire* 5, no. 3 (2022): 351–76. <https://doi.org/10.20473/ntr.v5i3.39063>.
- Republik Indonesia. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (Amandemen Keempat) (1945). <https://peraturan.bpk.go.id/Home/Details/53201/>

naskah-uud-1945.

Widiarty, Wiwik Sri. “Buku Ajar Metode Penelitian Hukum.” *RISTANSI: Riset Akuntansi* 17 (2019): 2. <http://repository.uki.ac.id/14688/1/BukuAjarMetodePenelitianHukum.pdf>.

Wiraguna, Sidi Ahyar. “Metode Normatif Dan Empiris Dalam Penelitian Hukum: Studi Eksploratif Di Indonesia.” *Public Sphere: Jurnal Sosial Politik, Pemerintahan Dan Hukum* 3, no. 3 (2024). <https://doi.org/10.59818/jps.v3i3.1390>.