

**PENGAWASAN MASSAL BERBASIS AI (*FACIAL RECOGNITION*) OLEH  
NEGARA DAN IMPUNITAS TERHADAP HAK ATAS PRIVASI DIGITAL: KAJIAN  
YURIDIS, SOSIOLOGIS, DAN FILOSOFIS**

**Binsar Gultom<sup>1</sup>, Yudhi Hertanto<sup>2</sup>**

Universitas Islam Sultan Agung<sup>1,2</sup>

e-mail: [yudhihertanto@gmail.com](mailto:yudhihertanto@gmail.com)

Diterima: 12/08/2026; Direvisi: 18/08/2026; Diterbitkan: 21/08/2026

**ABSTRAK**

Perkembangan *Facial Recognition Technology* (FRT) dalam layanan publik dan penegakan hukum menghadirkan manfaat bagi efisiensi identifikasi, tetapi sekaligus menimbulkan persoalan perlindungan data biometrik, privasi, dan kebebasan sipil. Persoalan menjadi semakin kompleks ketika pemrosesan dilakukan secara luas, otomatis, dan tanpa batas kewenangan serta pengawasan yang memadai. Penelitian ini bertujuan menganalisis batas kewenangan negara dalam penggunaan FRT berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), serta mengkaji implikasi sosial dan filosofisnya terhadap kebebasan, otonomi, dan martabat manusia. Penelitian menggunakan penelitian hukum normatif sebagai desain utama dengan pendekatan socio-legal berbasis studi kepustakaan dan pendekatan filsafat hukum. Bahan hukum dianalisis menggunakan *Siracusa Principles* dan *proportionality test*, sedangkan implikasi sosial dikaji melalui konsep *Chilling Effect* dan *Digital Panopticon*. Hasil penelitian menunjukkan bahwa data biometrik merupakan Data Pribadi yang bersifat spesifik, sementara penggunaan FRT yang luas dan tidak terarah memerlukan dasar hukum, tujuan, kebutuhan, proporsionalitas, serta *safeguards* yang lebih kuat. Penggunaan *indiscriminate* tanpa pengawasan memadai berpotensi membatasi privasi dan kebebasan sipil. Penelitian merekomendasikan penguatan pengawasan independen, audit algoritma, transparansi, pembatasan retensi, dan mekanisme pemulihan.

**Kata kunci:** *Facial Recognition Technology, data biometrik, UU PDP, proportionality test, Chilling Effect*

**ABSTRACT**

The development of Facial Recognition Technology (FRT) in public services and law enforcement offers benefits for identification efficiency, while simultaneously raising concerns regarding biometric data protection, privacy, and civil liberties. These concerns become more complex when processing is conducted extensively and automatically without clear limits on governmental authority or adequate oversight. This study aims to analyze the limits of state authority in using FRT under Law Number 27 of 2022 on Personal Data Protection (PDP Law), as well as its social and philosophical implications for freedom, autonomy, and human dignity. The study employs normative legal research as its primary design, complemented by a socio-legal approach based on literature and documentary analysis and a legal philosophy approach. Legal materials are analyzed using the Siracusa Principles and the proportionality test, while social implications are examined through the concepts of the Chilling Effect and Digital Panopticon. The findings show that biometric data constitutes specific Personal Data, while extensive and indiscriminate FRT use requires stronger legal grounds, legitimate purposes, necessity, proportionality, and safeguards. Indiscriminate use without adequate oversight potentially restricts privacy and civil liberties. The study recommends strengthening

independent oversight, algorithmic audits, transparency, retention limits, and effective remedies.

**Keywords:** *Facial Recognition Technology, biometric data, PDP Law, proportionality test, Chilling Effect*

## PENDAHULUAN

Perkembangan kecerdasan artifisial (*Artificial Intelligence/AI*) dalam tata kelola pemerintahan Indonesia menunjukkan pergeseran dari digitalisasi administrasi menuju pemanfaatan teknologi untuk verifikasi identitas, keamanan, dan pelayanan publik, sebagaimana terlihat dari kerja sama Indonesia–Republik Korea pada 2026 yang mencakup pengembangan AI dalam pemerintahan dan layanan publik digital. Perkembangan tersebut sejalan dengan Pratiwi et al. (2025) yang menunjukkan bahwa AI dalam sektor publik Indonesia berkembang sebagai bagian dari transformasi *e-government* dan *digital governance*, meskipun masih menghadapi tantangan kesiapan kelembagaan, tata kelola data, dan kapasitas implementasi. Basron et al. (2026) juga menegaskan bahwa AI berpotensi meningkatkan efektivitas dan kualitas pelayanan publik, tetapi memerlukan penguatan regulasi, tata kelola, dan etika. Dalam konteks yang lebih spesifik, *Facial Recognition Technology* (FRT) berkembang melalui kebijakan registrasi pelanggan jasa telekomunikasi berbasis biometrik yang diberlakukan secara nasional sejak 1 Juli 2026 melalui pencocokan wajah dengan data kependudukan Direktorat Jenderal Kependudukan dan Pencatatan Sipil. Perkembangan tersebut menunjukkan manfaat FRT bagi validitas identitas, efisiensi layanan, dan keamanan digital, tetapi sekaligus menimbulkan persoalan hukum ketika identifikasi biometrik dilakukan otomatis, berskala besar, dan berpotensi berlangsung tanpa persetujuan atau pengawasan yang memadai.

FRT perlu dibedakan dari kamera pengawas (*closed-circuit television/CCTV*) dan sistem penegakan hukum lalu lintas seperti *Electronic Traffic Law Enforcement* (ETLE), karena keberadaan kamera tidak selalu berarti adanya proses pengenalan wajah. FRT merupakan teknologi biometrik yang mendeteksi karakteristik wajah, menghasilkan representasi digital (*faceprint* atau *template*), kemudian membandingkannya dengan data wajah untuk melakukan verifikasi atau identifikasi. Perkembangan *deep learning* meningkatkan kemampuan pengenalan wajah dalam menghadapi variasi pencahayaan, ekspresi, dan oklusi, meskipun kondisi tersebut tetap dapat memengaruhi akurasi sistem (Fauziah & Kusuma, 2025), sementara Syahputra et al. (2026) menunjukkan adanya kerentanan sistem berbasis *deep learning* terhadap serangan *adversarial*. Secara hukum, persoalan utama FRT bukan semata kecanggihan algoritma, melainkan sifat data biometrik yang melekat pada individu, kemampuan identifikasi otomatis, skala pemrosesan, kemungkinan penyimpanan jangka panjang, serta risiko pemrosesan tanpa sepengetahuan subjek data. Dengan demikian, penggunaan FRT perlu dibedakan berdasarkan tujuan, karena verifikasi identitas tidak secara otomatis merupakan *mass surveillance*, sedangkan identifikasi biometrik massal di ruang publik memiliki karakter pengawasan yang jauh lebih invasif.

Identifikasi biometrik massal menjadi relevan ketika sistem secara berkelanjutan mencocokkan wajah individu terhadap basis data berskala luas, sehingga berpotensi memengaruhi privasi, kebebasan sipil, dan prinsip negara hukum. Dalam konteks Indonesia, Zahro (2025) menunjukkan bahwa penggunaan *face recognition* menimbulkan risiko privasi karena data wajah dapat diproses untuk identifikasi, sementara persoalan persetujuan, transparansi, dan potensi penyalahgunaan masih menjadi perhatian. Kurniawan dan Kurniawan (2025) juga mengidentifikasi normalisasi *mass surveillance* sebagai risiko sistemik *AI-based*

*facial recognition*, terutama ketika identifikasi dan pelacakan individu dilakukan secara luas tanpa mekanisme akuntabilitas yang memadai. Persoalan tersebut memperoleh relevansi yuridis setelah berlakunya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), yang melalui Pasal 4 ayat (1) dan ayat (2) huruf b mengategorikan data biometrik sebagai Data Pribadi yang bersifat spesifik, termasuk karakteristik fisik seperti gambar wajah. Sembiring et al. (2024) menegaskan bahwa data biometrik memiliki karakteristik unik dan tidak dapat dipertukarkan sehingga memerlukan pelindungan khusus, sedangkan Fadhilla dan Putra (2024) menunjukkan bahwa penggunaan FRT memiliki konsekuensi hukum khusus berdasarkan UU PDP dan memerlukan mekanisme pencegahan penyimpangan serta keamanan data.

Meskipun demikian, UU PDP melalui Pasal 15 memberikan sejumlah pengecualian terhadap hak subjek data, antara lain untuk pertahanan dan keamanan nasional, penegakan hukum, serta kepentingan umum dalam penyelenggaraan negara, sehingga diperlukan batas kewenangan agar pengecualian tersebut tidak berkembang menjadi diskresi yang terlalu luas. Penelitian terdahulu umumnya mengkaji FRT secara terpisah melalui perspektif keamanan dan akurasi teknologi, perlindungan data dan privasi, etika dan hak asasi manusia, maupun dampak sosial pengawasan digital. Pramudito (2025) menunjukkan bahwa penerapan FRT di Indonesia menimbulkan persoalan privasi, keamanan data, bias algoritmik, dan potensi penyalahgunaan untuk kepentingan pengawasan, sedangkan Putri (2025) menekankan pentingnya tata kelola biometrik, transparansi, persetujuan, pemenuhan hak subjek data, dan mekanisme penghapusan data. Namun, masih terdapat ruang kajian untuk mengintegrasikan UU PDP dengan *Siracusa Principles* dan *proportionality test*, sekaligus menghubungkannya dengan konsekuensi sosiologis berupa *chilling effect* dan konsekuensi filosofis melalui konsep *Digital Panopticon*. Kesenjangan tersebut menempatkan penelitian ini pada upaya menganalisis bukan hanya manfaat FRT bagi keamanan dan pelayanan publik, tetapi juga batas kekuasaan negara dalam memproses data biometrik serta mekanisme pengawasan dan pertanggungjawabannya dalam negara hukum demokratis.

Berdasarkan perkembangan tersebut, penelitian ini bertujuan menganalisis bagaimana UU PDP membatasi kewenangan negara dalam pemrosesan data biometrik melalui FRT serta bagaimana desain dan efektivitas pengawasan kelembagaan memengaruhi akuntabilitas penggunaannya. Analisis dilakukan melalui *Siracusa Principles* dan *proportionality test* untuk menilai legalitas, tujuan yang sah, kebutuhan, dan keseimbangan antara kepentingan keamanan dan perlindungan hak fundamental, kemudian diperluas melalui perspektif *chilling effect*, *Digital Panopticon*, dan martabat manusia. Urgensi penelitian semakin kuat karena pemanfaatan FRT berkembang lebih cepat daripada pembentukan batas sektoral khusus mengenai penggunaan pengenalan wajah untuk pengawasan negara, sementara mekanisme kelembagaan pelindungan data pribadi masih menjadi persoalan aktual, sebagaimana tercermin dalam Perkara Nomor 236/PUU-XXIV/2026 yang pada Juli 2026 masih berada dalam tahap pemeriksaan permohonan di Mahkamah Konstitusi. Kebaruan penelitian terletak pada integrasi perspektif yuridis, sosiologis, dan filosofis dengan UU PDP sebagai kerangka hukum nasional serta *Siracusa Principles* dan *proportionality test* sebagai parameter pembatasan kekuasaan negara. Kontribusi penelitian mencakup kontribusi doktrinal berupa perumusan batas kewenangan negara dalam pemrosesan data biometrik, kontribusi teoritis melalui integrasi *proportionality test*, *chilling effect*, dan *Digital Panopticon*, serta kontribusi kebijakan berupa rekomendasi pengawasan independen, otorisasi yudisial untuk pengawasan invasif, audit algoritma, transparansi pemrosesan, dan penguatan perlindungan Data Pribadi yang bersifat spesifik.

## METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif dengan pendekatan perundang-undangan (*statute approach*), konseptual (*conceptual approach*), dan kasus (*case approach*) untuk menganalisis batas kewenangan negara dalam pemrosesan data biometrik melalui *Facial Recognition Technology* (FRT). Pendekatan sosio-legal digunakan secara terbatas untuk membaca implikasi sosial pengawasan berbasis FRT melalui studi kepustakaan dan dokumen empiris, sedangkan pendekatan filsafat hukum digunakan untuk menganalisis privasi, otonomi, kebebasan, dan martabat manusia melalui konsep *Chilling Effect* dan *Digital Panopticon*. Bahan hukum primer meliputi UUD NRI Tahun 1945, UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, peraturan terkait, ICCPR, *Siracusa Principles*, serta dokumen resmi perkara Mahkamah Konstitusi; bahan hukum sekunder berupa buku dan jurnal ilmiah, sedangkan laporan ELSAM, SAFEnet, kebijakan penyelenggara layanan, dan dokumen kelembagaan digunakan sebagai dokumen pendukung atau sumber empiris. *Mass surveillance* dipahami sebagai pemantauan populasi secara luas dan tidak terarah, sedangkan *mass facial recognition* merujuk pada penggunaan FRT untuk mengidentifikasi atau mencocokkan wajah dalam jumlah besar secara sistematis di ruang publik, yang dibedakan dari verifikasi identitas individual dan *targeted surveillance*.

Penelusuran bahan dilakukan melalui basis data peraturan resmi, laman Mahkamah Konstitusi, basis data jurnal ilmiah, serta sumber resmi pemerintah dan organisasi masyarakat sipil dengan kata kunci seperti “*Facial Recognition Technology*”, “data biometrik”, “UU Pelindungan Data Pribadi”, “*mass surveillance*”, “*Siracusa Principles*”, “*proportionality test*”, “*Chilling Effect*”, dan “*Digital Panopticon*”. Seleksi sumber didasarkan pada relevansi, otoritas, keterkinian, dan kemampuannya mendukung analisis pemrosesan biometrik, pembatasan hak, akuntabilitas negara, dan dampak sosial pengawasan digital. Dokumen Mahkamah Konstitusi dibatasi pada dokumen resmi Perkara Nomor 236/PUU-XXIV/2026 yang relevan, dengan status perkara diperlakukan sesuai tahap pemeriksaannya sehingga dokumen persidangan tidak digunakan untuk menyimpulkan putusan final apabila belum tersedia. Analisis dilakukan secara kualitatif-preskriptif melalui analisis bahan hukum dan *legal reasoning*, pengujian pembatasan hak berdasarkan *Siracusa Principles* dan *proportionality test*, serta analisis terpisah terhadap implikasi sosial dan filosofis untuk merumuskan batas kewenangan negara dan rekomendasi pengawasan FRT.

## HASIL DAN PEMBAHASAN

### Hasil

#### Kedudukan Data Biometrik dan Batas Kewenangan Negara dalam UU PDP

Temuan penelitian menunjukkan bahwa UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) telah memberikan dasar normatif bagi perlindungan data biometrik, tetapi masih terdapat ruang diskresi dalam pemrosesan untuk kepentingan pertahanan, keamanan nasional, penegakan hukum, dan penyelenggaraan negara. Pasal 4 ayat (2) huruf b UU PDP secara eksplisit mengategorikan data biometrik sebagai Data Pribadi yang bersifat spesifik, sehingga pemrosesannya berada dalam rezim perlindungan yang lebih ketat. Pada saat yang sama, Pasal 15 UU PDP memungkinkan pembatasan hak tertentu subjek data untuk kepentingan yang ditentukan undang-undang. Dengan demikian, persoalannya bukan bahwa Pasal 15 merupakan “cacat hukum”, melainkan adanya kebutuhan untuk memperjelas batas kewenangan, ruang diskresi, dan mekanisme pengawasan negara.



### Data Biometrik sebagai Data Pribadi yang Bersifat Spesifik

Temuan penelitian menunjukkan bahwa klasifikasi data biometrik sebagai Data Pribadi yang bersifat spesifik menjadi dasar penting dalam menilai penggunaan FRT dalam perspektif perlindungan data. Pemrosesan karakteristik wajah melalui pengambilan, pencocokan, penyimpanan, atau penggunaan representasi wajah harus ditempatkan dalam kerangka prinsip perlindungan data, termasuk keterbatasan tujuan, relevansi, keamanan, dan akuntabilitas. Persetujuan merupakan salah satu dasar pemrosesan, tetapi bukan satu-satunya dasar yang dimungkinkan oleh UU PDP sesuai dengan kondisi yang ditentukan undang-undang. Oleh karena itu, persoalan utama penggunaan FRT oleh negara terletak pada keabsahan dasar pemrosesan, kejelasan tujuan, batas kewenangan, serta kecukupan perlindungan dan pengawasan.

### Pengecualian Hak Subjek Data dan Ruang Diskresi Negara

Temuan penelitian menunjukkan bahwa Pasal 15 UU PDP menjadi titik penting dalam menyeimbangkan perlindungan hak subjek data dengan kepentingan negara. Ketentuan tersebut memungkinkan pembatasan hak tertentu dalam konteks pertahanan dan keamanan nasional, penegakan hukum, serta kepentingan umum dalam penyelenggaraan negara, tetapi tidak dapat ditafsirkan sebagai pembebasan seluruh kewajiban perlindungan data. Semakin luas pengecualian diterapkan, semakin diperlukan batas tujuan, prosedur, dokumentasi, pengawasan, dan mekanisme pemulihan yang jelas. Dengan demikian, persoalannya bukan inkonstitusionalitas Pasal 15 secara otomatis, melainkan potensi ruang diskresi yang luas apabila pengecualian diterapkan tanpa *safeguards* yang memadai.

### Desain Kelembagaan dan Efektivitas Implementasi Pelindungan Data

Temuan penelitian menunjukkan adanya kesenjangan antara desain kelembagaan UU PDP dan efektivitas implementasinya dalam pengawasan perlindungan data pribadi. Pasal 58 sampai dengan Pasal 60 UU PDP telah menyediakan dasar normatif mengenai fungsi kelembagaan, sehingga istilah “kekosongan otoritas” kurang tepat dan lebih relevan dipahami sebagai persoalan pembentukan, independensi, kapasitas, dan efektivitas pengawasan. Dokumen perkara Mahkamah Konstitusi Nomor 236/PUU-XXIV/2026 digunakan sebagai dokumen proses hukum yang relevan, bukan sebagai putusan final yang menentukan keadaan hukum secara definitif. Dengan demikian, efektivitas perlindungan data biometrik bergantung tidak hanya pada norma substantif, tetapi juga pada kemampuan kelembagaan dalam melakukan pengawasan, pemeriksaan, koreksi, dan pemulihan hak.

### Posisi Pemrosesan Biometrik pada Layanan Publik: Kasus PT KAI

Temuan penelitian terhadap *face recognition boarding gate* PT Kereta Api Indonesia (KAI) menunjukkan adanya pemrosesan data biometrik dalam layanan publik yang lebih tepat dipahami sebagai verifikasi atau autentikasi identitas. Praktik tersebut tidak dengan sendirinya dapat dikategorikan sebagai pengawasan massal oleh negara karena hubungan antara sistem FRT PT KAI dan kewenangan aparat negara memerlukan bukti mengenai akses, integrasi, atau penggunaan bersama. Dokumen yang tersedia menunjukkan adanya persoalan mengenai transparansi, pilihan pengguna, penyimpanan, keamanan, dan tujuan pemrosesan data biometrik. Oleh karena itu, kasus PT KAI digunakan sebagai contoh empiris penetrasi FRT dalam layanan publik dan persoalan perlindungan data, bukan sebagai bukti konklusif praktik *state surveillance* atau *mass surveillance*.

### Batas Pembatasan Hak atas Privasi dalam Penggunaan FRT

Temuan penelitian menunjukkan bahwa penggunaan FRT oleh negara perlu dinilai berdasarkan legalitas, tujuan yang sah, *suitability*, *necessity*, *proportionality stricto sensu*, serta prinsip non-diskriminasi dan non-arbitrariness. *Siracusa Principles* digunakan sebagai parameter pembatasan hak, sedangkan *proportionality test* digunakan untuk menilai hubungan antara tujuan, instrumen, alternatif yang tersedia, dan beban terhadap hak individu. Semakin invasif pemrosesan FRT, semakin kuat tuntutan terhadap dasar hukum yang jelas, tujuan spesifik, kebutuhan yang nyata, *safeguards*, dan pengawasan yang efektif. Berdasarkan parameter tersebut, penggunaan FRT secara *indiscriminate* tanpa *safeguards* yang memadai tidak memenuhi unsur *necessity* dan *proportionality stricto sensu*.



**Gambar 1. Pergeseran Panoptik Klasik ke Panoptik Digital**

Gambar 1 menggambarkan alur analisis untuk menilai apakah penggunaan *Facial Recognition Technology* (FRT) oleh negara dapat dibenarkan sebagai pembatasan hak atas privasi dan kebebasan individu. Kerangka tersebut dimulai dari legalitas dan tujuan yang sah, kemudian dilanjutkan dengan pengujian *suitability*, *necessity*, dan *proportionality stricto sensu*. Setiap tahap mempertimbangkan *safeguards*, seperti transparansi, pembatasan tujuan, pengawasan independen, keamanan data, dan mekanisme pemulihan. Dengan demikian, kepentingan keamanan atau kepentingan publik tidak otomatis membenarkan penggunaan FRT, khususnya yang bersifat luas dan tidak terarah, tanpa memenuhi persyaratan hukum dan prinsip HAM.

### Pengujian Berdasarkan *Siracusa Principles*

Temuan analisis menunjukkan bahwa legalitas pembatasan hak melalui FRT tidak cukup didasarkan pada keberadaan norma umum, tetapi juga memerlukan dasar hukum yang jelas, dapat diakses, dan dapat diperkirakan. Prinsip *prescribed by law* dan *legitimate aim* mensyaratkan dasar kewenangan yang jelas serta tujuan pembatasan yang sah, sedangkan *necessity* dan proporsionalitas menuntut kebutuhan yang nyata dan keseimbangan antara kepentingan publik dan dampaknya terhadap hak individu. Pembatasan tersebut juga harus diterapkan tanpa diskriminasi dan tindakan sewenang-wenang sehingga alasan keamanan tidak menjadi dasar kewenangan yang tidak terbatas. Semakin luas dan tidak terarah penggunaan FRT, semakin kuat tuntutan terhadap kejelasan hukum, pembuktian kebutuhan, pembatasan tujuan, pengawasan independen, dan mekanisme pemulihan.

### Matriks Pengujian Proporsionalitas

Berdasarkan *proportionality test*, penelitian tidak menyatakan bahwa seluruh FRT gagal memenuhi *suitability* karena tidak tersedia data akurasi, *false-positive rate*, atau pengujian teknis setiap sistem yang digunakan di Indonesia. Analisis *suitability* karena itu dibatasi pada kemampuan rasional FRT dalam mendukung tujuan yang ditetapkan serta risiko teknis yang dapat memengaruhi keandalannya, termasuk bias algoritmik. Pada tahap *necessity*, persoalan menjadi lebih kuat pada penggunaan FRT yang luas dan tidak terarah karena perlu

dipertimbangkan apakah tujuan yang sama dapat dicapai melalui metode yang lebih terbatas dan kurang invasif. Pada tahap *proportionality stricto sensu*, pemrosesan biometrik terhadap populasi luas menimbulkan beban privasi yang lebih besar sehingga manfaat keamanan harus dapat dibuktikan sebanding dengan tingkat intervensi terhadap hak individu.

**Tabel 1. Matriks Analisis Pembatasan Hak dalam Penggunaan FRT**

| Tahapan/Prinsip                                                     | Pertanyaan Pengujian                                               | Dasar Normatif/Bukti                                       | Temuan                                                                               | Kesimpulan Bersyarat                                                                |
|---------------------------------------------------------------------|--------------------------------------------------------------------|------------------------------------------------------------|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Legalitas<br>( <i>Prescribed by Law</i> )                           | Apakah FRT memiliki dasar hukum yang jelas dan dapat diperkirakan? | UU PDP dan instrumen HAM                                   | UU PDP memberi kerangka umum, tetapi pengaturan sektoral FRT belum rinci.            | Semakin invasif penggunaan, semakin spesifik dasar hukum yang diperlukan.           |
| Tujuan yang Sah<br>( <i>Legitimate Aim</i> )                        | Apakah FRT digunakan untuk tujuan publik yang sah?                 | UU PDP dan <i>Siracusa Principles</i>                      | Keamanan dan penegakan hukum dapat menjadi tujuan sah dengan batas yang jelas.       | Dapat dibenarkan jika tujuan konkret dan relevan.                                   |
| Kesesuaian<br>( <i>Suitability</i> )                                | Apakah FRT mampu mendukung tujuan yang ditetapkan?                 | Literatur FRT dan risiko akurasi/bias                      | Data teknis sistem spesifik tidak tersedia; terdapat risiko akurasi dan bias.        | Belum dapat dipastikan tanpa bukti kinerja sistem.                                  |
| Kebutuhan<br>( <i>Necessity</i> )                                   | Apakah tersedia metode yang kurang membatasi hak?                  | <i>Siracusa Principles</i> dan <i>proportionality test</i> | FRT tidak terarah perlu dibandingkan dengan metode identifikasi yang lebih terbatas. | Berpotensi tidak memenuhi <i>necessity</i> jika alternatif kurang invasif tersedia. |
| Proporsionalitas Sempit<br>( <i>Proportionality Stricto Sensu</i> ) | Apakah manfaat seimbang dengan dampak terhadap hak?                | ICCPR, prinsip proporsionalitas, UU PDP                    | Pemrosesan populasi luas menimbulkan dampak privasi lebih besar.                     | Tidak proporsional jika manfaat tidak sebanding dengan tingkat intervensi.          |
| Non-diskriminasi & Non-arbitrariness                                | Apakah penggunaan bebas dari                                       | Prinsip HAM dan perlindungan data                          | Risiko bias dan penggunaan                                                           | Penggunaan luas memerlukan                                                          |

|                                              |                                                                   |                           |                                                                                     |                                                                                    |
|----------------------------------------------|-------------------------------------------------------------------|---------------------------|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
|                                              | diskriminasi<br>dan<br>kesewenang-<br>wenangan?                   |                           | tanpa batas<br>tujuan<br>memerlukan<br>audit dan<br><i>safeguards</i> .             | pengujian<br>teknis dan<br>kelembagaan.                                            |
| Pemulihan<br>( <i>Effective<br/>Remedy</i> ) | Apakah<br>tersedia<br>mekanisme<br>keberatan<br>dan<br>pemulihan? | UU PDP dan<br>prinsip HAM | Efektivitas<br>pemulihan<br>bergantung<br>pada<br>pengawasan<br>dan<br>kelembagaan. | Akuntabilitas<br>belum<br>optimal tanpa<br>mekanisme<br>pemulihan<br>yang efektif. |

*Sumber: Diolah penulis berdasarkan analisis bahan hukum, dokumen kelembagaan, dan instrumen HAM yang digunakan dalam penelitian.*

Tabel 1 menunjukkan hasil pengujian normatif penggunaan FRT berdasarkan *proportionality test* dan prinsip pembatasan hak dalam *Siracusa Principles*. Legalitas dan tujuan yang sah pada prinsipnya dapat dipenuhi apabila terdapat dasar hukum yang jelas dan kepentingan publik yang sah, sedangkan *suitability* belum dapat dinilai secara konklusif karena tidak tersedia data akurasi dan *false-positive rate* sistem yang dianalisis. Persoalan lebih kuat muncul pada aspek *necessity* dan *proportionality stricto sensu* ketika FRT digunakan secara luas dan tidak terarah tanpa pembuktian kebutuhan serta keseimbangan dampaknya terhadap privasi. Prinsip non-diskriminasi, non-arbitrariness, dan mekanisme pemulihan juga menjadi *safeguards* penting agar pembatasan hak tidak berkembang menjadi kewenangan negara yang tidak terkontrol.

### Matriks Pengujian Proporsionalitas

Matriks tersebut menunjukkan bahwa penggunaan FRT harus dinilai melalui rangkaian pengujian yang saling berkaitan, bukan hanya berdasarkan keberadaan tujuan keamanan. *Judicial warrant* ditempatkan sebagai *safeguard* yang direkomendasikan untuk pengawasan yang sangat invasif, bukan sebagai persyaratan universal yang secara eksplisit diwajibkan UU PDP untuk seluruh pemrosesan FRT. Klaim *suitability* harus didukung bukti kinerja sistem, sedangkan *necessity* dan *proportionality stricto sensu* menjadi semakin penting ketika pemrosesan dilakukan secara luas, tidak terarah, dan tanpa *safeguards* memadai. Berdasarkan parameter penelitian, pengawasan massal FRT yang dilakukan secara *indiscriminate* tanpa *safeguards* memadai tidak memenuhi unsur *necessity* dan *proportionality stricto sensu*.

### Potensi Dampak Sosial Pengawasan FRT terhadap Kebebasan Sipil

Temuan penelitian menunjukkan bahwa kemampuan FRT melakukan identifikasi otomatis dapat memengaruhi perilaku sosial ketika masyarakat menyadari bahwa aktivitasnya di ruang publik berpotensi direkam dan dikaitkan dengan identitas biometrik. Karena penelitian tidak menggunakan wawancara atau survei primer, dampak tersebut tidak diposisikan sebagai fakta empiris yang telah diukur secara langsung. Analisis *chilling effect* didasarkan pada literatur, dokumen masyarakat sipil, dan kerangka konseptual mengenai hubungan antara pengawasan, persepsi keterlihatan, dan perilaku individu. Dengan demikian, penggunaan FRT yang invasif berpotensi mendorong pembatasan ekspresi, penghindaran aktivitas tertentu, atau



penurunan partisipasi publik, tetapi temuan tersebut dipahami sebagai **potensi manifestasi sosial**, bukan besaran dampak yang telah dibuktikan melalui data lapangan.

**Tabel 2. Matriks Potensi Manifestasi Sosial Penggunaan FRT**

| Dimensi                        | Mekanisme Potensial                  | Potensi Manifestasi Sosial            | Dasar Analisis                                |
|--------------------------------|--------------------------------------|---------------------------------------|-----------------------------------------------|
| Kebebasan berekspresi          | Identifikasi otomatis                | Menahan ekspresi sensitif             | <i>Chilling effect</i> dan pengawasan digital |
| Kebebasan berkumpul            | Hilangnya anonimitas                 | Menghindari kegiatan berkumpul        | Privasi, HAM, dan pengawasan                  |
| Otonomi individu               | Persepsi terus diawasi               | Penyesuaian perilaku                  | <i>Chilling effect</i>                        |
| Kepercayaan terhadap institusi | Ketidakjelasan penggunaan data       | Meningkatnya ketidakpercayaan         | Tata kelola data dan privasi                  |
| Partisipasi publik             | Berkurangnya anonimitas ruang publik | Menurunnya partisipasi sosial-politik | Kebebasan sipil                               |

*Sumber: Diolah penulis berdasarkan studi kepustakaan dan dokumen pendukung; bukan hasil pengukuran empiris primer.*

Tabel 2 memetakan potensi dampak sosial penggunaan FRT terhadap kebebasan berekspresi, kebebasan berkumpul, otonomi individu, kepercayaan terhadap institusi, dan partisipasi publik. Dampak tersebut terutama berkaitan dengan berkurangnya anonimitas, meningkatnya persepsi keterlihatan, serta ketidakpastian mengenai tujuan dan penggunaan lanjutan data biometrik. Karena penelitian tidak menggunakan wawancara atau survei primer, dampak tersebut diposisikan sebagai potensi manifestasi sosial berdasarkan studi kepustakaan dan dokumen pendukung. Dengan demikian, risiko FRT tidak hanya berkaitan dengan kehilangan kendali atas data pribadi, tetapi juga berpotensi memengaruhi perilaku, kebebasan sipil, dan kepercayaan masyarakat terhadap institusi.

Hasil penelitian tidak menyatakan bahwa setiap penggunaan FRT pasti menghasilkan *Chilling Effect*, karena risikonya bergantung pada karakteristik dan tata kelola sistem yang digunakan. Potensi tersebut semakin kuat ketika FRT diterapkan secara luas, tidak transparan, sulit ditolak, tidak memiliki batas retensi yang jelas, atau memungkinkan pemrosesan lanjutan tanpa sepengetahuan subjek data. Sebaliknya, tujuan pemrosesan yang terbatas, pemberitahuan yang memadai, mekanisme keberatan, pembatasan retensi, dan pengawasan independen dapat mengurangi risiko tersebut. Oleh karena itu, *Chilling Effect* ditempatkan sebagai risiko sosial terhadap kebebasan sipil yang perlu diperhitungkan dalam pengujian proporsionalitas, bukan sebagai fakta empiris universal.

### Temuan Filosofis: FRT, Otonomi, Identitas, dan *Digital Panopticon*

Temuan filosofis menunjukkan bahwa FRT mengubah relasi antara individu dan pengawasan karena identifikasi dapat dilakukan secara otomatis, kontinu, dan dikaitkan dengan

identitas individual. Analisis ini berfokus pada konsekuensi kemampuan tersebut terhadap otonomi dan martabat, terutama ketika wajah diubah menjadi data yang dapat dicari, dicocokkan, diklasifikasikan, dan disimpan. Kondisi tersebut menciptakan asimetri informasi antara pengelola sistem dan individu yang menjadi objek identifikasi, khususnya ketika subjek tidak mengetahui kapan, untuk tujuan apa, dan oleh siapa datanya diproses. Dalam perspektif *Digital Panopticon*, daya pengawasan tidak hanya terletak pada kemampuan melihat individu, tetapi juga pada kemampuan mengubah identitas dan keberadaannya menjadi informasi yang dapat terus diproses oleh sistem kekuasaan.

FRT mengubah hubungan antara identitas dan otonomi karena karakteristik wajah yang melekat pada tubuh dapat menjadi kunci untuk menghubungkan seseorang dengan berbagai informasi lain. Berbeda dari kata sandi atau identitas yang dapat diganti, identitas biometrik bersifat melekat sehingga pemrosesan tanpa batas tujuan dan kontrol yang memadai dapat menimbulkan risiko yang lebih persisten terhadap otonomi individu. FRT juga mengubah hubungan antara ruang publik dan privasi karena keberadaan seseorang di ruang publik tidak serta-merta menghilangkan kepentingannya untuk mengendalikan informasi mengenai dirinya. Dengan demikian, kemampuan identifikasi otomatis dapat memperkuat asimetri antara negara atau pengelola sistem dan warga sebagai subjek data yang memiliki keterbatasan dalam mengetahui serta mengendalikan penggunaan representasi biometriknya.

Temuan tersebut dapat dirumuskan sebagai pergeseran dari “diawasi” menjadi “dapat diidentifikasi dan ditelusuri”, karena FRT memungkinkan pengamatan dikaitkan langsung dengan identitas individual. Konsekuensinya, risiko terhadap martabat manusia tidak hanya muncul dari pengamatan, tetapi juga dari kemungkinan reduksi identitas menjadi atribut komputasional yang dapat diklasifikasikan dan diproses. Dalam perspektif Kantian, kondisi tersebut relevan dengan prinsip bahwa manusia harus diperlakukan sebagai tujuan pada dirinya sendiri, bukan semata-mata sebagai sarana untuk mencapai tujuan administratif atau keamanan. Oleh karena itu, transparansi, pembatasan tujuan, kontrol subjek data, pengawasan independen, dan akuntabilitas algoritmik merupakan *safeguards* yang sekaligus melindungi otonomi dan martabat manusia.

## Pembahasan

### Batas Kewenangan Negara dalam Pemrosesan Data Biometrik melalui FRT

Temuan penelitian menunjukkan bahwa UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) telah memberikan fondasi normatif untuk membatasi pemrosesan *Facial Recognition Technology* (FRT) karena data biometrik dikategorikan sebagai Data Pribadi yang bersifat spesifik. FRT tidak dapat diperlakukan sebagai teknologi identifikasi biasa karena karakteristik wajah melekat pada individu dan dapat diproses serta dihubungkan dengan informasi lain secara otomatis, sehingga menimbulkan risiko pengumpulan data secara tidak sah, pemantauan berlebihan, *profiling*, kesalahan identifikasi, dan *function creep* (Anggriawan et al., 2026). Karakteristik tersebut menuntut tata kelola, pembatasan, keamanan, dan akuntabilitas yang lebih kuat dalam penggunaan FRT untuk mencegah pelanggaran privasi dan keamanan data (Husna et al., 2025). Dengan demikian, klasifikasi data biometrik sebagai Data Pribadi yang bersifat spesifik memiliki konsekuensi substantif berupa tuntutan kehati-hatian dan pertanggungjawaban yang lebih tinggi terhadap negara. Temuan ini menjawab tujuan penelitian pertama bahwa kewenangan negara dalam menggunakan FRT harus dibatasi berdasarkan perlindungan data biometrik dan prinsip pertanggungjawaban hukum.

Persetujuan tidak dapat dijadikan satu-satunya ukuran legalitas pemrosesan FRT karena UU PDP memungkinkan penggunaan dasar pemrosesan lain sesuai dengan kondisi yang ditentukan undang-undang. Oleh karena itu, pembatasan kewenangan negara harus mencakup kejelasan dasar dan tujuan pemrosesan, ruang lingkup penggunaan, retensi, akses, serta mekanisme pengawasan. Wirearme (2025) menunjukkan bahwa penggunaan FRT oleh pemerintah dalam pelayanan publik dan keamanan menghadirkan ketegangan antara kepentingan keamanan dan efisiensi administrasi dengan perlindungan privasi, kebebasan sipil, kesetaraan, *due process*, dan hak konstitusional warga. Selain itu, potensi kesalahan identifikasi dan bias algoritmik dapat menimbulkan diskriminasi serta penyalahgunaan sistem hukum sehingga memerlukan perlindungan hukum dan mekanisme akuntabilitas yang memadai (Hilmi & Marpaung, 2025). Dengan demikian, keberadaan dasar pemrosesan saja tidak cukup karena kewenangan negara harus disertai pembatasan tujuan, *safeguards*, transparansi, dan pengawasan yang efektif.

Persoalan tersebut semakin kompleks dalam penerapan Pasal 15 UU PDP yang memberikan pengecualian terhadap hak subjek data dalam konteks pertahanan, keamanan, penegakan hukum, dan penyelenggaraan negara. Pengecualian tersebut tidak tepat dimaknai sebagai pembebasan seluruh kewajiban perlindungan data karena kewenangan negara tetap harus dibatasi oleh prinsip *rule of law*. Dalam konteks Indonesia, penggunaan FRT dalam pengawasan dapat menimbulkan ketegangan antara kepentingan keamanan publik dan perlindungan privasi, terutama ketika pemrosesan wajah berpotensi memengaruhi hak-hak dasar warga (Rambe & Abdurrahman, 2024). Persoalan juga muncul dalam penegakan hukum karena FRT berbasis kecerdasan artifisial dapat memengaruhi proses pembuktian dan penilaian terhadap seseorang sehingga diperlukan standar hukum yang menjamin keandalan teknologi dan mencegah kerugian terhadap individu (Rustam et al., 2026). Oleh karena itu, penelitian ini tidak menempatkan Pasal 15 sebagai ketentuan yang otomatis inkonstitusional, tetapi menegaskan perlunya interpretasi yang ketat terhadap tujuan, ruang lingkup, dan prosedur penggunaan pengecualian tersebut.

Temuan mengenai kelembagaan menunjukkan bahwa persoalan perlindungan data biometrik lebih tepat dipahami sebagai kesenjangan antara desain kelembagaan UU PDP dan efektivitas implementasinya, bukan semata-mata ketiadaan otoritas pengawas. Efektivitas pengawasan bergantung pada independensi, kapasitas, kewenangan pemeriksaan, dan kemampuan penegakan terhadap pelanggaran pemrosesan data. Pemrosesan biometrik dalam layanan publik juga memerlukan kejelasan interoperabilitas dan pengelolaan data karena pertukaran antarinstansi dapat memperluas pihak yang terlibat sekaligus menimbulkan persoalan pembagian tanggung jawab (Supardi et al., 2026). Prartama dan Ahmad (2025) menegaskan bahwa pertukaran data melalui sistem yang saling terhubung membutuhkan kejelasan mengenai dasar pemrosesan, mekanisme pertukaran, akuntabilitas, dan perlindungan subjek data. Dengan demikian, batas kewenangan negara tidak hanya ditentukan oleh apa yang boleh diproses, tetapi juga oleh siapa yang mengawasi, kewenangan apa yang dimiliki, dan bagaimana pertanggungjawaban dapat dilakukan.

### **FRT, *Siracusa Principles*, dan *Proportionality Test***

Hasil penelitian menunjukkan bahwa penggunaan FRT sebagai instrumen yang berpotensi membatasi hak harus diuji melalui legalitas, tujuan yang sah, *suitability*, *necessity*, dan *proportionality stricto sensu*. *Siracusa Principles* menegaskan bahwa pembatasan hak harus memiliki dasar hukum, tujuan yang sah, diperlukan dalam masyarakat demokratis, serta bebas dari tindakan diskriminatif dan sewenang-wenang. Kerangka tersebut relevan karena

FRT memungkinkan identifikasi otomatis dan memiliki kapasitas pengawasan yang lebih besar dibandingkan pengawasan konvensional. Penggunaan *retrospective facial recognition*, misalnya, memungkinkan rekonstruksi aktivitas individu dari rekaman yang telah dikumpulkan sebelumnya sehingga dampaknya harus dinilai berdasarkan konsekuensi terhadap hak asasi manusia, bukan hanya kemampuan teknologinya. Gabrielli (2025) menunjukkan bahwa penggunaan FRT dalam pengawasan ruang publik dapat meningkatkan risiko *mass surveillance* serta memengaruhi privasi, kebebasan berekspresi, dan kebebasan berkumpul, sedangkan Salam et al. (2026) menekankan pentingnya *necessity*, proporsionalitas, transparansi, dan akuntabilitas dalam tata kelola teknologi pengawasan.

Pada aspek *suitability*, penelitian ini tidak menyatakan bahwa seluruh FRT gagal memenuhi persyaratan tersebut karena tidak tersedia data akurasi, *false-positive rate*, atau hasil audit terhadap sistem tertentu yang digunakan di Indonesia. Namun, adanya potensi bias algoritmik menunjukkan bahwa kinerja FRT dapat berbeda berdasarkan kondisi penggunaan dan karakteristik kelompok yang diuji. Oleh karena itu, *suitability* harus dibuktikan melalui data teknis, pengujian empiris, dan audit terhadap sistem yang benar-benar digunakan, bukan semata-mata berdasarkan klaim efisiensi atau akurasi. Pendekatan tersebut memungkinkan penelitian membedakan antara risiko umum teknologi FRT dan bukti mengenai kinerja sistem tertentu. Dengan demikian, penilaian proporsionalitas tetap didasarkan pada bukti dan konteks penggunaan, bukan pada asumsi bahwa seluruh sistem FRT memiliki tingkat akurasi atau risiko yang sama.

Persoalan menjadi lebih kuat pada tahap *necessity* ketika FRT digunakan secara luas dan tidak terarah terhadap populasi. Penggunaan untuk verifikasi identitas dengan tujuan terbatas masih memiliki hubungan langsung dengan tujuan pelayanan atau keamanan, sedangkan penggunaan *indiscriminate* memerlukan pembuktian bahwa metode alternatif yang kurang invasif tidak memadai. Kamal et al. (2024) menunjukkan bahwa penggunaan *face recognition* dalam layanan publik, seperti sistem *boarding gate*, tetap memiliki implikasi terhadap hak individu sehingga perlu dinilai berdasarkan konteks dan dampaknya terhadap subjek data. Sementara itu, Girsang (2024) menunjukkan bahwa perkembangan FRT dalam keamanan dan penegakan hukum memerlukan pengaturan lebih spesifik karena karakteristik dan risikonya tidak sepenuhnya dapat diakomodasi oleh kerangka perlindungan data pribadi yang bersifat umum. Dengan demikian, semakin luas cakupan identifikasi dan semakin tinggi intensitas pemrosesan, semakin besar pula beban negara untuk membuktikan bahwa penggunaan FRT benar-benar diperlukan.

Pada tahap *proportionality stricto sensu*, manfaat keamanan harus dibandingkan dengan beban yang ditimbulkan terhadap privasi, otonomi, dan kebebasan sipil. Pemrosesan wajah terhadap populasi luas memiliki tingkat intrusi lebih tinggi dibandingkan penggunaan FRT untuk verifikasi identitas dalam layanan tertentu. Oleh karena itu, penggunaan FRT secara *indiscriminate* tanpa *safeguards* yang memadai berpotensi tidak memenuhi prinsip *necessity* dan *proportionality stricto sensu*, tetapi kesimpulan tersebut merupakan penilaian normatif berdasarkan parameter penelitian dan bukan klaim bahwa seluruh penggunaan FRT selalu tidak proporsional. Kerangka *proportionality test* dengan demikian dapat digunakan untuk menilai tingkat pembatasan hak sesuai dengan tujuan, cakupan, dan risiko penggunaan teknologi. Semakin tinggi tingkat intervensi terhadap hak individu, semakin kuat pula tuntutan terhadap pembatasan, pengawasan, dan mekanisme perlindungan yang harus diterapkan negara.

Temuan tersebut menjawab tujuan penelitian mengenai penggunaan *Siracusa Principles* dan *proportionality test* dalam menentukan batas kewenangan negara. *Proportionality test* mengoperasionalkan prinsip HAM melalui tahapan pemeriksaan terhadap



dasar hukum, tujuan, kesesuaian teknologi, kebutuhan, alternatif yang tersedia, dan keseimbangan antara manfaat dengan dampak terhadap hak. Kerangka tersebut tidak hanya menentukan boleh atau tidaknya penggunaan FRT, tetapi juga menentukan tingkat *safeguards* yang harus diterapkan sesuai tingkat risiko. Dengan demikian, proporsionalitas menjadi instrumen untuk memastikan bahwa kewenangan negara tidak melebihi tingkat intervensi yang diperlukan untuk mencapai tujuan yang sah. Pendekatan ini sekaligus memberikan dasar analitis untuk menempatkan penggunaan FRT dalam kerangka negara hukum yang mengutamakan perlindungan hak fundamental.

### FRT dan *Chilling Effect* terhadap Kebebasan Sipil

Temuan penelitian menunjukkan bahwa konsekuensi FRT tidak hanya berupa hilangnya kendali atas data biometrik, tetapi juga berpotensi memengaruhi perilaku individu ketika terdapat persepsi bahwa identitas dan aktivitas mereka dapat diketahui secara otomatis. Kondisi tersebut dapat mengurangi keberanian individu untuk mengekspresikan pandangan, berkumpul, atau berpartisipasi dalam aktivitas tertentu. Murray (2024) menempatkan *chilling effect* sebagai salah satu konsekuensi penting peningkatan kemampuan pengawasan melalui FRT karena teknologi tersebut memperbesar kapasitas untuk mengidentifikasi dan menelusuri individu. Dalam konteks ini, privasi tidak hanya berfungsi sebagai perlindungan terhadap data pribadi, tetapi juga sebagai ruang yang memungkinkan individu bertindak secara otonom tanpa rasa terus-menerus diawasi. Dengan demikian, risiko *chilling effect* menjadi bagian penting dalam menilai dampak penggunaan FRT terhadap kebebasan sipil.

Penelitian ini tidak menyatakan bahwa *chilling effect* telah terjadi pada masyarakat Indonesia dalam besaran tertentu karena penelitian tidak menggunakan survei atau wawancara primer untuk mengukur perubahan perilaku masyarakat. Oleh karena itu, *chilling effect* diposisikan sebagai risiko sosial yang dapat diprediksi berdasarkan karakteristik pengawasan FRT, bukan sebagai temuan empiris mengenai besaran perubahan perilaku. Risiko tersebut dipengaruhi oleh transparansi, tujuan pemrosesan, akses terhadap data, durasi penyimpanan, serta persepsi masyarakat terhadap legitimasi institusi yang menggunakan teknologi. Semakin luas dan tidak transparan penggunaan FRT, semakin besar pula kemungkinan individu merasakan adanya pengawasan yang dapat memengaruhi kebebasan bertindak. Karena itu, potensi *chilling effect* perlu diperhitungkan dalam pengujian proporsionalitas penggunaan FRT oleh negara.

Dari perspektif *socio-legal*, perlindungan data tidak cukup diarahkan pada keamanan penyimpanan dan pencegahan kebocoran, tetapi juga harus memperhitungkan dampak sosial akibat persepsi pengawasan. Meloni (2026) menunjukkan bahwa penggunaan FRT dalam penegakan hukum tidak hanya menimbulkan persoalan perlindungan data dan diskriminasi, tetapi juga persoalan keadilan sosial dan dampak intrusif teknologi dalam kehidupan sehari-hari pada konteks *algorithmic governance*. Robles et al. (2025) juga menunjukkan bahwa perkembangan FRT dalam penegakan hukum membutuhkan kerangka regulasi yang mampu menyeimbangkan kepentingan keamanan dengan perlindungan hak, etika, dan akuntabilitas. Temuan tersebut menunjukkan bahwa regulasi FRT perlu memperhatikan bukan hanya bagaimana data dilindungi, tetapi juga bagaimana keberadaan sistem pengawasan memengaruhi perilaku masyarakat. Dengan demikian, penggunaan FRT yang sah secara administratif tetap perlu dievaluasi berdasarkan dampaknya terhadap ruang kebebasan sipil.

Temuan ini menjawab tujuan penelitian mengenai implikasi sosial penggunaan FRT dengan menunjukkan bahwa desain teknologi dan desain hukum dapat memengaruhi perilaku sosial. Batas tujuan, transparansi, mekanisme keberatan, pengawasan independen, dan

pemulihan yang efektif dapat mengurangi ketidakpastian serta persepsi pengawasan berlebihan. Sebaliknya, ketidakjelasan mengenai perolehan, pencocokan, penyimpanan, dan pembagian data wajah dapat memperkuat persepsi pengawasan dan meningkatkan risiko *chilling effect*. Oleh karena itu, perlindungan terhadap kebebasan sipil harus ditempatkan sebagai bagian dari tata kelola FRT dan bukan sebagai konsekuensi yang dipertimbangkan setelah teknologi diterapkan. Pendekatan tersebut memungkinkan negara memperoleh manfaat teknologi tanpa menciptakan lingkungan sosial yang mendorong individu membatasi dirinya karena rasa terus-menerus diawasi.

### **FRT, *Digital Panopticon*, Otonomi, dan Martabat Manusia**

Temuan filosofis menunjukkan bahwa FRT menghasilkan bentuk pengawasan yang berbeda dari pengawasan konvensional karena mampu menghubungkan pengamatan dengan identitas individu secara otomatis. Dalam perspektif *Digital Panopticon*, persoalannya bukan hanya individu dapat dilihat, tetapi juga dapat dikenali, diklasifikasi, dan ditelusuri melalui data biometrik. Kemampuan tersebut memperluas dimensi kekuasaan pengawasan karena wajah dapat menjadi penghubung antara identitas, lokasi, aktivitas, dan informasi lain dalam sistem digital. Gabrielli (2025) menunjukkan bahwa penggunaan FRT di ruang publik dapat meningkatkan risiko *mass surveillance* dan mengurangi ruang anonimitas individu, sedangkan Almeida et al. (2022) menempatkan FRT sebagai teknologi pengawasan yang menimbulkan persoalan keseimbangan antara keamanan kolektif dan hak privasi. Dengan demikian, *Digital Panopticon* dapat dipahami sebagai kondisi ketika individu selalu berpotensi untuk diidentifikasi dan diawasi melalui infrastruktur digital.

Implikasi penting berikutnya berkaitan dengan otonomi individu karena wajah merupakan karakteristik yang melekat pada tubuh dan tidak dapat dengan mudah diganti seperti kata sandi atau identitas digital. Sifat tersebut menyebabkan pemrosesan biometrik tanpa batas tujuan dan kontrol yang memadai berpotensi menimbulkan risiko yang lebih persisten terhadap individu. Otonomi tidak hanya berkaitan dengan kemampuan memberikan persetujuan, tetapi juga kemampuan mengetahui dan mengendalikan bagaimana representasi biometrik digunakan. Ketika individu tidak mengetahui kapan, untuk apa, dan oleh siapa data wajah diproses, terjadi ketimpangan informasi antara subjek data dan institusi yang mengendalikan teknologi. Oleh karena itu, pembatasan pemrosesan, transparansi, dan mekanisme pengawasan menjadi instrumen penting untuk menjaga otonomi individu dalam lingkungan pemerintahan digital.

Temuan tersebut juga memperlihatkan hubungan antara FRT dan martabat manusia karena wajah dapat direduksi menjadi *template*, *faceprint*, atau atribut komputasional yang digunakan untuk kepentingan administratif maupun keamanan. Kondisi tersebut tidak berarti bahwa setiap penggunaan biometrik secara otomatis merendahkan martabat, tetapi menunjukkan pentingnya memastikan bahwa individu tetap diperlakukan sebagai subjek hukum dan bukan semata-mata sebagai objek identifikasi. Transparansi, tujuan terbatas, akuntabilitas, dan mekanisme untuk mempertanyakan pemrosesan menjadi penting agar teknologi tidak menghilangkan posisi individu sebagai pemegang hak. Dengan demikian, perlindungan martabat manusia menuntut adanya batas terhadap kemampuan negara untuk mengidentifikasi, mengklasifikasi, dan menelusuri individu melalui sistem biometrik. Perspektif ini memperluas analisis FRT dari persoalan teknis dan privasi menuju persoalan hubungan kekuasaan dan kedudukan manusia dalam tata kelola digital.

Jika dikaitkan dengan tujuan penelitian, perspektif *Digital Panopticon* menjelaskan konsekuensi filosofis penggunaan FRT terhadap relasi negara dan warga negara. Kekuasaan

pengawasan tidak hanya berasal dari kemampuan melihat, tetapi juga dari kemampuan menghubungkan wajah, identitas, lokasi, aktivitas, dan data lain melalui proses komputasional. Karena itu, transparansi, pembatasan tujuan, audit algoritma, pembatasan retensi, pengawasan independen, dan mekanisme pemulihan memiliki fungsi tidak hanya administratif, tetapi juga dalam menjaga otonomi dan martabat individu. Dengan demikian, *Digital Panopticon* memperkuat argumentasi bahwa batas penggunaan FRT harus dibangun berdasarkan kepentingan keamanan dan efisiensi sekaligus perlindungan terhadap hak fundamental. Hasil tersebut menegaskan bahwa pengembangan teknologi pengawasan yang bertanggung jawab harus mempertahankan posisi warga negara sebagai subjek hukum yang memiliki hak untuk mengetahui, mengontrol, dan mempertanyakan pemrosesan data yang berkaitan dengan dirinya.

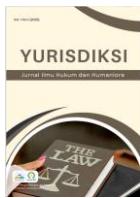
## KESIMPULAN

Penelitian ini menunjukkan bahwa penggunaan *Facial Recognition Technology* (FRT) oleh negara harus ditempatkan dalam batas kewenangan yang jelas karena data biometrik merupakan Data Pribadi yang bersifat spesifik dan pemrosesannya berpotensi membatasi hak atas privasi serta kebebasan individu. UU PDP memberikan dasar perlindungan, tetapi penerapan FRT tetap memerlukan kejelasan tujuan, batas kewenangan, pengawasan, dan *safeguards* yang memadai, terutama pada penggunaan yang luas dan tidak terarah. Berdasarkan *Siracusa Principles* dan *proportionality test*, penggunaan FRT secara *indiscriminate* tanpa pembuktian kebutuhan dan keseimbangan manfaat dengan dampaknya terhadap hak individu berpotensi tidak memenuhi prinsip *necessity* dan *proportionality stricto sensu*. Dari perspektif sosiologis dan filosofis, kondisi tersebut juga berpotensi menimbulkan *Chilling Effect* serta memperkuat karakter *Digital Panopticon* yang memengaruhi otonomi dan martabat manusia.

Implikasi penelitian ini menegaskan perlunya tata kelola FRT yang mengintegrasikan kepastian hukum, pengawasan independen, transparansi, audit algoritma, pembatasan tujuan dan retensi, serta mekanisme pemulihan bagi subjek data. Bagi pembuat kebijakan, hasil penelitian dapat menjadi dasar untuk memperjelas regulasi sektoral dan membangun mekanisme pengawasan yang sebanding dengan tingkat intrusi teknologi terhadap hak individu. Bagi penelitian selanjutnya, diperlukan kajian empiris mengenai akurasi sistem, *false-positive rate*, praktik kelembagaan, serta dampak penggunaan FRT terhadap perilaku dan kebebasan sipil masyarakat Indonesia. Dengan demikian, pengembangan FRT di masa mendatang diharapkan tetap mendukung kepentingan keamanan dan pelayanan publik tanpa mengorbankan privasi, otonomi, kebebasan, dan martabat manusia.

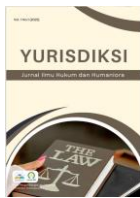
## DAFTAR PUSTAKA

- Almeida, D., Shmarko, K., & Lomas, E. (2022). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: A comparative analysis of US, EU, and UK regulatory frameworks. *AI and Ethics*, 2, 377–387. <https://doi.org/10.1007/s43681-021-00077-w>
- Anggriawan, R., Hamsin, M. K., Karsai, K., & He, Y. (2026). Facial recognition in asylum seeker procedures: Criminal implications of data misuse and profiling. *Jurnal Media Hukum*, 33(1), 99–117. <https://doi.org/10.18196/jmh.v33i1.29861>
- Basron, B., Adellah, A., & Athaya, N. (2026). Penerapan artificial intelligence (AI) dalam sistem administrasi publik: Peluang, tantangan, dan etika pelayanan publik di Indonesia. *Public Service and Governance Journal*, 7(1), 217–229. <https://doi.org/10.56444/psgj.v7i1.3579>



- Fadhilla, S. R., & Putra, M. S. (2024). Kompleksitas penggunaan face recognition technology oleh PT Kereta Api Indonesia ditinjau dari aspek perlindungan data pribadi dan sistem interoperabilitas. *Jurnal Al Azhar Indonesia Seri Ilmu Sosial*, 5(3).  
<https://doi.org/10.36722/jaiss.v5i3.3031>
- Fauziah, H. Y., & Kusuma, T. M. (2025). Penerapan Deepface dan Retinaface dalam pengenalan wajah parsial untuk aplikasi keamanan digital. *Jurnal Ilmiah Informatika Komputer*, 30(2). <https://doi.org/10.35760/ik.2025.v30i2.241>
- Gabrielli, G. (2025). The use of facial recognition technologies in the context of peaceful protest: The risk of mass surveillance practices and the implications for the protection of human rights. *European Journal of Risk Regulation*, 16(2), 514–541.  
<https://doi.org/10.1017/err.2025.26>
- Girsang, S. Y. B. (2024). Pentingnya regulasi khusus sistem face recognition technology sebagai produk artificial intelligence dalam peningkatan keamanan dan penegakan hukum di Indonesia. *Nommensen Journal of Legal Opinion*, 5(2), 86–98.  
<https://doi.org/10.51622/njlo.v5i2.1817>
- Hilmi, F., & Marpaung, Z. A. (2025). Perlindungan hukum bagi korban penggunaan teknologi pengenalan wajah. *Jurnal Antologi Hukum*, 5(1), 18–37.  
<https://doi.org/10.21154/antologihukum.v5i1.5128>
- Husna, N., Nurman, M., & Nugroho, Y. (2025). Pembentukan Peraturan Pemerintah tentang face recognition technology ditinjau dari Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. *Jurnal Ilmiah AKSES*, 3(2).  
<https://unars.ac.id/ojs/index.php/akses/article/view/7126>
- Kamal, M. Y., Azhar, M., & Suhartoyo. (2024). Implikasi penggunaan artificial intelligence terhadap hak-hak pekerja (studi terhadap face recognition boarding gate di Stasiun Semarang Tawang Bank Jateng). *Diponegoro Law Journal*, 13(2).  
<https://doi.org/10.14710/dlj.2024.43580>
- Kurniawan, K. S., & Kurniawan, I. G. A. (2025). The limitations of lex generalis: Analyzing the readiness of the GDPR and PDP Law for AI-based facial recognition technology. *SIGn Jurnal Hukum*, 7(2). <https://doi.org/10.37276/sjh.v7i2.533>
- Meloni, F. (2026). Facial recognition on trial: Data protection, discrimination, and the ethics of algorithmic governance in policing. *Information & Communications Technology Law*. <https://doi.org/10.1080/13600834.2026.2638629>
- Murray, D. (2024). Police use of retrospective facial recognition technology: A step change in surveillance capability necessitating an evolution of the human rights law framework. *The Modern Law Review*, 87(4), 833–863. <https://doi.org/10.1111/1468-2230.12862>
- Pramudito, D. K. (2025). Facial recognition technology in Indonesia: Opportunities and ethical challenges. *The Journal of Academic Science*, 2(2). <https://doi.org/10.59613/vfs73h61>
- Prartama, A. S., & Ahmad, G. A. (2025). Analisis peraturan pemrosesan data lintas negara Undang-Undang Perlindungan Data Pribadi Indonesia dibandingkan dengan General Data Protection Regulation (GDPR) Uni Eropa. *Indonesian Journal of Contemporary Law*, 2(5). <https://journal.unesa.ac.id/index.php/ijcl/article/view/44672>
- Pratiwi, A., Rahmawyanet, M. E., Wibowo Putra, P. A., & Sensuse, D. I. (2025). Systematic literature review on artificial intelligence in Indonesia's public sector: Reimagining digital government. *JITK (Jurnal Ilmu Pengetahuan dan Teknologi Komputer)*, 11(2).  
<https://doi.org/10.33480/jitk.v11i2.6842>
- Putri, D. T. (2025). Regulating digital privacy in Indonesia: The practice of data subject rights and controller duties in the FotoYu app. *Istinbath: Jurnal Hukum*, 22(2), 230–262.





<https://doi.org/10.32332/istinbath.v22i02.art01>

- Rambe, R., & Abdurrahman, L. (2024). Implikasi etika dan hukum dalam penggunaan teknologi pengenalan wajah: Perlindungan privasi versus keamanan publik. *Jurnal Hukum Caraka Justitia*, 4(2), 90–104. <https://doi.org/10.30588/jhcj.v4i2.1828>
- Robles, P., Mallinson, D. J., Best, E., et al. (2025). Global perspectives on regulating facial recognition technology utilization for criminal justice arrests. *Global Public Policy and Governance*, 5, 186–204. <https://doi.org/10.1007/s43508-025-00117-9>
- Rustam, D. R., Widiastih, N. P. S., & Tise, S. (2026). The probative value of artificial intelligence-based facial recognition in the Electronic Traffic Law Enforcement (ETLE) system under the beyond a reasonable doubt standard. *Jurnal Hukum Volkgeist*, 10(2), 325–332. <https://www.jurnalumbuton.ac.id/index.php/Volkgeist/article/view/8336>
- Salam, S., Asmah, Kiro, M. R., Yasim, S., & Muhammed, I. K. (2026). Human rights protection in the ecosystem of surveillance technology and big data law enforcement. *Indonesia Media Law Review*, 5(1). <https://journal.unnes.ac.id/journals/imrev/article/view/44290>
- Sembiring, P. E., Ramli, A. M., & Rafianti, L. (2024). Implementasi desain privasi sebagai pelindungan privasi atas data biometrik. *Veritas et Justitia*, 10(1), 127–152. <https://doi.org/10.25123/vej.v10i1.7622>
- Supardi, D. A., Ghofar, H. S. A., Dzaki, D. H. N., Hadiyantina, S., & Magistra, M. R. (2026). Joint data controller responsibility in OSS RBA system interoperability after the Personal Data Protection Law enactment. *Kertha Patrika*, 48(1), 1–19. <https://doi.org/10.24843/KP.2026.v48.i01.p01>
- Syahputra, F., Sabrina, E., Sitorus, A., Lubis, K. M. N., Saragi, F. J., & Sinaga, N. N. (2026). Keamanan pengenalan wajah berbasis deep learning: Tinjauan sistematis serangan adversarial dan strategi pertahanan (systematic literature review). *TRILOGI: Jurnal Ilmu Teknologi, Kesehatan, dan Humaniora*, 6(4). <https://doi.org/10.33650/trilogi.v6i4.13424>
- Wiredarme. (2025). Constitutional limits on government use of facial recognition technology in public services and public security. *Jurnal Kecerdasan Buatan dan Teknologi Informasi*, 4(3), 356–363. <https://ojs.ninetyjournal.com/index.php/JKBTI/article/view/491>
- Zahro, A. K. (2025). Perlindungan privasi individu dalam penggunaan face recognition: Tinjauan hukum dan etika. *SPEKTRUM HUKUM*, 21(2), 150–159. <https://doi.org/10.56444/sh.v21i2.5779>